apdcat
Autoritat Catalana de Protecció de Dades

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

File identification

Resolution of sanctioning procedure no. PS 45/2021, referring to the Terrassa Mutual Assistance Foundation, FPC

Background

1. On 09/19/2020, the Catalan Data Protection Authority received a letter from a person for which he filed a complaint against the Fundació Assistance Mútua de Terrassa, FPC (hereinafter, FAMT), with reason for an alleged breach of the regulations on the protection of personal data. The complainant ((...)) stated the following:

- That on 09/17/2020 he exchanged several emails with a worker (...) of the FAMT (Mrs. (...)) in relation to the medical assistance that could be provided to his father That same day, this worker (...) sent him an email - specifically from the address (...) that was accompanied by an attached document (hereinafter, DOCS 1)

- That once he accessed DOCS 1, he found that it did not refer to his father, but to a third person with whom he had no connection.

In order to substantiate the facts reported, the reporting person provided the following documentation:

a) Copy of the emails exchanged with the worker (...) on 09/17/2020. In one of them, sent by the employee (...) at 2:58 p.m. that day, a document titled *"Dependency Act.7z" was attached,* and contained the following text: *"I am attaching the documentation . As soon as you confirm, I'll send you the access code to open it."*

b) Copy of DOCS 1 which contained the following documents referring to Mrs. (...):

b.1) *"Request for recognition of the dependency situation and the right to benefits",* signed by Ms. (...) which includes, among others, the following personal data relating to this person: name and surname, VAT number, address, health card number (CIP), telephone number and the fact that he requested to be able to access the dependency situation.
b.2) *"Health report for the request for recognition of the dependency situation and the right to benefits",* signed by Mrs. (...), which includes a list of the diagnosis of the diseases presented by this person.
b.3) *"Care report"* issued by a doctor from the FAMT (CAP (...), in which the pathologies presented by Mrs. (...), its evolution over time and the treatment to follow.

2. The Authority opened a preliminary information phase (no. IP 288/2020), in accordance with the provisions of article 7 of Decree 278/1993, of November 9, on the sanctioning procedure of application to areas of competence of the Generalitat, and article 55.2 of Law 39/2015, of 1

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

of October, of the common administrative procedure of public administrations (henceforth, LPAC), to determine if the facts were likely to motivate the initiation of a sanctioning procedure.

3. In this information phase, on 10/29/2020 the reported entity was required to report on the following:

- Indicate in detail the procedure through which the FAMT communicates electronically with its patients or relatives; especially with regard to the inclusion of documents attached to said communications. If this procedure is contained in a protocol, it must be provided.

- What explanation would be given to the fact that the person reporting here was sent, in a document attached to the email that the FAMT employee (...) sent to him on 09/17/2020, DOCS 1.

4. On 12/11/2020, the FAMT responded to the aforementioned request in writing in which it set out the following:

- That, *"a visit had been arranged* [with the complainant] *on 22/09/20 with the professional (...), employee(...) of the University Hospital of Mútua de Terrassa, in relation with certain medical documentation required to process the request for the recognition of his father's dependency status (...). The usual procedure in these cases is that the medical reports that must be attached to this type of administrative request are delivered personally to the patient, or to their representative, at the specialist's consultation or at the Center's Primary Care Center of health But due to the exceptional situation we are experiencing due to the COVID19 pandemic, these CAPs cannot attend to these administrative procedures, and the Customer Service and the social workers of the entity are provisionally taking on this task (. ..). According to the worker(...) who sent the email that is included with the complaint, Ms. (...)*

  he had expressed to him by telephone (...), his logistical difficulties in arranging a face-to-face visit (...). For this reason, when, by email, the complainant addressed the worker (...) to cancel the arranged visit and expressly asked her if she could send her the documentation she needed by this same means, this professional , with the intention of giving the greatest facilities to Ms. (...) so that she would look after her father's interests, in an exceptional way she acceded to his request, and sent him the requested documentation by email, adopting as security measures the encryption of the file, and communicating the decryption key later, separately, and only once had its receipt by the correct recipient been verified. The problem in this case lies in the fact that, due to human error, the professional made the wrong file, and attached to her email a file corresponding to another patient (...)".

