File identification

Resolution of sanctioning procedure no. PS 1/2022, referring to Reus City Council.

Background

1. On 10/28/2020, Reus City Council (hereinafter, the City Council) notified the Catalan Data Protection Authority of a data security breach (NVS 67/2020). In this notification it was stated that on 26/10/2020 knowledge was gained, through the notice of a citizen, of the discovery in the debris dump "(...)" of the municipality of Tarragona (deposit of debris and construction), of some plastic bags that contained files from the City Council's social services area (which included data on minors) and documentation from the economic services area (lists of worker productivity and of suppliers), for its destruction.

Likewise, the City Council reported that on the same morning that it became aware of the incident, it sent an authorized unit to the debris deposit in order to collect the information and return it to the municipal departments, and that the cause that would have led to its appearance in the debris dump, instead of being destroyed in accordance with the safe circuit of the City Council, reason for which an internal investigation had been initiated, in order to determine the circumstances and also if "third companies" would have intervened in the security breach suffered.

2 . As a result of this security breach notification, the Authority opened a preliminary information phase (no. IP 362/2020), in accordance with the provisions of article 7 of Decree 278/1993, of 9 November, on the sanctioning procedure applied to 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 (henceforth, LPAC), to determine if the facts were likely to motivate the initiation of a sanctioning procedure, specifically, in relation to the appropriate technical and organizational measures in order to guarantee a level of security adequate to the risk (art. 32 of RGPD) in the management of the documentation destined for its destruction, the identification of the person or persons who could be responsible and the relevant circumstances that occurred.

A copy of the actions carried out as part of the notification of said security breach (NVS 67/2020) will be incorporated into this previous information. Also incorporated are the screenshots of the news about the incident published in different digital media, and the video recorded by the citizen who found the municipal files in the debris dump, and which was published by the newspaper of Tarragona, in its digital version, on 02/11/2020.

3 . As part of this information phase, on 15/01/2021 Reus City Council was required to report on the following:

- of the result of the internal investigation into the incident that happened.
- of the protocol implemented by the City Council for the management of documentation in paper format destined for its destruction and its circulation, including the documentation found in the landfill, and whether as a result of the security incident suffered reviewed and updated said protocol/circuit.

4. On 28/01/2021, the City Council responded to the previous request, through a letter in which it set out, among others, the following:

- That with regard to the results of the internal and reserved investigation carried out by the council immediately, once it became aware of the appearance of municipal files in the debris deposit, a copy of the report of the same date is provided 01/28/2021 prepared by the City Council's security officer ("Executive report on the internal investigation resulting from the security breach detected following the discovery of files and municipal documentation at the debris and controlled waste depot of the (. ..)").

- In the conclusions section of said report, the following is stated:

" In light of the proven facts, the open investigation concludes the following:

FIRST.- Loss of control and breakdown of procedures within the organization.

a. In relation to the social services files, the cause that originates the loss of control over the information is specified at the moment when the order is given, via telephone, that the documentation must be destroyed, taking care of this task the unit of brigades and without starting the procedure of "document transfers" to transfer the documentation to the Municipal Archives to be destroyed later by an authorized certifying entity that certifies that the destruction is in accordance with the regulations in data protection matter.

b. In relation to the economic services files, the cause that originates the loss of control over the information is specified at the moment when it is decided to transport this documentation to the brigade unit, through the logistics services, so that it is destroyed, and without start the procedure of "document transfers" to transfer the documentation to the Municipal Archives to be destroyed later by an authorized certifying body that certifies that the destruction is in accordance with the regulations on data protection.

c. In both cases, and after interviewing the people involved, there is a lack of knowledge of the protocols and procedures to be followed on the part of the people belonging to the units and departments, whose documentation is the object of the transfer, since the "document transfers" procedure is not activated through the applicable Municipal Archive within the organization and which ensures the correct transfer and disposal.

d. That in conclusions a) and b) the origin of the cause of the whole incident is detected, which includes part of the documentation that is in the municipal brigades in the deposit of (...), although it cannot be determined with certainty the reason that explains its appearance in this place.

e That the destruction of documentation in the municipal brigades' offices and the personnel in charge of doing so show that this unit does not have the optimal security conditions or an adequate control to guarantee that the destruction is done safely , in addition to not being the unit in charge of making this type of removals, which are done through the Municipal Archive, by the procedure mentioned in the previous letters.

