apdcat
Autoritat Catalana de Protecció de Dades

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

File identification

Resolution of sanctioning procedure no. PS 35/2021, referring to the Pere Mitjans Foundation

Background

1. On 02/07/2020, the Catalan Data Protection Authority received a letter from a person who filed a complaint against the Pere Mitjans Foundation (hereinafter, the Foundation), on the grounds of a alleged breach of the regulations on the protection of personal data, and attached various documentation on the facts reported.

Specifically, the complainant complained that the Foundation, on 18/05/2020, sent an email with the subject "(...)", from a corporate address of the Foundation (...)), to numerous private recipients (63), without using the blind copy option, and therefore the personal email address of all of them being legible. In the message, they were invited to an electronic meeting of "(...)", and to that effect, they were indicated an electronic link to access it.

2. The Authority opened a preliminary information phase (no. IP 189/2020), 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 were capable of motivating the initiation of a sanctioning procedure.

3. In this information phase, on 30/09/2020 the reported entity was required to, among others, report on the reasons why the option was not used in the aforementioned electronic submission of blind copy, and if the option of blind copy is usually used in the rest of the electronic dispatches you send, and if you had any protocol or instruction on the use of email.

4. On 06/10/2020, the Foundation responded to the aforementioned request in writing in which it set out the following:

- That "the shipment is confirmed by the FPM, specifically by the worker (...) from the email identified by you."

- That "this Foundation always sends these types of emails using the hidden copy option, with the exception of this one, due to a human error by the employee indicated."

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

- That "we have a protocol on the use of electronic mail where the worker is told that this type of mass mail must always be sent with the hidden copy option."

The reported entity attached various documents to the letter, including the "Guide for working people for protection in the use of e-mail" prepared by the Foundation.

5. On 06/21/2021, the director of the Catalan Data Protection Authority agreed to initiate a sanctioning procedure against the Pere Mitjans Foundation for an alleged violation 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 07/02/2021.

6. On 07/21/2021, the Foundation made objections to the initiation agreement, which are addressed in section 2 of the legal foundations.

The accused entity provided various documents with its letter, including the following:

- copy of the various documents issued by the company Prodades (reports, certificates, emails) relating to the Foundation's compliance with data protection security measures, since 2018.
- copy of the letter addressed to the employee who sent the email without hidden copy, in which he is warned of the

fact. - copy of the Statutes of the Pere Mitjans

Foundation - copy of Minutes 1/2020, dated 29/05/2020, of the Board of Trustees meeting, where one of the points to be discussed is the financial situation of the entity. - copy of the

Foundation's email, dated 07/15/2021, which, in relation to the controversial email "(...)", dated 05/18/2020, asks the recipients the following: "(1) Do you consider it to have been a human error and that it only happened that one time?; (2) Has this event caused you any harm?; (3) Do you want the entity to be penalized for this error?". From the collection of the multiple answers received, the coincidence with the answers is verified: (1) they consider that it is a human error and it has only happened once; (2) has not caused them any harm; and (3) they do not want the entity sanctioned.

In this regard, the accused entity stated that it had provided the response emails received so far, and proposed as a test practice to provide more, but, at the discretion of the instructing person, it was considered relevant to not admit it for unnecessary

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

7. On 11/17/2021, the person instructing this procedure formulated a proposed resolution, by which it was proposed that the director of the Catalan Data Protection Authority admonish the Pere Mitjans Foundation 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 18/11/2021 and a period of 10 days was granted to formulate allegations.

8. The deadline has been exceeded and no allegations have been submitted.

proven facts

The Pere Mitjans Foundation sent on 05/18/2020, from a corporate email address, an email with the subject "(...)" to numerous private recipients (63), without using the option of hidden copy This allowed all the recipients of said email, including the complainant, to access the private email address of the rest of the people to whom the message was addressed.

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.

The reported data processing falls within the competence of the Authority under the provisions of article 156.b) of the Statute of Autonomy of Catalonia (EAC) and article 3.h) of the Law 32/2010, to the extent that this treatment would have been carried out within the framework of the provision of a specialized social service provided by the Foundation on behalf of the Department of Social Rights, and, therefore, within the powers attributed to the Administration of the Generalitat in matters of social affairs.

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 On the penalty to be imposed

In this regard, it is necessary to start from the premise that the entity recognizes the commission of the imputed facts, and in this sense the allegations made are not allegations in themselves tending to distort the reality of the facts that motivated the initiation of the procedure or the legal qualification established in the initiation agreement, but instead focus on listing a series of mitigating circumstances that he believes should be taken into account to assess

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

the opportunity to sanction with a warning, or when graduating the amount of the sanction, and to that effect provides supporting documentation.

