File identification

Archive resolution of the previous information no. IP 474/2021, referring to the Prat de Llobregat Town Council

Background

1. On 19/11/2021, the Catalan Data Protection Authority received a letter written by two people representing the union section SPL-CME El Prat de Llobregat, for which they denounced the City Council of El Prat de Llobregat, due to an alleged breach of the personal data protection regulations.

Specifically, the complainant union highlighted that, on 15/09/2021, 16/09/2021 and 17/09/2021, several officers from the Local Police of the Ajuntament del Prat de Llobregat would have received in their corporate e-mail addresses, an e-mail sent from the address <(...)@gmx.com> whose subject referred to " *Reflexionemos sobre el SPL-CME* ", by which it criticized the "behavior union" of the representatives of the SPL-CME El Prat de Llobregat Union (the complainant here). Then, he pointed out that the sending of the e-mail to the referred workers was carried out without using the option of the hidden copy, at the same time he showed his concern that people outside the City Council (specifically, the account holder <(...)@gmx.com> had been able to access the corporate email addresses of some officers of the Local Police.

Likewise, the complainant union explained that, faced with the sending of these e-mails to the corporate addresses of members of the Local Police - a fact that it considered " *a computer attack"*- , it contacted by telephone and also by e-mail - sent from the union's corporate address, with the City Council's Information Systems and Technologies unit (hereinafter, SITIC), bringing these facts to their attention; and that, in response to this e-mail, on 18/10/2021 the SITIC sent them an e-mail informing them about how workers should act in the face of an allegedly malicious e-mail, and informing them that the incident regarding the sending of e-mails from the address <(...)@gmx.com> " *had no more significance than the annoyance of the users who received it, but that is inevitable, they are e-mail addresses of a public entity and, therefore, much more exposed to the public domain".*

Finally, the union complaining here stated that, after receiving this email from SITIC, they found that the emails they had received from the address <(...)@gmx.com> had disappeared from the account of corporate e-mail of the union, as of the e-mails of the agents who received it. Faced with this fact, the complainant here stated that they did not understand " *how they were able to access both the union account and the agents' accounts and do cleaning, since each one has its own password"*

The letter of complaint is accompanied, among other documents, by the copy of the email received from the address <(...)@gmx.com>, in which it is verified that it was only sent to certain corporate e-mail addresses of City Council personnel.

2. The Authority opened a preliminary information phase (no. IP 474/2021), in accordance with the provisions of article 7 of Decree 278/1993, of November 9, on the sanctioning procedure applied to 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 susceptible to motivate the initiation of a sanctioning procedure.

3. In this information phase, on 07/13/2022 the reported entity was required to report on whether the City Council or any person linked to it, sent the controversial email to certain police officers Local, from the address <(...)@gmx.com>. Likewise, the City Council was also required to confirm whether it manages the e-mail accounts of its staff and whether, as manager or administrator of these accounts, it accessed the mailboxes of the workers by proceeding to delete the reference e-mail .

4. On 07/18/2022, the reported entity responded to the aforementioned request through a letter in which, in summary, it stated the following (the emphasis is ours):

- " *On Monday 09/20/2021 13:20 the technician [...] of the Information and Communications Systems and Technologies service (SITIC) requests the specialized technical office service, which offers support and advice in cross-cutting issues of security in the service, the verification of two emails received, which present the profile of dangerous or undesirable mail (SPAM), among which is the mail sent to the local police officers, the titles of the mails are following: "MICROSOFT VERIFICATION TEAM !!!" and "Forward: Let's reflect on the SPL-CME". The procedure in these cases is as follows: 1. E-mails are analyzed to check if they are potentially dangerous or unwanted e-mails (SPAM). 2. If the result is positive, it will be removed automatically from the City Council's IT systems, with the aim of avoiding any risk that could arise . 3. Source addresses are blocked to prevent future receipt of those addresses. In both cases, unwanted emails or SPAM were detected, and the protocol was applied . This is a very common and ordinary task for the technology and security services of any organization, computer attacks are a great risk that constantly and globally compromises the security of computer systems."*

In this regard, the City Council informed that the account <(...)@gmx.com> is foreign and external to the corporation, and that the sending of the said email was not an intrusion into the systems of the City Council, but that it was an unsolicited type of mail. In this regard, he added that, as soon as SITIC became aware of the receipt of this message, " the malicious mail and *anti -SPAM protocol was applied , and the mail was purged as well as the blocking of the senders, resulting from the own request formulated by the SPL-CME Union".*

Finally, the accused entity pointed out that SITIC cannot find out who sent the original email, as it is a third-party account and external to the City Council.

5. On 08/25/2022, also during this preliminary information phase, the City Council was again required to, among others, confirm whether it manages the email accounts of its staff and whether, how a manager or administrator of these accounts, accessed them by deleting the reference message from the recipient's email inbox.

6. On 08/28/2022, the City Council responded to the request for information indicated in the previous antecedent, in the following terms:

- " *The City Council did not provide the data relating to the corporate email addresses of certain employees to any person internal or external to the organization (...)"*

- " *The City Council has the obligation to manage the security of email accounts, therefore it has a protocol for the mass removal of emails suspected of being spam or malicious. No personal mailboxes are entered, they are deleted en masse when they are detected using the tools offered by the systems themselves for such purposes* .

Fundamentals of law

1. In accordance with the provisions of articles 90.1 of the LPAC and 2 of Decree 278/1993, in relation to article 5 of Law 32/2010, of October 1, of the Catalan Authority of Data Protection, and article 15 of Decree 48/2003, of February 20, which approves the Statute of the Catalan Data Protection Agency, the Director of the Authority is competent to issue this resolution Catalan Data Protection Authority.

