apdcat
Autoritat Catalana de Protecció de Dades

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



File identification

Resolution of sanctioning procedure no. PS 27/2020, referring to the Mutual Aid Foundation of Terrassa, FPC

Background

1. On 08/10/2019, the Catalan Data Protection Authority received a letter from a person filing a complaint against the Fundació Assistencial Mútua de Terrassa FPC (hereinafter, FAMT), on the grounds of 'an alleged breach of the regulations on the protection of personal data. Specifically, the complainant complained that on 09/30/2019 someone who provides services at the Primary Care Center (...) - managed by the FAMT - accessed his shared medical history (HC3). The complainant added that he had not been a patient of this CAP for 8 years, which is why he considered that no worker at that center should have accessed his HC3.

In order to substantiate the facts reported, the reporting person provided a copy of what would be the log of access to his HC3 taken from the *"Lamevasalut"* portal of the Department of Health (portal that the Department makes available to interested persons for so that they can consult the accesses made to their HC3). In this register there are five consecutive accesses (which can be grouped into a single access) to the HC3 of the reporting person carried out on 09/30/2019 from the *"CAP (...)" health center,* with the following details :

- 2:06 p.m. *"Information consulted: Summary clinical history information".*
- 2:14 p.m. *"Information consulted: Information Clinical reports".*
- 2:15 p.m. *"Information consulted: Social Data Information".*
- 2:15 p.m. *"Information consulted: Integral Clinical Course Information".*
- 2:15 pm *"Information consulted: Summary clinical history information".*

2. The Authority opened a preliminary information phase (no. IP 270/2019), 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, by means of a letter dated 10/21/2019, the reported entity was required to comply with the following:

- Provide a copy of the record of access to the reporting person's medical history available to the CAP (...), in the period between 01/01/2019 and 09/30/2019, both inclusive .

- Justify each of the accesses made to the medical history of the reporting person during the indicated period.

4. On 07/11/2019, the FAMT responded to the aforementioned request in writing in which it set out the following:

- That, in the period between 01/01/2019 and 09/30/2019, there have been two accesses to the medical history of the complainant, both made by the nurse Mrs. (...) of the CAP (...).

- That on 10/24/2019 Ms. (...) in order to justify its access to the medical history of the person reporting.

- That Mrs.(...) responded to this request by letter dated 10/30/2019, in which she stated that *"access to the medical history is because the patient in question is my sister ( ...), and the reason is the concern for her state of health".* That, therefore, in this case, *"the worker has admitted that access to the medical history of the patient who has filed the complaint before the "APDCAT does not respond to the purpose of care, but to personal motivations, given its kinship relationship with the patient".*

- That *"regardless of whether the disciplinary procedure continues, the worker has already been verbally reprimanded (...)".*
- That *"we consider that in this case there is no need to appreciate the entity's responsibility in relation to the access that has motivated the complaint of Ms. (...), because the entity's action has been in accordance with the personal data protection policy, both in the adoption of prior measures, and in the collaboration with the APDCAT in the investigation of the 'incident and repair of possible damages (...). We understand that the entity's actions have been proactive in terms of measures to prevent improper access, and diligent in the investigation of the facts that have motivated the patient's complaint. Taking into account the particular circumstances that the patient has not at any time addressed any previous complaint or claim for this reason to the Customer Service Service of Mútua de Terrassa or to the DPD, and that only a week had passed from the consultation made and the filing of the complaint before the APDCAT (...)".*

In its letter, the FAMT detailed certain measures it had implemented in its organization in order to comply with data protection regulations, among others, the definition of different access profiles to information systems, the drafting *of a "patient security document in which the obligations of the users of the patient database are collected",* the realization of monthly audits on access to clinical histories, training of the working people, adherence to codes of conduct, etc. He also provided, among other things, the following documentation:

- Register of accesses to the reporting person's clinical history available to the CAP (...) in the period between 01/01/2019 and 09/30/2019. This record states that

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

on 22/07/2019 at 7:08 p.m. and 30/09/2019 at 2:06 p.m., Ms. (...) with a professional profile of "Nurse", she accessed the HC3 of the person making the complaint.