Having said that, it should be noted that, as indicated in the resolution proposal, without prejudice to the fact that it may be considered that the sending of the controversial email without using the blind copy option could have contributed to some of the mitigating circumstances listed by the entity, it cannot be questioned that this fact led to data processing that violated the principle of confidentiality of the personal data of those affected, as it allowed all the recipients of said e-mail to know the private e-mail addresses of the rest of the recipients, and, at the same time, inferring information that all of them were relatives of users of the services provided by the Foundation, since in the message they were invited to a telematic meeting of "(...)", all and that, this last information, could easily also be known by all the recipients of the mail by the simple fact of participating in the subsequent joint meeting to which they were summoned to t via e-mail.

The analysis of the eventual imposition of a financial penalty, as well as the mitigating factors that could apply, will be carried out in the 4th legal basis.

2.2 About the proposed test

One of the mitigating circumstances that the accused entity exposed is that the sending of the email without using the blind copy option was a specific "human error" of the worker who sent the controversial email with the subject "(...)", and that this fact did not cause damage or prejudice to the majority of recipients.

To prove these circumstances, the entity provided an important sample of e-mails, where different recipients of the controversial e-mail respond to a series of questions formulated by the entity about the imputed facts (reproduced in the 6th legal antecedent), and in general terms state that they consider it to be a human error and that it was the first time it happened, and that this fact had not caused them any harm.

In this regard, the entity proposed as proof, the contribution of more answers received after the submission of the statement of objections to the initiation agreement.

Well, in this respect, the person instructing this procedure indicated in the resolution proposal that the collection of responses provided was a sufficient sample to reinforce the entity's statement that the sending of the controversial email to be a one-time event and that the general perception is that "human error" would be the main explanation, as well as that the majority of recipients considered that it would not have caused them great damage or prejudice the fact that all the recipients of the finger mail could know their private electronic addresses.

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

At this point, it should be remembered that the lack of intentionality (human error), a mitigating factor invoked and that can be taken into consideration when determining the penalty, cannot exonerate responsibility for the acts charged, a responsibility that includes the entity itself assumes by recognizing the facts. In this regard, it is necessary to take into account the doctrine of the principle of culpability, which considers that in order to attribute responsibility for the violations committed to the author, the element of fault must be present, which includes the actions or omissions committed by "mere negligence". In this regard, note that negligence does not require a clear intention to infringe, but rather lies precisely in carelessness, and in this specific case, in the lack of attention required by the entity in fulfilling the duty of confidentiality to what article 5.1.f) of the RGPD refers to, and in relation to this, it should be emphasized that the duty of care is maximum when activities are carried out that affect fundamental rights, such as the right to data protection personal

In accordance with all the above, the person instructing this procedure, goes
consider relevant that, in the resolution proposal, the evidence relating to the entity providing more response emails was not admitted, as unnecessary, because it was considered
that the documentation provided was sufficient to prove that it was an unintentional one-off event and that it did not cause serious harm to the majority of recipients.

3. In relation to the facts described in the proven facts section, relating to the sending of an email without using the blind copy option, it is necessary to refer to article 5.1.f) of the RGPD, which provides for the following:

"1. The personal data will be:
(...)
f) processed in such a way as to guarantee adequate security for personal data, including protection against unauthorized or illegal processing and against accidental loss, destruction or damage, through the application of appropriate technical and organizational measures ("integrity and confidentiality")".

This principle of integrity and confidentiality provided for by the RGPD must be complemented with the duty of secrecy contained in Article 5 of Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (hereinafter, LOPDGDD), which establishes the following:

"Article 5. 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 the applicable regulations.
3. The obligations established in the previous sections remain even if the obligee's relationship with the person in charge or in charge of the treatment has ended.

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

Likewise, it is appropriate to mention article 13 of the LPAC, which lists a catalog of rights of people in their relations with public administrations, in which the right "To the protection of personal data, and in particular the security and confidentiality of the data contained in the files, systems and applications of public administrations".

During the processing of this procedure, the fact described in the section on proven facts has been duly proven, which is constitutive of the violation provided for in article 83.5.a) of the RGPD, which typifies the violation of the "basic principles for the treatment (...)", in relation to article 5.1.f) of the same RGPD.

The conduct addressed here has been included as a very serious infraction in article 72.1.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. Since the Pere Mitjans Foundation is a non-profit private foundation, as indicated in article 3 of its statutes, and which is registered as such in the Register of private foundations of the Generalitat of Catalonia, the general penalty 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, in addition or as a substitute, some other of the measures provided for in article 58.2 RGPD may be applied, especially the one contemplated in sentence b), consisting of a warning.