2. Based on the background story, it is necessary to analyze the reported events that are the subject of this archive resolution.

The complainant union complained about the fact that a third person, owner of the account <(...)@gmx.com> , had sent an email to the corporate email accounts of certain employees of the City Council, without these had previously provided their addresses and without having obtained the consent of these people, in order to carry out the sending of the referred message. Likewise, the now complainant also pointed out that, after informing SITIC, a third person - whom he does not identify - would have deleted the controversial message from the corporate e-mail accounts of the people who received it.

2.1 In relation to the alleged leakage of data relating to corporate email addresses

As a preliminary question, it is necessary to analyze whether the corporate e-mail addresses of the City Council staff fit within the definition of personal data which, in accordance with article 4.1 RGPD, is the following: "all information about a natural *person identified or identifiable ("the interested party"); Any person whose identity can be determined, directly or indirectly, in particular by means of an identifier, such as a number, an identification number, location data, an online identifier or one or more elements of identity, shall be considered an identifiable physical person physical, physiological, genetic, psychological, economic, cultural or social of said person;*

In this regard, it is necessary to bear in mind the opinion CNS 4/2011 of this Authority which includes the following argumentation:

> *"It should be borne in mind that an email address will always appear necessarily linked to a specific domain, in such a way that it is possible to proceed with the identification of its owner by consulting the server on which this domain is managed, without this requiring a disproportionate effort on the part of whoever proceeds with the identification. On the other hand, the e-mail addresses of employees of a company (public, in this case) are usually configured in such a way (name_surname@ domain name) that it is easy to identify their holders. Therefore, according to these definitions, there can be no doubt that the information relating to the e-mail addresses of the people working in the public company can be qualified as personal data. Therefore, its treatment will be subject to the principles and obligations of the regulations on data protection."*

From the above, there is no doubt in attributing the status of personal data to the corporate e-mail addresses of City Council employees, and therefore their treatment must be subject to the principles and guarantees of the 'RGPD.

Having established the above, and with regard to the eventual leakage of the reported corporate addresses, the City Council has affirmed that it has not supplied this data to third parties, and has informed that the list of working people, their extensions and their e-mails electronic, can be consulted in the directory of the City Council's Intranet. In this sense, the reported entity has alleged that " *in the case of the local police, communications are usually made to the group of agents in an ordinary way, therefore it is viable for any internal person to obtain this information",* and has informed who does not know the identity of the person holding the email account <(...)@gmx.com>.

In this regard, this Authority does not have any evidence to support that the City Council has leaked this information to the person who owns the controversial email account , nor that the City Council has any connection with the owner of the account <(...)@gmx.com>.

In relation to the above, it should be borne in mind that, aside from the employees of the City Council who, obviously, can have access to said corporate addresses, it cannot be ruled out that third parties have obtained this information for their own media - for example, people who have provided services to the City Council, citizens who have been in contact with these public employees, among others - especially considering the fact that the message was received by some Local Police officers, but not all.

As things stand, this Authority cannot attribute to the City Council neither the sending of the said message, nor the disclosure or leakage to the holder of the e-mail account <(...)@gmx.com> of the information relating to the corporate email addresses of certain employees of the corporation.

2.2 In relation to the deletion of emails

With regard to the deletion of the message sent from the address <(...)@gmx.com> the complainant union stated that " *we do not understand how they were able to access both the union's account and the agents' accounts and do cleaning, since each one has its own password".*

In turn, the reported entity, consulted by this Authority, has acknowledged having deleted from the inbox of certain corporate addresses, corresponding to agents of the Local Police force and the reporting union, the email sent from the 'address <(...)@gmx.com> given its spam character.

In addition, the City Council has reported having applied the Protocol it uses in the case of detecting unwanted emails, which consists in the elimination, by means of an automated system, of the reference message, without it being necessary for any person enter the e-mail boxes of the recipients of the message.

Therefore, in accordance with what has been said, given that the City Council has confirmed that it has deleted the reference message, by automated means, without having entered the

account of the people who received it - an action that is technically completely feasible - , and given that this Authority does not have elements to support the contrary, it must be concluded that the action of the reported entity did not contravene data protection regulations.

3. In accordance with everything that has been set out in the 2nd legal basis, and since during the actions carried out in the framework of the previous information it has not been accredited, in relation to the facts that have been addressed in this resolution, any fact that could be constitutive of any of the infractions provided for in the legislation on data protection, it is necessary to agree to its archive.

Article 10.2 of Decree 278/1993, of November 9, on the sanctioning procedure applied to the areas of competence of the Generalitat, provides that "(... *) no charges will be drawn up and the dismissal of the file and the archive of actions when the proceedings and the tests carried out prove the non-existence of infringement or liability. This resolution will be notified to the interested parties"* . And article 20.1) of the same Decree determines that the dismissal proceeds: " *a) When the facts do not constitute an administrative infraction; b) When there are no rational indications that the facts that have been the cause of the initiation of the procedure have occurred (...)"*

Therefore, I resolve:

1. Archive the actions of prior information number IP 474/2021, relating to the Prat de Llobregat Town Council.

2. Notify this resolution to Prat de Llobregat City Council and the person making the complaint.

3. Order the publication of the resolution 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 article 14.3 of Decree 48/2003, of 20 February, which approves the Statute of the Catalan Data Protection Agency, the persons interested parties may file, as an option, an appeal for reinstatement before the director of the Catalan Data Protection Authority, within one month from the day after their notification, in accordance with what provided for in article 123 et seq. of Law 39/2015. An administrative contentious appeal can also be filed directly 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, governing the contentious administrative jurisdiction.

Likewise, interested parties may file any other appeal they deem appropriate to defend their interests.

The director,