SECOND.- Appearance of the documents in the controlled deposit of (...).

a. The only connection between the files found (located in the municipal brigades) and the landfill of (...) is the subcontracted company that collects the debris and dumps it in different landfills, among which is the one of (.. .). Therefore, it can be seen that the loss of control of the documentation occurs since the documentation is located in the municipal brigades unit and through a procedure that lacks sufficient and appropriate guarantees.

b. The place where the documentation is located (landfill) is not an easily accessible space, separated from the urban center of the city of Tarragona, being an area authorized by waste transport companies, which is why the data leak is considered very remote, except for the person making the complaint, and there is no evidence that he went further, having checked with the affected departments that the recovered documentation is the one found in the landfill.

c. It has not been possible to accredit or appreciate the intention of any employee that involves bad faith, or grief with the purpose of causing reputational or financial damage to the City Council. Nor has it been possible to specifically identify a subject or group of people as directly and immediately responsible for the events that occurred, but rather they are the result of a chain of ignorance and errors throughout the entire procedure of transfer and elimination of the documentation

THIRD.- Recommendations.

a. The brigades must not destroy administrative documentation since the facilities are not suitable for these tasks nor are their personnel trained to do so with the appropriate security conditions.

b. The action protocols must be reviewed and, especially, those relating to the transfer and destruction of paper documentation, and new ones must be created that clearly define the guidelines and procedures to be followed and those responsible of transfers and elimination.

c. It must be ensured that the removal of the documentation is done through a company and a container service that guarantees a service of certified and confidential destruction of administrative data.

d. The new protocols must be disseminated and trained to employees and their compliance must be guaranteed."

-A copy of the new protocol drawn up by the City Council, and approved by Decree dated 01/28/2021 "Protocol for the treatment and destruction of non-automated media that contain personal data of which the Reus City Council is responsible" and " *which includes the procedure and circuit to be followed with regard to the treatment, conservation and subsequent destruction of non-automated media that have personal data. This circuit includes from when the City Council begins to process documentation with personal data until its subsequent destruction and elimination." (...)* " *Having been approved by the relevant body of the Entity, the Protocol will be made available to employees for their knowledge and practical application."*

5. On 10/01/2022, the director of the Catalan Data Protection Authority agreed to initiate a disciplinary procedure against the Reus City Council for an alleged violation provided for in article 83.4.a), in relation to article 32; both 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 (hereinafter, RGPD). This initiation agreement was notified to the imputed entity on 01/11/2022.

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 01/25/2022, the City Council made objections to the initiation agreement . Along with his statement of objections, he provided various documentation in order to justify his claims, and also asked that the documents provided in NVS 67/2020 and in the information phase prior to the present procedure be reproduced. which, according to what was reported, were already included in the present procedure.

8. On 03/28/2022, the person instructing this procedure formulated a resolution proposal, by which he proposed that the director of the Catalan Data Protection Authority admonish Reus City Council as responsible for 'an infringement provided for in article 83.4.a) in relation to article 32, both of the RGPD.

This resolution proposal was notified on the same day 28/03/2022 to Reus City Council and a period of 10 days was granted to formulate allegations.

9. The accused entity presented a statement of objections to the resolution proposal.

proven facts

On 10/25/2020, a citizen found in the debris deposit "(...)", of the municipality of Tarragona, several plastic bags containing documentation with personal data relating to files of the Social Services Area of the City Council (which included data on minors), of the citizens served by the Welfare Area in District V between 2012 and 2015, and of the Economic Services Area (lists of productivity of workers and suppliers), that were destined to be destroyed.

All this documentation with personal data was transferred, at the request of council staff, to the facilities of the Brigades Unit of the City Council, for their destruction, and deposited in the space where the industrial machine for paper destruction, area without any perimeter fence, a few meters from the debris containers, which led to external companies moving them to the "(...)" landfill, so that unauthorized third parties they would have had access to the information contained therein.

