Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

File identification

Resolution of sanctioning procedure no. PS 5/2022, referring to Torredembarra City Council

Background

1. 05/25/2020 , the Catalan Data Protection Authority received two letters from a person who filed two complaints against the Torredembarra City Council for alleged non-compliance with the regulations on personal data protection .

In the first letter of complaint, the complainant stated that he was part of the municipal police force of Torredembarra City Council, which would have allowed him to access the computer server of the local Police. On this, he complained that on said server, there was a computer file relating to a complaint made by the complainant himself in the year (...) to the Mossos d'Esquadra, which contained his personal data. Said computer file had the title " *(...)* ", and was stored in the following path " *(...)* " . The complainant added that all local police officers and personnel (...) could access said document through the route referred to. Finally, he formulated several questions relating to the treatment of said file: " *how has dicho documento been accessed, who has facilitated it, who proceeded to its scan, what was done with said document, to whom it was transmitted or what type of treatment I tell him."*

The second letter of complaint referred to an email sent by (...) of the local Police to different email addresses of people who make up the local Police and staff of the Torredembarra City Council. In said e-mail, you were informed of the judicial proceedings opened before a court of inquiry, relating to a complaint filed by the person here making the complaint against said (...).

The complainant provided various documentation.

2. The Authority opened a preliminary information phase corresponding to each complaint (no. IP 144/2020 and no. IP 145/2020), in accordance with what is provided for in article 7 of Decree 278/1993, of 9 of November, on the sanctioning procedure applied to the areas of competence of the Generalitat, and article 55.2 of Law 39/2015, of 1 October, on the common administrative procedure of public administrations (from now on , LPAC), to determine if the facts were likely to motivate the initiation of a disciplinary procedure.

3. On 09/01/2020, as part of the preliminary information phase no. IP 144/2020 an information request was made to the reported entity, in which it was required to report on whether in the computer server of the Local Police of the City Council, it was or had been found stored in the folder (...)", a scanned copy on 27/02/2020, of the complaint that the person making the complaint here made to the Mossos d'Esquadra on 12/01/(...). It was also required to report on the legal basis that would legitimize the storage on the server of the local police of said complaint, as well as the people who would have had access to it, and the jobs they hold within the organization . Finally, he was

required to report through which channel the Local Police of the City Council would have accessed the controversial complaint document.

4. On 09/25/2020, Torredembarra City Council responded to the request through a letter in which, among others, it stated the following:

- That " IT IS *COMPLETELY FALSE: NO POLICE OFFICIAL OR (...) can access the server (only the administrator who is the (...) of Torredembarra City Council can do it), users have selective privileges of 'access/permissions restricted to certain folders by user groups but NEVER ON THE SERVER."*

- That *"In consultation with the (...) of Torredembarra City Council, last September 7, 2020, it states that this document IS NOT STORED in the indicated location."*

- That the document with the title " *(...)* " was filed in " *a scan junk folder and periodically delete its contents."*

- That " *YES a document existed on February 27, 2020, scanned at 10:47 a.m."* and that " *was possibly deleted in June/July 2020 together with the contents of the rest of the documents as the technical services usually and periodically do computers".*

- Which **"** *IS COMPLETELY FALSE that the statement/complaint: "all local and personal police officers (...) can access said document through the route referred to",* and that " *ONLY the folder (...) can be accessed electronically and with prior access key of the user/session to the terminal PREFECTURE ((...)) and (...) attached to the same from the OFFICE OF (...)((...)), together with the IT administrator ((...)Torredembarra City Council). However, it is a junk document scan folder without storage since the IT services (administrator) of the city council periodically cleans this computer folder .*"

- That *"Questioned to the officials mentioned in which I include myself* - reference that must be understood made to the person signing the report, the (...) of the local police - *about the scan, existence of the document or of any incidence related to it, ALL of them (except the (...)) state that they DO NOT REMEMBER OR ACKNOWLEDGE HAVING SCANNED THE DOCUMENT IN QUESTION. What's more, it is a folder not used by the Prefecture and of which it has been a surprise for us that this document exists in it .***"**

- That " *he himself contributed this IDENTICAL document to the file at the courthouse transferring a copy of it to the attorney/s of the Torredembarra City Council for the defense of its officials, councilors and mayor who were reported . The temporality of the existence of the document since the year (...), the disposition of it by the parties involved, and the current reference to February 27, 2020, is completely incomprehensible."*

