apdcat
Autoritat Catalana de Protecció de Dades

Opinion in relation to the query formulated by a City Council in relation to the consideration of corporate email as personal data and the consequences of its use for the sender

A query formulated by a City Council is presented to the Catalan Data Protection Authority, in which an opinion is requested from this Authority in relation to the consideration of corporate email as personal data, and the consequences that its use may have for the sender, in various situations.

After analyzing the consultation, which is accompanied by a report from the General Secretary of the City Council on the issue raised, in view of the current applicable regulations, and in accordance with the report of the Legal Counsel, the following is ruled:

I

(...)

II

The query asks, at the outset, whether the corporate email consisting of the first surname, the initial of the second surname and the initial of the first name, as well as the identification of the corporation to which it belongs, is considered personal data, protected by the data protection regulations data

Likewise, the query asks the following:

> *"The sending of an email by a member of the corporation to another member or members of the corporation, dealing with issues about the same, and copying an email address from outside the corporation, would be liable to incur in violation of data protection regulations? What consequences or actions can be brought in this case, against the person who is part of the corporation and holder of the corporate mail account, who sent (sender) to the mail of other members of the corporation, putting in a copy a non-corporate email address? Has the sender committed any breach of data protection regulations?*
>
> *The same situation, but in the case that the shipment was made, by a member of the corporation, but from his personal email address, could it incur a violation of the regulations on data protection? what consequences or actions could be brought against said person?"*
>
> The inquiry adds that, in both cases, the sending in question is always *"without the consent of the recipient or recipients of the mail members of the corporation to provide their email address to a third party, not a member of the corporation".*

With the consultation in these terms, it is necessary to start from the basis that, according to article 4.1) of Regulation (EU) 2016/679, of April 27, general data protection (RGPD), they are personal data . *any information about an identified or identifiable natural person ("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;*

Therefore, at the outset, any information that allows a natural person to be directly or indirectly identified is personal data, and is protected by the principles and guarantees of the data protection regulations (RGPD and Organic Law 3/2018, of December 5, of Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD)).

According to recital 26 of the RGPD: *"(...). To determine whether a natural person is identifiable, all means, such as identification, that can reasonably be used by the data controller or any other person to directly or indirectly identify the natural person must be taken into account. (...)."*

For the purposes of this opinion, Recommendation 1/2013 of the Catalan Data Protection Authority, on the use of email in the workplace, is of particular interest, as well as the *"Manual of good use of e-mail. Guide for working people to protect privacy in the use of e-mail",* available on the Authority's website (www.apdcat.cat).

According to the aforementioned Recommendation (section 2), an email address can be defined as *"the set of words or signs that identify the sender or receiver of an email message. It is made from a set of words or signs freely chosen, usually by its holder or by the organization to which it belongs, with the only limit that this address does not coincide with that of another person. It consists of a user identification, followed by the @ sign, and then the domain (identification provided by the mail service provider, with a period, and some abbreviations that can identify the organization's activity (p .eg ".org ") or the country's initials (eg ".es" or ".cat").*

As set out in the Recommendation, we can distinguish different types of addresses:

- Personalized addresses: addresses that directly contain information about their owner. Usually, in personalized addresses you can use the full name and surname, only the initials, or the initial of the first name and surname, etc. These email addresses directly identify the owner of the account and therefore must be considered as personal data.

- Non-personalised addresses: these are those which, although it is an address linked to an email account of a specific natural person, do not contain information about their holder (use an abstract or meaningless alphanumeric combination). In this case, the address alone would not identify the person who owns it. But this person can be easily identified, without a disproportionate effort, either because the address can appear together with other data that allow identification, either by the content of the message, or through the data available to the mail server. Therefore, this address would also be given of a personal nature.

- Generic email addresses: these are those that respond to a generic, shared account or an area of the organization (for example, consultes@empresa.cat). In this case, the email address cannot be linked to an identified or identifiable natural person, but can be regularly served by different users. Therefore, it cannot be considered personal data.

In line with this, as this Authority has done in several reports (CNS 55/2019, IAI 18/2019, IAI 2/2021, or CNS 36/2022, which can be consulted on the City Council's website), the addresses of work or professional emails that can be associated with identifiable natural persons (art. 4.1 RGPD), must be considered as personal data.

As stated in Opinion CNS 4/2011 *"It should be borne in mind that an email address will always appear necessarily linked to a specific domain, so that it is possible to proceed with the identification of its owner by consulting the server in that this domain is managed, without this requiring a disproportionate effort on the part of the person carrying out 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 data protection regulations."*

For all that has been said, there can be no doubt that a corporate email address, in this case, of a City Council, which uses in its format the first surname, the initial of the second surname and the initial of the first name, as well as the identification of the corporation, since it allows the identification of the account holder, is personal data protected by the principles and guarantees of the data protection regulations (RGPD and LOPDGDD).