For its part, article 83.2 of the RGPD determines the following, regarding the graduation of the amount of the administrative fine:

> "2. The administrative fines will be imposed, depending on the circumstances of each individual case, as an additional or substitute for the measures contemplated in article 58, section 2, letters a) ah) yj). When deciding the imposition of an administrative fine and its amount in each individual case, the following shall be duly taken into account:
> a) the nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the processing operation in question as well as the number of interested parties affected and the level of damages and losses they have suffered;
> b) intentionality or negligence in the infringement;
> c) any measure taken by the person responsible or in charge of the treatment to alleviate the damages and losses suffered by the interested parties;

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

d) the degree of responsibility of the person in charge or of the person in charge of the treatment, given the technical or organizational measures that have been applied by virtue of articles 25 and 32;
e) any previous infringement committed by the person in charge or the person in charge of the treatment;
f) the degree of cooperation with the control authority in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

g) the categories of personal data affected by the infringement;

h) the way in which the control authority became aware of the infringement, in particular if the person in charge or the manager notified the infringement and, if so, to what extent;

i) when the measures indicated in article 58, paragraph 2, have been previously ordered against the person in charge or the person in charge in relation to the same matter, the fulfillment of said measures;
j) adherence to codes of conduct under article 40 or certification mechanisms approved under article 42, and
k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as the financial benefits obtained or the losses avoided, directly or indirectly, through the infringement."

In turn, article 76.2 of the LOPDGDD provides that, apart from the criteria established in article 83.2 RGPD, the following can also be taken into account:

"a) The continuing nature of the infringement.
b) Linking the offender's activity with the practice of processing personal data.

c) The profits obtained as a result of the commission of the infringement.
d) The possibility that the conduct of the affected person could have led to the commission of the offence.
e) The existence of a merger process by absorption subsequent to the commission of the infringement, which cannot be imputed to the absorbing entity.
f) Affecting the rights of minors.
g) Have, when not mandatory, a data protection delegate.
h) The submission by the person in charge or person in charge, voluntarily, to alternative conflict resolution mechanisms, in cases where there are disputes between them and any interested party."

In this case, as the instructing person explained in the resolution proposal, it is considered appropriate to replace the sanction of an administrative fine with the sanction of reprimand provided for in article 58.2.b) of the RGPD. In this sense, of the criteria provided for in article 83.2 of the RGPD, some of them invoked by the Foundation as mitigating criteria, the following are taken into account:

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

- The number of sendings carried out and the level of damage caused - At this point, it must be taken into account that it is a one-time sending of an email without a hidden copy whose main purpose was to call a telematic meeting to the families of the center, and regarding this, it should be indicated that the information that could be inferred from the text of the email, the fact that all the recipients were relatives of users of the services provided by the Foundation, is information that could easily also be known by all recipients of the mail for the simple reason of participating in the subsequent joint meeting to which they were summoned via email. Likewise, it must also be taken into account that according to the majority of recipients, the fact has not caused them any harm (art.83.2.a RGPD).

- The lack of intentionality (art.83.2.b RGPD).
- The notice to the employee who sent the email to prevent a repeat similar fact (art. 83.2.c RGPD).
- There is no evidence that the Foundation has previously committed any infringement or been sanctioned in the field of data protection, despite having been reported on several occasions by the same reporting person (art.83.2.e RGPD).
- The category of personal data affected by the infringement - there is no evidence that affecting special categories of data (art. 83.2.g RGPD).
- The lack of benefits as a result of the infringement (art. 83.2.k RGPD and 76.2.c LOPDGDD).
- The Foundation has a "Guide for working people for protection in the use of e-mail", which expressly indicates the use of the blind copy tool when sending of mails with different recipients, and the existence of the commitment to comply with data protection regulations, as inferred from the documentation that certifies that the entity has external advice from a company dedicated to the sector data protection, to carry out training, risk analysis reports and monitoring of security measures (art. 83.2. k RGPD).

- The nature of the entity, which is not for profit (art. 3 of its Statutes), its recognition of the imputed facts (art. 83.2. k RGPD), added to the delicate economic situation in which this entity finds itself , as recorded in the Minutes 1/2020 of the Board of Trustees dated 05/29/2020, therefore prior to the date of presentation of this claim to the Authority

5. 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, 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, which would have consummated the effects of the infringement.

For all this, I resolve:

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

1. Admonish the Pere Mitjans Foundation as responsible for an infringement provided for in article 83.5.a) 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 5th legal basis.

2. Notify this resolution to the Pere Mitjans Foundation.

3. 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 what they provide
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,