  Likewise, they added that they had no evidence that the person reporting here had made a complaint to the FAMT about the fact that he had been the subject of a complaint to the Authority.

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

- That, *"due to the exceptional situation due to the COVID19 pandemic, since last March 2020 our organization, as a medical assistance center attached to the Public Health System of Catalonia ("SISCAT"), by recommendation of the Catalan Health Service ("CATSALUT") (...) has started various electronic communication channels with our patients and users, in such a way that they represent an alternative to face-to-face with regard to some procedures (...) . In the case of our entity, the procedures that can be carried out electronically are the appointment request via the Mútua Terrassa website (...) and all the electronic procedures that the portal allows at any given time. MY HEALTH (...). As a general rule, our institution does not consider the use of email as a means of communication with patients and users, although, exceptionally, this means of communication is allowed , but always subject to appropriate security measures and the subscription by the entity's professionals to the compliance with the INTERNAL RULES FOR USE OF THE CORPORATE SYSTEMS of the entity, which is provided through Document No. 1 that we accompany in our writing, and always within the parameters of the recommendations that, jointly, have been published by Catsalut, the TIC Health and Social Foundation and various professionals from SISCAT centers (...). It is worth saying that the Foundation Asistiental de Mútua de Terrassa provides IT tools to its professionals, always within a context of security measures appropriate to the processing of special category data that are processed, which are periodically verified by an external Auditor.*
  In this sense, the entity has adopted a proactive policy of compliance with the regulations on personal data protection. and among the measures adopted, workers have been properly trained, among whom a DECALEG has been disseminated on the processing of personal data that we provide as Document No. 2, (...); and the use of the entity's information systems has been conditioned on the subscription by them of a commitment of confidentiality and compliance with the duty of privacy in the treatment of the data to which they have access with reason for carrying out their tasks within the entity. (...), the professional who made the mistake in sending the file that has motivated the complaint of Ms. (...) has carried out specific training on the protection of personal data, as evidenced by the certificate attached as Document No. 3. and has also expressly assumed the duty of confidentiality and compliance with the regulations on personal data protection, (...). As a conclusion, we consider that the facts that have motivated the complaint of Ms. (...) are not constitutive of an infringement of the current regulations on the protection of personal data, because these facts respond to a one-off human error, which in no case could have been avoided with the application of technical measures and organizational in the transmission different from those effectively applied in this case (encryption of the file, and the prior confirmation of its receipt by the correct recipient before communicating the decryption code (...)".

The reported entity attached the following documentation with its letter:

a) *"Internal regulations for the workers and collaborators of Mútua Terrassa in relation to the information systems and data confidentiality".*

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

b) *"Decal for data protection for health and administrative personnel published by the AEPD",* which includes the following verbatim in point 6: *"Do not send health data by email. If it is essential, don't forget to encrypt the data".*

c) Certificate of attendance at data protection training regarding Mrs. (...).

5. On 14/07/2021, 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); 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). This initiation agreement was notified to the imputed entity on 07/16/2021.

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 07/27/2021, the FAMT made objections to the initiation agreement.

8. On 18/10/2021, the instructor of this procedure formulated a resolution proposal, by which she proposed that the director of the Catalan Data Protection Authority admonish the FAMT as responsible for an alleged infringement in article 83.5.a) in relation to article 5.1.f), both of the RGPD.

This resolution proposal was notified on 10/20/2021 and a period of 10 days was granted to formulate allegations.

9. On 04/11/2021, the accused entity submitted a letter in which it acknowledged its responsibility for the alleged acts and stated that it had made the voluntary advance payment of the pecuniary penalty proposed by the instructor, which it certified through the 'contribution of a copy of the transfer made.

Indeed, on 02/11/2021, the accused entity paid in advance 1,500 euros (one thousand five hundred euros), corresponding to the pecuniary penalty proposed by the instructor in the resolution proposal, once the reductions foreseen in article 85 of the LPAC.

proven facts

On 09/17/2020, Ms. (...), worker(...) who provides services to the FAMT, sent by email to the person making the complaint (Mrs. (...)) certain documents containing data relating to an unrelated third party with the complainant. These documents -
which were sent encrypted and which the reporting person was able to access using a password - contained various data relating to this third person - many of them from

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

health - among others: first and last name, VAT number, address, health card number (CIP), telephone, the fact that he was asking to be able to access the dependency situation, the pathologies he presented, their evolution over time and the treatment to follow.