III

Having said that, from the point of view of data protection, it should be borne in mind that the City Council, as responsible for the processing of the personal information it has (Article 4.7 RGPD), is responsible for the general task of guaranteeing that the data treatments that are carried out through its information systems and the devices it provides to its staff for the exercise of their professional functions, are adapted to the data protection regulations, and must be in a position to demonstrate this compliance, in application of the principle of proactive responsibility (article 5.2 RGPD).

This requires the City Council, in the case at hand, to carry out a series of actions (Article 24 RGPD), among others:

- Carrying out a risk analysis.
- The definition of a policy for the use of information systems and digital devices.
- The implementation of technical and organizational security measures appropriate to the risk.

These aspects which, in addition, must be considered not only with respect to the personal data of natural persons, which the City Council has for the exercise of their powers, but also with respect to the personal data of the municipal workers themselves who employ the

information systems and other corporate tools to carry out the professional tasks entrusted to them.

The person in charge must take into consideration the implications that, for the privacy and data protection of these municipal employees and, where applicable, of third parties, the establishment of control measures on the use of the tools may entail mentioned by the council, in application of the current regulatory framework, and criteria for the correct use of these instruments.

According to article 87 of the LOPDGDD:

"1. Workers and public employees have the right to the protection of their privacy in the use of digital devices made available to them by their employer.

2. The employer will be able to access the content derived from the use of digital media provided to the workers for the sole purpose of monitoring compliance with labor or statutory obligations and guaranteeing the integrity of said devices.

3. ***Employers must establish criteria for the use of digital devices*** *respecting in any case the minimum standards of protection of their privacy in accordance with social uses and constitutionally and legally recognized rights. Workers' representatives must participate in its preparation.*

The access by the employer to the content of digital devices with respect to those that have admitted their ***use for private purposes will require that the authorized uses be precisely specified*** *and that guarantees be established to preserve the privacy of the workers, such as, where appropriate, the determination of the periods in which the devices may be used for private purposes.*

Workers must be informed of the use criteria referred to in this section."

Likewise, we agree that the National Security Scheme (ENS), approved by Royal Decree 311/2022, of May 3, is applicable, among others, to local administrations in accordance with the first additional provision of the LOPDGDD. Article 12 of the aforementioned RD defines the security policy (section 1), and determines that each public administration must have a security policy formally approved by the competent body that regulates the use of equipment (section 3.2 and 5.8 .1 of Annex II).

It is also necessary to take into account several provisions of the regulations in the field of employment, in relation to the legality of control measures by the City Council, in this case, the fulfillment by its staff of their work obligations.

In particular, article 52 of the Revised Text of the Law of the Basic Statute of the Public Worker (TRLEBEP), approved by Royal Legislative Decree 5/2015, of October 30, according to which "los empleados públicos must perform with *diligence the tasks they have assigned and look after the general interests with subjection and observance of the Constitution and the rest of the legal system (...)",* and article 20.3 of the revised text of the Workers' Statute Law (ET), approved by Royal Legislative Decree 2/2015, of October 23, according to which "the employer may adopt the measures he deems most *appropriate of vigilance and control*

to verify compliance by the worker of his obligations and labor duties, keeping in his adoption and application the consideration due to his dignity (...)".

So, the applicable regulatory framework establishes the possibility that the employer, in the case at hand, a City Council, exercises control or supervision of the use made by its staff of the means available to it in the workplace, with the limitations that derive from the right to privacy and the dignity of the staff, as specified by repeated jurisprudence, among others, in the SSTEDH of September 5, 2017 (Barbulescu case) of February 28, 2018 (Libert case); in SSTC 241/2012, 170/2013, or 61/2021; or SSTS 119/2018, of February 8, or 489/2018, of October 23.

In summary, the jurisprudence has admitted that the employer can establish controls on the use of the tools that he makes available to workers for the need to coordinate and guarantee the continuity of work activity in the event of absences of workers, for the protection of information systems, which may be negatively affected by certain uses, and also for the prevention of responsibilities that for the employer may derive from illicit forms of use to third parties.

However, the company must specify these rules for the use of said tools, and inform the workers accordingly.