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

- That *"it is very surprising the appearance of this document in this folder of little or no frequent use, which can be scanned by anyone who works at the Local Police facilities, being that the code of the printers/ (...) is the same for all "(...)" personnel, and can only be consulted by the Prefecture and the deputy of the Office of (...)Mr. (...), a circumstance that can even come to presuppose and suspect that it could have presumably been introduced by the complainant himself or by a person collaborating with him, presumably with the intention of instrumentalizing or manipulating the various procedures that drive the own (...)".*

- That the document with the title " *(...)* " contains a *"DECLARATION ACT".*

- That the complainant makes " *a continuous use and instrumentalization of judicial bodies, institutions and public bodies in a clear and fraudulent manner by constantly filing complaints in Local Administration, Courts, Anti-Fraud Office and now the Catalan Data Protection Authority* ". The entity lists the total number of files (9) currently being processed that originate from complaints/lawsuits by the person making the complaint against the City Council.

The reported entity attached various documents to the letter, among others, the " *List of shared folders (...)* ", which includes the different "user groups" of the City Council and the "summary of accesses and permissions" to those who have access. There it was stated that only the members of the Prefecture ((...)) have permission to access the " *(...) " folder* and Mr. (...).

5. On 09/29/2020, as part of the preliminary information phase no. IP 145/2020, the Authority made a request to the City Council, which was answered by the entity on 19/11/2020.

6. On 14/01/2021 , the City Council presented documentation relating to the various judicial proceedings arising from the demands presented by the complainant here, dealing with the majority of court decisions favorable to the City Council.

7. On 14/07/2021, the Director of the Catalan Data Protection Authority issued a resolution by which she archived the actions of prior information no. IP 144/2020 and no. IP 145/2020. This resolution was notified on 07/15/2021 to the data protection delegate of Torredembarra City Council and to the complainant.

8. On 08/12/2021, the complainant filed an appeal against the file resolution of 07/14/2021.

9. On 08/13/2021 , this appeal was transferred to the data protection delegate of the Torredembarra City Council so that, within ten days, he could formulate the allegations he considered relevant without, after this term, presented any allegation in this regard.

10. On 01/10/2021, the Director of the Catalan Data Protection Authority issued a resolution partially upholding the appeal filed against the Resolution of 07/14/2022, in the sense of leaving without effect the archive of file IP 144/2020 and reopen it in order to collect more information that would allow to determine the origin or not to initiate a sanctioning procedure regarding the facts linked to

whether the City Council had a measure that would guarantee the traceability of the system in relation to the documentation contained in the digital folder "(...)", and dismiss the appeal with regard to the file of the IP 145/2020 file.

11 . On 03/12/2021, as part of the reopening of the preliminary information phase no. IP 144/2020, the Authority made a request to the City Council to report on whether the City Council, on the date of the events reported (25/05/2021), had a system in place to guarantee the traceability of the system. In other words, a system that would make it possible to know which specific users had accessed the information contained in the digital folder "(...)", and specifically in the document "(...)", at what time, and which actions they had taken.

12. On 01/24/2022, Torredembarra City Council responded to the request through a letter in which, among others, it stated the following:

- That " *At the time of the events, there was no system that would allow us to know which specific users had accessed the information contained in the digital folder "(...)", and specifically in the document "(...)", nor at what time, and what actions they would have taken."*
- That " *Access to this folder is organized by access privileges and limited to users who selectively have access privileges/permissions restricted to certain folders:*
  - (...) of the Local Police of the town hall of Torredembarra
  - (...) attached to the same from the OFFICE OF (...)
  - Computer administrator ((...)Torredembarra City Council)."

13. On 08/02/2022, the director of the Catalan Data Protection Authority agreed to initiate disciplinary proceedings against Torredembarra City Council for an alleged violation provided for in article 83.4.a) in relation to the Article 32; 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). Likewise, he appointed Mrs. (...), an employee of the Catalan Data Protection Authority, as the person instructing the file . This initiation agreement was notified to the imputed entity on 08/02/2022.

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.

The deadline has been exceeded and no objections have been submitted.

proven facts

Torredembarra City Council, for an indeterminate period of time but, at least, in the period between 02/27/2020 and 05/25/2020, did not have an information system that allowed to guarantee the traceability of the actions he carried out in relation to the information contained in the digital folder

"(...)". This fact meant that it was not possible to verify, in relation to the document "(...)" stored in the aforementioned digital folder and which contained personal data of the complainant here, which users had accessed it, at what time, and what actions they had taken.

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. In accordance with article 64.2.f) of the LPAC and in accordance with what is indicated in the agreement initiating this procedure, this resolution should be issued without a previous resolution proposal, given that the accused entity has not made allegations in the initiation agreement. This agreement contained a precise statement of the imputed liability.

