Autoritat Catalana de Protecció de Dades

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

File identification

Resolution of sanctioning procedure no. PS 51/2021, referring to the Hospital de Palamós-Baix Empordà Integrated Health Services Foundation.

Background

1. On 09/24/2020, the Catalan Data Protection Authority received a letter from a person for which he filed a complaint against the Fundació Hospital de Palamós Serveis de Salut Integrats Baix Empordà (hereinafter, FHP- SSIBE), due to an alleged breach of the regulations on personal data protection. Specifically, the person reporting stated that, on (...)/2020, the FHP-SSIBE sent an email to parents who had sons or daughters who could be affected by COVID 19, without using the hidden copy option.

The complainant provided a copy of the email that was the subject of the complaint, sent to 14 people, through which the survey and the list of contacts that the parents of the girls had to bring on the day the PCR test was carried out were attached to these; as well as other information about it.

2. The Authority opened a preliminary information phase (no. IP 296/2020), 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 01/25/2021 the reported entity was required to report, among others, on the reasons why the option was not used in the aforementioned electronic submission of hidden copy.

4. On 08/02/2021, the FHP-SSIBE responded to the above-mentioned request in writing in which it set out, among others, the following:

- That the reasons why the e-mail referred to in the file was sent is due to human error caused by the poor knowledge of ICT technologies on the part of the employee sending the e-mail.

- That the recruitment process of the worker who sent the email, as a COVID Manager, took place in the context of a health emergency (she was hired on (...).
- That the employment contract signed with this worker included a series of additional clauses, including the following:
  - The "Contractual clause for the use of media and tools", which stated that "People authorized to enter the computer network, use an account of

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

corporate mail and/or who have access to the Internet, are responsible for their proper use".

o The "Contractual Confidentiality Clause", where it was stated that "All the information and all the documentation that can be generated or that is delivered by the company due to the development of the employment relationship is reserved and confidential according to with Organic Law 15/1999 on the Protection of Personal Data, development and concordant regulations. Therefore, the employee must at all times respect the professional secrecy required by the aforementioned reserved and confidential nature and must refrain from actions that could harm this condition. Any action by the worker that violates the duty of confidentiality established above will be considered very serious misconduct without prejudice to other responsibilities".

- That to access the computer systems of the FHP-SSIBE for the first time, the following documents must first be accessed: Institutional Welcome Manual, Good Practices Manual and the Zimbra Email Server Guide.
- That as part of the processing of the security incident, the worker stated that she had accessed the said documents, although doing a quick reading focusing only on what was highlighted, either in bold or with capital letter
- That in the Institutional Reception Manual (specifically, in the "Information Technologies" section) it is indicated that "When you want to send (or forward) a message to multiple recipients, it is better to put the addresses in CCO (Hidden Carbon Copies) so that they are hidden from other recipients, to prevent someone from making inappropriate, and in any case unauthorized, use. It is also advisable to delete all the addresses that may be in the body of the text of a received message before forwarding it.
- That in the Quick Guide of the Zimbra e-mail service (specifically, in the section "Usando el correo electrónico") it is stated that "If you want to enable the field for hidden copy (BCC) touch the option "Show BCC field "."
- That when the aforementioned worker joined her workplace, she was given training in which it was emphasized that personal data could not be transferred to third parties; he was provided with a guide for Covid Managers drawn up by CatSalut in which it was indicated that during the development of the interview the patient must be informed that "The data you provide us is confidential"; she was informed that on the intranet she could download the Welcome Guide for primary care admissions staff and consult the security document in force at that time; and he was given instructions relating to the confidentiality of the personal data being processed and specifically on the use of e-mail.

- That despite the above, this employee sent the email subject to the complaint to a plurality of recipients without a blind copy because she was unaware of the existence of this option on the Zimbra email server.
- That the worker stated that she had a personal email but
  who was unaware of the existence of the hidden copy option.
- That it is concluded that the email in question was sent without use
  the hidden copy option due to the worker's poor knowledge of ICT technologies in general and of the Zimbra e-mail server in particular.

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

- That the error committed cannot be attributed (at least exclusively) to the worker who materially sent the mail, but that the FHP-SSIBE must also assume its responsibility to be the one who ultimately choose the worker,
  despite the extreme circumstances involved in the worker's recruitment, hiring and incorporation into the workplace.
- That the worker had already started (at the time of answering the request) a training course on data protection and information security and that she would take another course on the organization's IT tools, including the server Zimbra email.

- That the email addresses that appear in the sending of the email that is the subject of the complaint, do not belong to patients of the FHP-SSIBE.
- That the electronic addresses were provided by the owner of a center of (...) in which screening was to be carried out for the children of that activity; and corresponded to their parents. In that email, they were told the day, time and place in which they had to take their children to do the PCR, as well as that they should hand in the form that was filled out.

- That field work has been carried out consisting of viewing emails sent by the worker in question and three other Covid Managers, both prior to (...)/2020 (date of sending the email subject to complaint) as after that date. The result is that in the exercise of the functions of the Covid Managers, they never send emails to more than one recipient. Therefore, the case under complaint is exceptional.