- Document entitled *"Internal regulations for the workers and collaborators of Mútua Terrassa in relation to information systems and data confidentiality",* signed by Ms. (...) on 07/19/2012.
- *"Patient safety document".* Point 5.4 of said document states the following literal:

  *"the fact that the user wants to access the corporate assistance application, the security measures of which we will develop later, is relevant, must mark a box according to which he accepts the content in a clause. A screen print with the corresponding clause is presented below, which is still a reminder about the maintenance of the duty of confidentiality".*

5. On 16/06/2020, 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) 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 circulation thereof (hereafter, RGPD), in relation to the article 5.1.f) of this same rule and 5 of Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (hereinafter, LOPDGDD). This initiation agreement was notified to the imputed entity on 07/01/2020.

6. On 07/15/2020, the FAMT formulated a statement of objections to the initiation agreement, together with which it provided various documentation.

7. On 05/11/2020, the instructor of this procedure formulated a resolution proposal, by which she proposed that the director of the Catalan Data Protection Authority
imposed on the FAMT a fine of 2,500 euros as responsible for an infringement provided for in article 83.5.a) in relation to article 5.1.f) of this same rule and 5 of the LOPDGDD.

This resolution proposal was notified on 11/11/2020 and a period of 10 days was granted to formulate allegations.

8. On 11/24/2020, the accused entity submitted a written statement in which it acknowledges its responsibility for the alleged acts and attests to having made on 11/23/2020 the voluntary payment in advance of 1,500 euros (one thousand five -hundreds) corresponding to the monetary penalty proposed by the instructor in the resolution proposal, once the reductions provided for in article 85 of the LPAC have been applied.

proven facts

Ms. (...), who provides service as a nurse at the Primary Care Center (...)-managed by the Mutual Aid Foundation of Terrassa (FAMT)- accessed on 07/22/2019 at 18:08

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

hours and 09/30/2019 at 2:06 p.m., through the FAMT's clinical history management computer application, in the shared clinical history of the person reporting here - and at the same time sister of Mrs. (...)-, without the access being justified for an assistance or administrative reason.

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 85.3 of the LPAC, both the recognition of responsibility and the voluntary advanced payment of the proposed monetary penalty lead to the application of reductions. The effectiveness of these reductions is conditioned on the withdrawal or renunciation of any action or appeal through the administrative route against the sanction. For both cases, sections 1 and 2 of article 85 of the LPAC provide for the termination of the procedure.

Although it presented allegations in the initiation agreement, the accused entity has not formulated allegations in the resolution proposal, since it has accepted the two options to reduce the amount of the penalty. Nevertheless, it is considered appropriate to reiterate below the most relevant of the reasoned response that the instructor gave to the allegations before the initiation agreement.

2.1. About the applicable penalty regime.

In its statement of objections to the initiation agreement, the accused entity stated that, to the extent that the data processing that had motivated the complaint was related to access to the HC3 - who is responsible the Department of Health - and that the FAMT's access to this platform is carried out, not as part of its private activity, but *"as an entity in charge of the treatment"* of the data of the patients treated on behalf of the Catalan Health Service (CATSALUT), must apply to the FAMT the special sanctioning regime provided for in article 77 of the LOPDGDD, which foresees not imposing financial sanctions on certain categories of persons responsible (or in charge) of treatment that have violated the regulations.

In this regard, it must be said that the list of entities cited in this legal precept is a closed list that does not allow an application by analogy, and the legislator has not considered it appropriate to include in this closed list the entities that act as in charge of the treatment of a public administration, whatever its legal form.

2.2. On the implementation of security measures.

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

In the 2nd section of its statement of objections to the initiation agreement, the accused entity set out that *"the Agreement to implement the HCCC acknowledges, in Exhibit 12, that FAMT has certified before CATSALUT compliance with the requirements of procedural, functional and technical that have been required",* and that the *"FAMT complies with both the rules, recommendations and the homogeneous criteria of the Technical Commission on Clinical Documentation (Order SLT/108/2013) for the control of access to the electronic clinical history by the professionals of health centers in Catalonia".* In short, the FAMT argued in its defense that *"it has complied at all times with the appropriate technical and organizational security measures to protect the confidentiality of access to the personal data of the HCCC file",* and in order to accredit - this was provided by various and numerous documentation, among other things, a specific risk analysis report for the *"Treatment: access to the HC3",* the certification of an external auditor on *"compliance with the legal requirements in terms of the record of access to patient databases";* and, the certification issued by the Secretary of the Commission for Data Protection of the companies and entities of Mútua de Terrassa, of which the FAMT is an integral part certifying that
*"in the course of 2019, the corresponding control audits of the Register of Access to the entity's electronic medical records have been carried out on a monthly basis".*