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 violation of the principle of confidentiality".*

In the 1st section of its statement of objections to the initiation agreement, the accused entity related the set of technical and organizational measures it had implemented in its organization in order to comply with the regulations for the protection of data, and emphasized those intended to avoid leaks and losses of information, as well as those related to staff training.

In this regard, it must be said that in this procedure, the failure to implement security measures is not penalized, 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 Organic Law 3/2018, of December 5, on the protection of personal data and the 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 to security measures, In other words, one thing is the obligation of the person in charge 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 its unauthorized or unlawful treatment; 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.

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

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.

2.2. About the penalty to be imposed.

In paragraph 2 of its statement of objections, the FAMT advocated that the Authority, in the event that it considered that an infringement had been committed, impose corrective measures in lieu of the sanction of an administrative fine. And then, in section 3 of said letter, the FAMT listed the set of mitigating circumstances that, in the event that a financial penalty was imposed, it considered should be taken into consideration in order to determine its amount.

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.

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"*

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

4. As the FAMT does not fit into any of the subjects 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 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 2,500 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 shipments made - a one-time shipment to a single particular email address-. It is also taken into account that the data that was unduly disclosed affected a single person (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).
- 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 rapid reaction of the FAMT, which as soon as the complainant herself learned of the error committed in the shipment, asked her to remove the improperly sent documentation (art. 83.2.k RGPD).

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

On the contrary, 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 responding to the requirements of this Authority is an obligation of the entities subject to its scope of action (article 19 of Law 32/2010).
- Continuing character of the infringement. The FAMT advocates the application of this mitigating factor on the basis that it was a one-off mistake and therefore it was not a continuous infringement. In this regard, it must be said that the fact that it was an isolated event in time is a circumstance that has already been taken into account in the first of the mitigating factors related to the previous section - art. 83.2.a RGPD-.
- 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 harm and damage caused to the affected person, the lack of previous infringements and the link between the activity of the offender and the practice of processing personal data, cannot be seen as mitigating criteria either, as intended by the accused entity, for the reasons set out in the following section in which the 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 damage or harm to the person to whom the personal data sent by mistake referred, 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 health data of 'a person, 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). And it should be noted that the information sent, all affecting a single person, consisted of several documents with very detailed information about the state of health and medication and treatment plans.

- The link between FAMT's activity and the processing of personal data.
  The FAMT defends the application of this circumstance as mitigating to the extent that the professional who sent the email with the controversial documentation had the professional profile that allowed her to process this type of data. In this regard, it should be noted that this circumstance cannot be seen as mitigating, since the fact that people

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

employees of an entity process personal data in accordance with their professional profile and because of the functions entrusted to them is an obligation imposed by the data protection regulations. The connection of the person in charge with the processing of personal data will operate in this case as an aggravating factor, since the FAMT, precisely because of the amount and quality of personal data it processes, must exercise extreme diligence in all the processing it carries out (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 here, it should be noted that the FAMT has been previously sanctioned (sanctioning procedures no. PS 28/2012, PS 13/2020, PS 27/2020 and PS 50/2020, all of them instituted by this Authority). This circumstance therefore operates as an aggravating criterion in the present sanctioning procedure.

5. Article 85.3 of the LPAC determines that if before the resolution of the sanctioning procedure, the accused entity acknowledges its responsibility or makes the voluntary payment of the pecuniary penalty, a 20% reduction should be applied to the amount of the provisionally quantified penalty. If the two aforementioned cases occur, the reduction is applied cumulatively (40%).

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, by means of a letter dated 04/11/2021, the imputed entity has acknowledged its responsibility. Likewise, he has certified that he has paid 1,500 euros (one thousand five hundred euros) in advance, 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. 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:

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 article 83.5.a) of in relation to the 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 advance payment of 1,500 euros (one thousand five hundred euros), which corresponds to the total amount of the penalty imposed, once the corresponding 40% deduction percentage has been applied to the reductions provided for in article 85 of the LPAC.

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,