- That regarding the sending of e-mails with more than one recipient by the rest of the FHP-SSIBE staff, it has been verified that the use of the blind copy option is the usual .

- That on 10/06/2020 the "SSIBE Group Data Governance Policy" was approved and on 10/21/2020 the new "Personal Data Protection Compliance Regulations", which adapted the entity's protocols and clauses to the new regulatory framework for data protection.

- That on 11/16/2020 and 11/17/2020, the FHP-SSIBE carried out an external audit on personal data protection, as part of the active responsibility measures it carries out.

The reported entity attached various documentation to the letter.

5. On 18/10/2021, the director of the Catalan Data Protection Authority agreed to initiate a sanctioning procedure against the Fundació Hospital de Palamós-Serveis de Salut Integrats Baix Empordà for an alleged violation provided for in article 83.5 .a), in relation to 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 10/22/2021.

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

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 08/11/2021, the FHP-SSIBE made objections to the initiation agreement.

The accused entity provided with its writing a copy of the document that certifies that the FHP-SSIBE is an entity that has adhered to the "Type Code for the Protection of Personal Data of the Catalan Union of Hospitals" since 2002, and the copy of the attendance certificate of the worker who sent the controversial email to the "Training in personal data protection and information security", dated 11/08/2021.

8. On 01/02/2022, the person instructing this procedure formulated a resolution proposal, by which it was proposed that the director of the Catalan Data Protection Authority impose on the Fundació Hospital de Palamós-Serveis de Salut Integrats Baix Empordà the penalty consisting of a fine of 1,500.- euros (one thousand five hundred 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 04/02/2022 and a period of 10 days was granted to formulate allegations.

9. On 08/02/2022, the accused entity paid in advance 900.- euros (nine hundred euros), corresponding to the payment of the monetary penalty that the investigating person proposed in the resolution proposal, once applied cumulatively the two reduction options provided for in article 85 of Law 39/2015.

10. On 02/16/2022, the accused entity submitted a letter in which it acknowledges its responsibility for the alleged acts and communicates the voluntary advanced payment of the pecuniary penalty, once the two corresponding reductions have been applied cumulatively.

proven facts

On (...)/2020, a Covid Manager from the FHP-SSIBE sent an email message to 14 recipients in relation to the PCR test that their sons and daughters (users of a center of (...).

This e-mail message was sent without using the Bcc tool or option, which resulted in all recipients of this e-mail having access to the e-mail address of others in the who the message was addressed to and that they knew the information regarding their sons or daughters having to undergo a PCR test.

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

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 by virtue of article 3.f) of Law 32/2010, to the extent that the FHP-SSIBE is an entity belonging to the comprehensive public utilization system of Catalonia-SISCAT- (Decree 196/2010), and in this sense, provides public health services in concert with the Catalan Health Service.

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 properly allegations in the resolution proposal, since the letter presented is a statement in which it acknowledges responsibility for the alleged facts and, in relation to this, informs that it has already proceeded to the voluntary advanced payment of the amount of the resulting penalty , once the percentage of deduction corresponding to the cumulative application of the two reduction options provided for in article 85.3 of the LPAC has been applied. However, it is considered appropriate to reiterate below the most relevant of the reasoned response that the instructing person gave to the allegations before the initiation agreement.

As a premise, it should be pointed out that the entity invoked its status as an entity adhering, since 2002, to the "Unió Catalana d'Hospitals Standard Code for the Protection of Personal Data". From here, the allegations made against the initiation agreement 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 agreement d 'initiation, but refer, in general terms, to the response that the entity gave to this Authority's request in the prior information phase, and they focus, mainly, on exposing the corrective measures implemented in order to 'to prevent events similar to those proven to be repeated, as well as to alleviate the damages that may have been caused.

In this regard, the entity states that, as a specific measure, specific training on the use of the "Zimbra" application (the entity's e-mail system) has been included in the employee's training itinerary) and on personal data protection and information security. Also, the entity has carried out a risk analysis which resulted in the need to implement security measures such as equipping its managers with Covid

of the application to make encrypted shipments, and reinforce their training in the matter of processing personal data. It also explains that it has ordered the preparation of a proposal to modify the document "Compliance regulations regarding the protection of personal data of the SSIBE group" which includes the possibility of submitting to alternative conflict resolution mechanisms in the event of disputes with the entity's users. Finally, he informs that he has contacted the complainant here to apologize for the events reported, and that he plans to send him a second message to inform him about the changes implemented in the processing of data by of the COVID Managers and on the outcome of the present disciplinary proceedings, as well as, to regret the damage that may have been caused and to thank him for his contribution to the improvement of the system.

In the proposed resolution, this Authority positively assesses the measures adopted by the entity, which make it easier for Covid managers to expand their training in the field of data processing, and in particular, in the appropriate use of email, but points out that the adoption of the different measures does not distort the alleged facts nor its legal qualification.