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. Reus City Council has made objections to both the initiation agreement and the proposed resolution. In the statement of objections to the proposal, the entity will reiterate those already formulated before the initiation agreement. That is why, although said allegations were already analyzed in the proposed resolution, they are reproduced here.

2.1. About the measures previously adopted.

The accused entity asserts that the City Council had, at the time of the events, appropriate technical and organizational measures in the terms of article 32 of the RGPD, known to all staff, for the transfer and secure destruction of documentation with personal data, although these, due to an internal human error of the intervening units, were not applied correctly.

He adds that, for this purpose, the City Council had two internal documents, which were available to staff on the Intranet, and which regulated the processes of transfer and destruction of documentation, specifically, the " *internal procedure document of transfer* " and the " *internal office management archive document* ", which were provided during the previous information phase, and evidenced the existence of security measures for the destruction of the documentation.

And that, " *in addition to the procedures indicated in said documents, the City Council applied certain standardized processes relating to the processing of data in a non-automated format, although these were not documented* ".

Regarding these allegations, as indicated by the instructor, the first thing to note is that neither of the two internal documents referred to by the accused entity establish a procedure or circuit to be followed for the safe destruction of the paper documentation with personal data (that is, from the moment it is decided that the documentation must be destroyed, until its final destruction) but what they establish is, in the case of the " *internal document of the procedure of transfer* ", the guidelines that the different administrative units must follow to transfer the administrative documentation of more than five years to the Municipal Archives (how to organize and prepare said documentation), so that said body n assume its custody and decide its fate after a document evaluation process, without making any reference to the destruction process, and in the case of the " *internal office management archive document* ", explain what the documents are and are part of an administrative file that can be deleted in the administrative units themselves, although it also does not include any indication of the process that must be followed for the destruction of said information.

Having said that, article 5.1.f) of the RGPD establishes that personal data will be *" treated in such a way as to guarantee a security data adequacy _ personal , including the protection against unauthorized or illegal treatment and against it loss , destruction or accidental damage , through the application of measures technical or organizational appropriate (" integrity and confidentiality ")."*

In turn, article 32.1 RGPD provides that *"the person responsible and the person in charge of the treatment they will apply measures technical and organizational appropriate to guarantee a level of security adequate to the risk (...)"* .

What Article 32.1 RGPD requires is that the security measures, which must be determined taking into account the risks arising from the loss or unauthorized access to the data (among others), are adequate.

Well, in the specific case that concerns us, it has become clear that the City Council did not have the appropriate technical and organizational measures implemented in order to guarantee a level of security appropriate to the risk in the management of the paper documentation intended for its destruction, and this has been evidenced by the reality of the proven facts, not contradicted by the City Council, which lead to the conclusion that the security of the data was not effectively guaranteed in the procedure of destruction of the

paper documentation , and in particular its proper custody to prevent access by unauthorized third parties.

In fact, the security of the data was compromised, as the City Council itself recognizes in its conclusions reproduced in this resolution (background 4), from the moment when the staff did not know what the procedure to follow for the destruction was secure documentation with personal data, and that the destruction was carried out through a " *procedure lacking sufficient and adequate guarantees* ", which led to the documentation being deposited in an area that " *did not have the security conditions adequate nor of an adequate control to guarantee that the destruction is done safely* ".

As things stand, the statement of the accused entity cannot succeed in the sense that the City Council, at the time the events occurred, had implemented the appropriate or appropriate technical and organizational measures to guarantee the security of the data in the destruction phase.

Lastly, it should be noted that, according to the system of responsibility provided for in the RGPD and particularly in article 70 of the LOPDGDD, the responsibility for breaches of the data protection regulations falls, in any case, on the those responsible for the treatments, and not about their staff. Specifically, the mentioned article 70 of the LOPDGDD establishes that:

"Responsible subjects.
1. They are subject to the sanctioning regime established by Regulation (EU) 2016/679 and this Organic Law:
a) Those responsible for the treatments.