The FAMT added that, specifically with regard to access to medical history, *"information is repeatedly provided to users of corporate databases about the consequences in the event that they carry out improper access through the internal rules sheet for the use of systems who sign upon being granted a user code of the patient database, the 3 legal notices on the duty of confidentiality and compliance with the regulations on data protection that must be accepted each time when accessing the corporate PC, in the electronic clinical history database (HCIS) and HC3; the dissemination of the internal Code of Conduct, the Data Protection Decalogue for health and administrative staff, the internal control procedure for the HCE access register and the disciplinary procedure, specific training in the field of personal data protection (. .. )".*

Finally, the FAMT highlighted that from the risk analysis carried out by the entity, to which reference has been made, it was inferred that the database *"of shared electronic clinical histories of Catalonia is a treatment of high risk for the rights of the interested parties, due to the type of data that is the subject of the treatment (health data), but with the application of the corrective measures the probability of the risk is reduced, so that the only residual risk but the confidentiality must necessarily come from the intention of the users who carry out the improper access",* as would be the case of the action of the nurse who had given rise to the initiation of this sanctioning procedure, and who the FAMT had imposed a disciplinary sanction.

In this regard, it must be said that the lack of security measures is not penalized in this procedure, but the confidentiality of the data has been breached, an obligation provided for in article 5.1.f) of the RGPD and 5 of the LOPDGDD, and that has a different content to the obligations described in articles 25 and 32 of the RGPD, linked to 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 accidental loss, destruction or damage of data or its unauthorized or unlawful processing; and another the duty of confidentiality that

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

it is up to 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.

Finally, it must be noted that according to the system of responsibility provided for in the RGPD and particularly in article 70 of the LOPDGDD, responsibility for breaches of data protection regulations falls, among others, on those responsible and those in charge of the treatments, and not about their employees.

It is because of all the above that it was considered that the allegations made by the FAMT could not prosper

2.3. About the penalty to be imposed.

In its latest plea to the initiation agreement, the FAMT listed a series of mitigating factors that, in its opinion, should be taken into account when determining the penalty to be imposed.

The analysis of mitigating factors will be carried out in the 4th legal basis, which analyzes the penalty to be imposed in this procedure.

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 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".*

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 *" los principios 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 in article 5 of this Organic Law"*

4. When the FAMT does not fit into any of the entities provided for in article 77.1 of the LODGDD, 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, to be 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 a maximum of the global total annual business volume of the previous financial year, opting for the higher amount. This, without prejudice to the fact that, as an additional or substitute, the measures provided for in clauses a) ah) ij) of Article 58.2 RGPD may be applied.

In the present case, as explained by the instructor in the resolution proposal, the possibility of replacing the sanction of an administrative fine with the sanction of reprimand provided for in article 58.2.b) RGPD should be ruled out. The nature of the declared proven facts, relating to the violation of the confidentiality principle with respect to data of special protection (health data), prevents the application of the warning figure. And it is that health data enjoys special protection in the data protection regulations, precisely because it is data that affects the most intimate and private sphere of people.

Once it has been ruled out that the penalty of an administrative fine should be replaced by a warning, the amount of the administrative fine to be imposed must be determined. According to what is established in articles 83.2 RGPD and 76.2 LOPDGDD, and also in accordance with the principle of proportionality enshrined in article 29 of Law 40/2015, as indicated by the investigating person in the proposed resolution, the sanction should be imposed of 2,500 euros (two thousand five hundred euros). This quantification of the fine is based on the weighting between the aggravating and mitigating criteria indicated below.

On the one hand, the following circumstances can be seen that operate as mitigating criteria, some of them invoked by the FAMT:

- The limited number of improper accesses (2 in the period of 9 months) which, given the circumstance, were carried out by an employee who in turn is the sister of the complainant, accesses which, according to what she explained in within the disciplinary procedure initiated by the FAMT, they were prompted by the family's concern for the state of health of the complainant with whom her partner was preventing her from having a fluid relationship (art. 83.2.a RGPD).
- 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).

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

- FAMT's adherence to the code of conduct of the Catalan Hospitals Union (art. 83.2.j GDPR).
- The lack of profits obtained as a result of the commission of the infringement (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).
- That the FAMT has a specific body ("LOPD Commission") whose objective is to ensure good practices in relation to the processing of personal data (art. 83.2.k RGPD).