On the other hand, given that the entity refers in general terms to the response it gave to this Authority's request for information, in which it concluded that the cause of the controversial sending of the email had been "a human error " of the worker who sent it, in the proposed resolution it should be noted that this Authority has recalled in several resolutions (for all, the resolution of sanctioning procedure no.
PS 52/2012, also cited by the entity in its pleadings) the jurisprudential doctrine on the principle of guilt, both of the Supreme Court and of the Constitutional Court. According to this doctrine, the sanctioning power of the Administration, as a manifestation of the "ius puniendi" of the State, is governed by the principles of criminal law, and one of its principles is that of guilt, incompatible with a regime of objective responsibility without fault. In this sense, the Supreme Court in several rulings, including those of 15/04/2016 and 24/11/2011, refers to the doctrine of the Constitutional Court when it quotes verbatim "objective responsibility does not fit in the scope of administrative sanctions or without fault, doctrine that is reaffirmed in sentence 164/2005, of June 20, 2005, under which the possibility of imposing sanctions for the mere result is excluded, without proving a minimum of culpability, even for mere negligence ". In this sense, he considers that in order to attribute responsibility for the offenses committed to the author, the element of fault must be present, which includes actions or omissions committed due to "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. At this point 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 the protection of personal data. Certainly, in the present case, the sending of the disputed e-mail without using the blind copy option, entailed data processing that

breached 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 other recipients, and, at the same time, to know information relating to their sons or daughters they had to undergo a PCR test.

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 provides that personal data will be "treated in such a way as to guarantee adequate security of personal data, including the protection against unauthorized or illegal treatment and against its loss, destruction or accidental damage, through the application of appropriate technical or organizational measures".

For its part, article 5 of Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (hereinafter LOPDGDD) regulates the duty of confidentiality in the following terms:

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

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 "principles treatment basics, including the conditions for consent pursuant to articles 5, 6, 7 and 9", which includes the principle of integrity and confidentiality (art. 5.1.f 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 in article 5 of this Organic Law."

4. As FHP-SSIBE is a private law entity, the general penalty regime provided for in article 83 of the RGPD 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,

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

of an amount equivalent to a maximum of 4% 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 instructing person 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, given that it is considered that the 'entity, located in the health care sector, must know and take care to properly manage the processing of personal data in all its areas of action.

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 1,500 euros (one thousand five hundred euros). This quantification of the fine is based on the weighting between the aggravating and mitigating criteria indicated below.

As mitigating criteria, the concurrence of the following causes is observed:

- The nature, gravity and duration of the infringement, taking into account the nature and scope of the treatment and the number of those affected and the level of damages caused (art.83.2.a RGPD).
- The lack of intentionality (art. 83.2.b RGPD) .
- The measures taken by the person in charge of the treatment in order to alleviate any damages suffered by the interested parties, given that he proactively addressed the complainant here to apologize for sending the mail, as well as the commitment taken to send you a new email with the terms set out in the legal basis 2on (art. 83.2.c RGPD).

- The lack of violations previously committed by the FHP-SSIBE (art. 83.2.e RGPD).
- The category of personal data affected by the breach - there is no evidence that it affected special categories of data, as the text of the email message only informed the families about the documentation they had to deliver on the day of the PCR test – (art. 83.2.g RGPD).

- The entity's adherence to the Union's "Type Code for the protection of personal data Catalana d'Hospitals" since 2002 (art.83.2.j RGPD).
- The lack of benefits as a result of the commission of the offense (art. 83.2.k RGPD and 76.2.c LOPDGDD).
- The measures adopted by the entity in order to prevent events such as those proven here from being repeated, as well as the order to modify the document "Compliance regulations regarding the protection of personal data of the SSIBE group" to include the possibility for the entity to submit to mechanisms for alternative resolution of conflicts in the

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

cases of disputes with users of the entity (art.83.2.k RGPD and 76.2.h LOPDGDD).

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

- Linking the offender's activity with the practice of data processing personal data (art. 83.2.k RGPD and 76.2.b 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, by means of a letter dated 02/16/2022, the accused entity has acknowledged its responsibility. Likewise, on 08/02/2022 he had already paid 900 euros (nine 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.

In the present case, however, it becomes unnecessary to require corrective measures for the effects of the infringement given that, on the one hand, the infringing conduct refers to a single and already accomplished fact, the sending of an email, which by its instantaneous nature cannot be corrected by the application of corrective measures, and, on the other hand, the fact that the entity has adopted different measures in order to improve the training of Covid managers in the proper use of email, and to avoid so that in the future events similar to those tried here are repeated

For all this, I resolve:

1. To impose on the Fundació Hospital de Palamós-Serveis de Salut Integrats Baix Empordà the sanction consisting of a fine of 1,500.- euros (one thousand five hundred euros), as responsible for an infringement provided for in article 83.5.a) in relation to article 5.1.f), both of the RGPD.

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

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 Hospital de Palamós-Baix Empordà Integrated Health Services Foundation has made effective the advanced payment of 900 euros (nine hundred euros), which corresponds to the total amount of the penalty imposed, after applying the 40% deduction percentage corresponding to the reductions provided for in article 85 of the LPAC.

3. Notify this resolution to the Hospital de Palamós-Baix Empordà Integrated Health Services Foundation.

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 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,