2.2 On the measures taken after the proven facts.

The City Council has alleged that once the facts that led to the initiation of the present procedure occurred, certain measures were immediately adopted in order to correct the effects of the imputed infringement, such as " *the collection and custody of all files in a closed space with restricted access" and* the subsequent transfer to the Municipal Archives, and that, likewise, and in order to prevent, as far as possible, incidents of the same nature from occurring again, " *immediately proceeded to update the existing circuit, (...) and draw up a new protocol, replacing the existing documented procedures at that time, called "action protocol for the treatment and destruction of non-automated media that contain personal data for which the Reus City Council is responsible" (hereinafter , the Protocol), which includes the procedure and circuit to be followed with regard to the treatment, conservation and subsequent destruction of non-automated media that have personal data. This circuit includes from when the City Council begins to process documentation with personal data until its subsequent destruction and elimination".*

In this same sense, the City Council details the measures it has implemented, following the approval of the Protocol, in order to guarantee the safe destruction of documentation with personal data, and requests that, for this purpose, have by reproducing the supporting documentation of these that was provided before the initiation agreement. The measures can be summarized as follows:

- The installation of airtight containers, in various rooms and workplaces of the City Council, " *for the safe collection and transfer of documentation with personal data*

subject to destruction to the Municipal Archive, and the subsequent destruction through the external company (...) ".

- Although the Municipal Brigades Unit continues to participate in the documentation transfer process, in full coordination with the administrative units, said Unit " *is no longer competent to carry out" any function - or collaboration - related to the destruction and elimination of City Council documentation that contains personal data".*

- The Municipal Archive, " *in the line already adopted prior to the approval of the Protocol* (...)" is the only body that *coordinates the service of secure destruction of documentation,* through the services provided by the company (...), in accordance with what is proven with the certificates of safe destruction provided (documents 11 to 57).

- The Protocol it has made available to all _ the employees of the City Council , through the Intranet, (document 59 provided in front the agreement of initiation) and they have been informed of theirs content _

In this regard, it must be made clear, as already advanced in the proposed resolution, that although all these measures, carried out once the incident took place, do not distort the facts imputed here nor their legal qualification , if they deploy effects in the sense that they make it unnecessary for the Authority to require the adoption of corrective measures to correct the effects of the infringement.

2.3 On the lack of complaints by the affected persons.

Finally, in order to justify its request for the postponement of the procedure, the City Council asserts that, once the public communication of the incident was made, in accordance with the provisions of article 34 of the 'RGPD, none of the affected persons (owners of the personal data contained in the files found in the debris dump), has made any complaint in this regard, nor is there any record that the Authority has received any complaint.

In this regard, it must be said that, among the objective elements that make up the infringing type provided for in article 83.4.a) of the RGPD, the need for the person holding the data, in relation to which has produced the infringement, considers his privacy or intimacy violated. The type only requires 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 32.1 of the RGPD. In other words, the target element of the infringing type will occur whenever and wherever there is an effective lack of security measures appropriate to the risk.

That is why this allegation cannot succeed either.

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 (integrity and confidentiality).*

For its part, article 32.1 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."

In the present case, it has been proven that the City Council of Reus, as the person responsible for processing the affected data, did not adopt or implement appropriate technical and organizational measures to guarantee its security (tending to prevent these data from being could be accessed by unauthorized persons), which is considered constitutive of the violation provided for in article 83.4.a) of the RGPD, which typifies the violation of *" the obligations of the responsible and of the manager pursuant to articles 8, 11 , 25 to 39, 42 and 43 "* , among which there is that provided for in article 32 RGPD.

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

"f) 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 32.1 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".

As progress has been made in the antecedents and the 2nd legal basis, the City Council of Reus has informed this Authority that it has carried out certain measures in order to correct the effects of the imputed infringement, and also those tending to avoid that events like those that had led to the initiation of the present sanctioning procedure were to occur again. That being the case, in this case, and as progress has been made, there is no need to require corrective measures.

For all this, I resolve:

1. Admonish the City Council of Reus as responsible for an infringement provided for in article 83.4.a) in relation to article 32, 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 legal basis 4rt.

2. Notify this resolution to Reus City Council.

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

4 . Order that the 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,