File identification

Resolution of sanctioning procedure no. PS 60/2022, referring to Vic City Council.

Background

1. On 12/08/2021, the Catalan Data Protection Authority received two letters in which two people made separate complaints against the City Council of Vic, on the grounds of an alleged breach of the regulations on data protection personal data

The two complainants agreed to state the same facts, given that when the reported facts occurred, one was acting on behalf of the other. Specifically, the complainants stated that one of them, in his functions as (...) of Vic City Council, and acting on behalf of 36 employees of the entity (among them, the other person here complainant) presented, on August 7, 10 and 11, 2021, a total of 36 optional appeals against the Agreement approving the List of Workplaces (RLT) of the City Council of Vic, on behalf of all the people he represented and also on his own behalf.

In relation to this, the complainants stated that on 10/08/2021, the City Council sent an email to all the employees of this City Council, informing them that they could consult the administrative file corresponding to the RLT (reference (...)) through a certain link. In this regard, the two complainants complained that once the electronic file was accessed, they had access to all appeals filed against the RLT without anonymizing the personal data. In this way, the personal data of the workers (name and surname, ID, telephone number and address) who had filed a replacement appeal, either in their own name or through a representative, were made available to the rest of the organization's workers who were sent the controversial email dated 08/10/2021.

The two complainants provided a copy of the email sent by the City Council on 08/10/2021. Also, a screenshot was attached of the different steps to follow, starting from the link, which finally allowed access to the content of the file with the different replenishment resources interposed.

2. On 24/09/2021 and 03/10/2021, the Authority received three more letters submitted by City Council workers, who made individual complaints against Vic City Council for the same facts that had been reported in date 08/12/2021.

3. The Authority initiated investigative actions (prior information phase) in relation to the five complaints presented, 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.

4. Within the framework of these information phases, on the dates 07/02/2022 and 09/05/2022, two requests for information were made to the reported entity about the reported facts. In these requirements, the entity was required to report, among others, on who were the recipients of the controversial email dated 08/10/2021, and on which personal data of the

workers was included in the resources of replacement incorporated into the electronic file. Also, to report on whether the workers who received the mail could only access the written appeal (that is, their own personal data), or whether they also had access to the other written appeals filed by the rest of workers. In the last one, it was also required if access to the file was still accessible through the link indicated in the email dated 08/10/2021.

5. The entity responded to the aforementioned request through a letter in which it acknowledged the " *error* ", and in which it stated, among others, the following:

- That *"The total number of employees who were notified and who were able to access the replacement resources presented were 238 employees who formed and appeared in the RLT.* "

- That " *this access to replenishment resources was possible between the period between 08/10/2021 and 08/12/2021. This access was deleted the moment the City Council realized the error and quickly asked the (...) the OAC not to associate the resources with the file relating to RLT .*"

The reported entity attached various documentation to the letter, specifically, the following:

- Copy of the Agreement of the Municipal Plenum, dated 07/12/2021, by which the List of Workplaces of Vic City Council and the Autonomous Organization of Fairs and Markets (OFIM) is approved, and copy of the publication of said RLT in the BOPB dated 07/23/2021.

- Copy of the report issued by the Human Resources unit of the City Council, dated 07/07/2022, on the events reported.

  In said report, the facts reported and the causes that allowed all the workers of the entity, to whom the email of 08/10/2021 was sent (238 people), had the possibility, between 08/10/2021 and 08/12/2021, to access the personal data included in the different appeals filed against the RLT:

  " From August 10, it was decided to create a new file where all the resources ((...)) are grouped due to the enormous amount of documents uploaded in the first file and which did not facilitate the processing of the notifications, incidents, or the concealment of documents.
  (...)
  On 12/08/2021, it is known that the resources are being associated with the first file (a reference that must be understood to be made in the file *(...)) and that their display is not being hidden, reason for which an e-mail is sent to the (...) the OAC.*
  (...)
  It is during this period between 10-08-2021 and 12-08-2021 (date on which notice is given that no more resources will be associated with the file from the Citizen Service Office (...)), that workers can view files that have not been hidden.

  On 04/07/2022, based on the report required by the Catalan Data Protection Authority, the IT department of Vic City Council is required to carry out a comprehensive audit of the 46 documents likely to have been viewed.
  (...)"

6. On 09/22/2022, also during this preliminary information phase, the Authority's Inspection Area found that Vic City Council had not notified the security breach linked to the events reported here.

7. On 09/09/2022, the director of the Catalan Data Protection Authority agreed to initiate disciplinary proceedings against Vic City Council for two alleged infringements: an infringement provided for in article 83.5.a) in relation to article 5.1.f); and another violation provided for in article 83.4.a) in relation to article 33, all of them of Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, relating to the protection of natural persons with regard to the processing of personal data and the free movement thereof (hereafter, RGPD). This initiation agreement was notified to the imputed entity on 10/03/2022.

8. 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.

9. On 07/10/2022, the City Council made objections to the initiation agreement.

10. On 16/12/2022, the person instructing this procedure formulated a resolution proposal, for which he proposed that the director of the Catalan Data Protection Authority admonish Vic City Council as responsible , in the first place, of an infringement provided for in article 83.5.a) in relation to article 5.1.f); and secondly, of an infringement provided for in article 83.4.a) in relation to article 33, all of them of the RGPD.

This resolution proposal was notified on 19/12/2022 and a period of 10 days was granted to formulate allegations.