3. In relation to the facts described in the proven facts section, it is necessary to refer 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 guarantees an adequate security of personal data, including protection against unauthorized or illegal treatment and against accidental loss, destruction or damage, through the application of appropriate technical or organizational measures".*

For its part, article 32 of the RGPD, regarding data security, provides the following:

> *"1. Taking into account the state of the art, the costs of application, and the nature, scope, context and purposes of the treatment, as well as risks of variable probability and severity for the rights and freedoms of natural persons, the person responsible and the person in charge of the treatment will apply appropriate technical and organizational measures to guarantee a level of security adequate to the risk, which if applicable includes, among others:*
> *a) pseudonymization and encryption of personal data;*
> *b) the ability to guarantee the confidentiality, integrity, availability and permanent resilience of the treatment systems and services;*
> *c) the ability to quickly restore availability and access to personal data in the event of a physical or technical incident;*
> *d) a process of regular verification, evaluation and assessment of the effectiveness of the technical and organizational measures to guarantee the security of the treatment.*
>
> *2. When evaluating the adequacy of the level of security, particular consideration will be given to the risks presented by data processing, in particular as a result of the accidental or unlawful destruction, loss or alteration of personal data transmitted,*

stored or otherwise processed, or unauthorized communication or access to said data.

3.(…)

4. The person in charge and the person in charge of treatment will take measures to ensure that any person who acts under the authority of the person in charge or the person in charge and has access to personal data can only process said data following the instructions of the person in charge, unless they are obliged to do so in virtue of the Law of the Union or of the Member States."

In this respect, the first additional provision of the LOPDGDD establishes the following: " *The National Security Scheme must include the measures that must be implemented in the event of processing of personal data to avoid its loss, alteration or unauthorized access, with the adaptation of the criteria for determining the risk in the processing of data to that established in article 32 of Regulation (EU) 2016/679* ".

Well, with respect to the facts that have motivated the initiation of the procedure, it is inferred that the accused entity has violated the security measure provided for in article 23 of the National Security Scheme, a provision that regulates the registration of activity of the users.

Likewise, it should be noted that Law 26/2010, of August 3, on the legal regime and procedure of the public administrations of Catalonia, in its eleventh additional provision, on the management of documentation and archiving of electronic documents, establishes the following: " *5. The information systems used by the public administrations included in the scope of application of this law must guarantee, whenever possible, the authenticity and integrity of their data, and also the traceability of the actions they carry out. "*

Torredembarra City Council, therefore, had to be able to guarantee the security of the personal data for which it is responsible. Regarding this, it should be noted that the RGPD sets up a security system that is based on determining, following a prior risk assessment, which security measures are necessary in each case (recital 83 and article 32). It cannot be denied that these risks exist, and that an analysis of the risks derived from these data treatments must necessarily lead to the conclusion that, considering that the digital folder "(...)" may contain information of a very different nature, which may lead to the categorization of the system as a high category from the point of the required security visa, it would have been necessary to determine and apply the appropriate technical and organizational security measures, such as having a record of the 'user activity that would guarantee the traceability of the system, to prevent these risks from materializing and thus safeguard the right to data protection.

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 83.4.a) of the RGPD, which typifies the violation of *" the obligations of the person in charge and of the person in charge ”* ,

among which is the collection in article 32 of the RGPD transcribed above, referring to the security of the treatment.

The conduct addressed here has been included as a serious infraction in article 73.f) of the LOPDGDD, in the following form:

> *"The lack of adoption of technical and organizational measures that are appropriate to guarantee a level of security adequate to the risk of the treatment, in the terms required by article 32 of Regulation (EU) 2016/679"*

4. 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".*

By virtue of this power, it is necessary to require the Torredembarra City Council to adopt the appropriate technical and organizational security measures, such as having a record of user activity, which allow to guarantee the traceability of the actions carried out in relation to the information contained in the digital folder "(...)".

Once the corrective measure described has been adopted, within the period indicated, the Torredembarra City Council must inform the Authority within the following 10 days, without prejudice to the inspection powers of this Authority to carry out the corresponding checks.

For all this, I resolve:

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

1. Warn the Torredembarra City Council as responsible for an infringement provided for in article 83.4.a) in relation to article 32, both of the RGPD.

2. To require the Torredembarra City Council to adopt the corrective measures indicated in the 4th legal basis and to accredit before this Authority the actions taken to comply with them.

3. Notify this resolution to Torredembarra City Council.

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

5. 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,