On the contrary, as indicated by the instructor, it is considered that the application of the following mitigating circumstances presented by the accused entity does not apply:

- Degree of cooperation with the control authority. In this regard, it is worth saying that the mere fact of having responded to this Authority's request in the prior information phase, would not justify the application of the mitigating factor provided for in letter f) of article 83.2; essentially because answering the requirements of this Authority is an obligation of the entities subject to the its scope of action (article 19 of Law 32/2010).
- How the Authority became aware of the infringement. The fact that the complainant went directly to this Authority, without first going to the FAMT, cannot be considered as a mitigating circumstance either. In accordance with the wording of letter h) of article 83.2 of the RGPD, this mitigating factor would be applied in those cases in which it would have been the person responsible or in charge of the treatment who would have informed the authority of control a possible violation of the data protection regulations, which does not occur in the present case.

- Voluntary submission to alternative conflict resolution mechanisms. In this regard, it must be said that having a data protection delegate cannot be included in this mitigating factor, when in the case of the FAMT it is mandatory (art. 37 RGPD); nor have a Customer Service. This mitigating factor would be applied, fundamentally, if the entity had extrajudicial conflict resolution mechanisms, such as mediation by an independent body outside the organization itself.

- The lack of prejudice and damage caused to the affected person and the lack of previous infractions cannot be seen as mitigating criteria, as the accused entity intends, for the reasons set out in the following section in which aggravating causes are analyzed.

In contrast to the attenuating causes set out, a series of criteria from article 83.2 of the RGPD that operate in an aggravating sense also apply:

- Damage or damages caused. The FAMT states that it is not aware of having caused any damage or harm to the reporting person, so it intends to consider this lack of accreditation as a mitigating element of responsibility. Well, in this regard it must be said that, although the existence of a concrete and specific harm to the person affected by the processing of their data cannot be proven, it must be made clear that access to the data

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

of a person's health, without their consent and without legal authorization, assumes *per se* a detriment to the affected person, since this is data that, as stated before, affects the most intimate and private sphere of people (83.2.a of the RGPD).

- The link between FAMT's activity and the processing of personal data (art. 83.2.k of the RGPD and 76.2.b of the LOPDGDD).
- The previous offenses committed (art. 83.2.e of the RGPD). The FAMT as it has been advanced, cites this criterion as mitigating, in the sense that said entity *"has not been subject to any sanction regarding this data processing".* First of all, it should be noted that the wording of article 83.2.e) of the RGPD *["all previous infractions committed by the person in charge or the person in charge of the treatment"]* does not at all imply that the infraction previously committed by the person in charge or person in charge must be related to the same type of treatment subject to a subsequent sanctioning procedure. Starting from this, it should be pointed out that in PS 28/2012 instituted by this Authority, it was determined that the FAMT had been responsible for the commission of three serious infringements. This circumstance therefore operates as an aggravating criterion in the present sanctioning procedure.

5. On the other hand, in accordance with article 85.3 of the LPAC and as stated in the initiation agreement and also in the resolution proposal, if before the resolution of the sanctioning procedure the entity accused acknowledges his responsibility or makes voluntary payment of the pecuniary penalty, a 20% reduction should 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 background, by means of a letter dated 11/24/2020, the accused entity has acknowledged its responsibility and has certified that it paid on 11/23/2020 in advance 1,500 euros (one thousand five hundred), corresponding to the amount of the penalty resulting once the cumulative reduction of 40% 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 Notwithstanding the above, in the present case no measure should be required to cease or correct the effects of the infringement, given that it is of isolated and specific facts, with which the effects of the infringement would have been consummated.

resolution

For all this, I resolve:

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

1. To impose on the Mutual Aid Foundation of Terrassa the sanction consisting of a fine of 2,500 (two thousand five hundred) euros, as responsible for an infringement provided for in 83.5.a) of the RGPD), in relation to the article 5.1.f) of this same rule and 5 of the LOPDGDD.
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, in application of article 85 of the LPAC, has made effective the advance payment of 1,500 euros (one thousand five hundred), an amount that corresponds to 60% of the amount of the monetary penalty proposed by the instructor in the resolution proposal.

3. Notify this resolution to the Mutual Aid 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,