11. The deadline has passed and no objections have been submitted.

proven facts

1. The City Council of Vic, between 10/08/2021 and 12/08/2021, made available to all employees listed in the RLT of the entity (a total of 238 workers) , access to the personal data of the municipal workers who had lodged an appeal against the RLT approval agreement (name and surname, ID, telephone and address).

The City Council made available to municipal employees access to said personal data, by sending an email dated 08/10/2021, in which they were informed of the link to access in the electronic file relating to the RLT's Approval Agreement, which contained all the appeals lodged, without anonymisation.

2. Vic City Council did not notify the Authority of the security breach of personal data, despite the fact that it became aware of the above facts on 08/12/2021, the date on which it sent an email to Citizen Service Office (OAC) - input channel for replacement resources -, to warn of the facts and request that no more resources be associated with the RLT's electronic file, since they had given permission to view the said file to City Hall workers.

Fundamentals of law

1. The provisions of the LPAC , and article 15 of Decree 278/1993, according to the provisions of DT 2a of Law 32/2010, of October 1, of Catalan Data Protection Authority. In accordance with articles 5 and 8 of Law 32/2010, the resolution of the sanctioning procedure corresponds to the director of the Catalan Data Protection Authority.

2. 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.

First of all, it should be noted that the allegations that the accused entity made before the initiation agreement did not question any of the facts imputed in the present sanctioning procedure.

Indeed, in its letter, the City Council limited itself to reiterating, briefly, that some of the circumstances that were already set out in the report issued by the City Council's Human Resources unit on the facts reported, which was provided as part of the previous information. Specifically, that the entity has registered that there were few people who accessed the file relating to the RLT Approval Agreement - which contained all the replacement resources that had been filed -, and that access was only given to six written appeals for replacement of the total that were filed. Also, in the statement of objections, the diligence with which it was acted is made, since the access was only operational for two days, from 08/10/2021 to 08/12/2021 .

Well, as already indicated in the resolution proposal, it must be highlighted that neither the fact that the effective accesses were reduced - both by the number of people who accessed the file, and by the number of written recourse to which they accessed -, as well as the quick action of the City Council, when it became aware of this breach of the confidentiality principle, to avoid the possibility that improper access could continue, allow to distort the imputed facts, which have have been fully accredited, nor their legal qualification. It is for this reason that said allegations must be dismissed.

3. In relation to the facts described in the first point of the proven facts section, 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 confidentiality provided for by the RGPD must be supplemented with the duty of secrecy contained in Article 5 of Organic Law 3/2018, of December 5, on the protection of personal data and the 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 person in charge of the treatment has ended .

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 point 1 of the proved facts section, which is considered constitutive of the violation provided for in article 83.5.a) of the RGPD, which typifies the violation of the *"basic principles of treatment, including the conditions for consent pursuant to articles 5, 6, 7 and 9 "* , which include the principle of 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 by article 5 of this Organic Law."*

4. With regard to the fact described in point 2 of the proven facts section, it is necessary to go to article 33 of the RGPD, which provides that " *In case of violation of the security of personal data, the person responsible for the treatment will notify the competent control authority in accordance with article 55 without undue delay and, if possible, no later than 72 hours after he has had evidence of it, unless it is unlikely that said breach of security constitutes a risk for the rights and freedoms of individuals. If the notification to the control authority does not take place within 72 hours, it must be accompanied by an indication of the reasons for the delay."*

In accordance with what has been explained, the fact recorded in point 2 of the section on proven facts constitutes the violation provided for in article 83.4.a) of the RGPD, which typifies as such, the violation of *" the obligations of the person in charge and the person in charge pursuant to articles 8, 11, 25 to 39, 42 and 43 ;"*

In turn, this conduct has been included as a serious infraction in article 73.r) of the LOPDGDD, in the following form: *"r) Failure to comply with the duty to notify the data protection authority of "a security breach of personal data in accordance with the provisions of article 33 of Regulation (EU) 2016/679."*

5. Article 77.2 LOPDGDD provides that, in the case of infractions committed by those in charge or in charge listed in art. 77.1 LOPDGDD, the competent data protection authority:

> *"(...) must issue a resolution that sanctions them with a warning. The resolution must also establish the measures to be adopted so that the conduct ceases or the effects of the offense committed are corrected.*

The resolution must be notified to the person in charge or in charge of the treatment, to the body to which it depends hierarchically, if applicable, and to those affected who have the status of interested party, if applicable."

In terms similar to the LOPDGDD, article 21.2 of Law 32/2010 , determines the following:

"2. In the case of violations committed in relation to publicly owned files, the director of the Catalan Data Protection Authority must issue a resolution declaring the violation and establishing the measures to be taken to correct its effects . In addition, it can propose, where appropriate, the initiation of disciplinary actions in accordance with what is established by current legislation on the disciplinary regime for personnel in the service of public administrations. This resolution must be notified to the person responsible for the file or the treatment, to the person in charge of the treatment, if applicable, to the body to which they depend and to the affected persons, if any".

In the present case, however, security measures should not be required to correct the effects of the imputed infringements, given that these derive from facts already accomplished, which by their nature cannot be corrected with the implementation of corrective measures.

For all this, I resolve:

1. Admonish Vic City Council as responsible for two infringements: an infringement provided for in article 83.5.a) in relation to article 5.1.f); another violation provided for in article 83.4.a) in relation to article 33, all of them 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 Vic City Council.

3. Communicate the resolution to the Ombudsman, in accordance with the provisions of article 77.5 of the LOPDGDD.

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,