According to the STS of September 26, 2007 (FJ III):

"(...) it is necessary to remember what has already been said about the existence of a generalized social habit of tolerance with certain moderate personal uses of computer and communication media provided by the company to workers. That tolerance also creates a general expectation of confidentiality in those uses; expectation that cannot be unknown, although it does not become a permanent impediment to business control, because, although the worker has the right to respect his privacy, he cannot impose that respect when he uses a medium provided by the company against the established instructions for this use and outside of the controls provided for that use and to guarantee the permanence of the service. Therefore, ***what the company must do in accordance with the requirements of good faith is to establish beforehand the rules for the use of these media - with the application of absolute or partial prohibitions - and to inform the workers that there was control*** *and of the media which must be applied in order to verify the correctness of the uses, as well as* ***the measures that must be adopted*** *in their case to guarantee the effective occupational use of the medium when necessary, without prejudice to the possible application of other preventive measures , like the exclusion of certain connections. Thus,* ***if the medium is used for private purposes against these prohibitions and with knowledge of the controls and applicable measures, it cannot be understood that, when the control is carried out, "a reasonable expectation of privacy" has been violated in the*** *terms which establish the judgments of the European Court of Human Rights of June 25, 1997 (Halford case) and April 3, 2007 (Copland case) to assess the existence of a violation of Article 8 of the European Convention for the Protection of Human Rights ."*

For the purposes that concern, it will be based on the data protection regulations and other regulations mentioned, taking into account the relevant jurisprudence and, where appropriate, the indications and instructions on the appropriate uses of the work and communication tools established by the City Council, which can determine the legality or

illegality of this use in each specific case and, where appropriate, the responsibilities that may arise.

IV

The query refers to the sending of e-mails by a worker to other workers of the corporation, "dealing with issues about the same", copying an e-mail address external to the corporation, without the consent of these others workers (who would not, according to the query, have authorized their address to be known by the council's external addressee). The query also refers to the same assumption, but using the said worker (sender of the message) a "personal email address".

The RGPD provides that all processing of personal data must be lawful (Article 5.1.a)) and, in this sense, establishes a system of legitimizing data processing based on the need for one of the legal bases to be met established in its article 6.1, among others:

" 1. The treatment will only be lawful if at least one of the following conditions is met:

a) the interested party gives his consent for the treatment of his personal data for one or several specific purposes;
b) the treatment is necessary for the execution of a contract in which the interested party is a party or for the application at the request of this pre-contractual measures;
c) the treatment is necessary for the fulfillment of a legal obligation applicable to the person responsible for the treatment;
d) the treatment is necessary to protect the vital interests of the interested party or another natural person;
e) the treatment is necessary for the fulfillment of a mission carried out in the public interest or in the exercise of public powers conferred on the person responsible for the treatment;
(...).”

Therefore, the processing of personal data that occurs as a result of the sending of e-mail messages by a public worker will be lawful, from the outset, depending on whether one or more legal bases exist that enable said processing .

Obviously, the consent of the affected persons (such as, given the terms of the consultation, the holders of the corporate electronic addresses included in the message, which would be considered personal data), could be a legitimizing legal basis for the treatment (art. 6.1. a) RGPD).

Now, as the Article 29 Working Group (currently, European Data Protection Committee) points out, in its Opinion 2/2017, on the processing of data in the work environment, the basis legal basis for the processing of data in the field of labor relations can hardly be consent - at least, in general -, given that we are in a context of clear imbalance between the affected (employee) and the person responsible for the treatment (company).

According to this Opinion: *"It is very unlikely that consent constitutes a legal basis for data processing at work, unless the workers can refuse without adverse consequences (...). Except in exceptional situations, employers will have to rely on another legal basis other than*

consent, such as the need to process the data for their legitimate interest. However, a legitimate interest in itself is not sufficient to prioritize the rights and freedoms of workers"

In the labor field, the processing of workers' data is mainly justified on other legal bases other than the consent of those affected, such as the execution of the contract to which the worker is a party, which would enable its processing by of the company (art. 6.1.c) RGPD), or the fulfillment of a mission carried out in the public interest or in the exercise of public powers, in this case, of the City Council (art. 6.1.e) RGPD).

These provisions may enable, in general terms, the sending of mails by a council worker to other people (either other workers or, where appropriate, external recipients), if this treatment of corporate contact data it is justified in the development of their work, or is related to it.

To this it should be added that according to article 2.b) of Law 19/2014, of December 29, on transparency, access to public information and good governance (LTC), public information is "the information prepared by the Administration and that which it has in its power as a result of its activity or the exercise of its functions, including that supplied by the other obliged subjects in accordance with the provisions of this law".

Corporate email addresses of public employees (and, where applicable, other professional contact details), would be public information for the purposes of transparency legislation.

According to article 70.2 of Decree 8/2021, of February 9, on transparency and the right of access to public information: " *For the purposes of what is provided for in article 24.1 of Law 19/2014, of 29 December, are merely identifying personal data consisting of the name and surname, the position or position held, body and scale, the functions performed and the telephone and addresses, postal and electronic, of professional contact, referred to the staff at the service of the public administrations, senior officials and managerial staff of the public sector of public administrations."*

Thus, in principle it does not seem that workers should have an expectation of privacy regarding the use of corporate electronic addresses by other workers.

This, as long as the professional contact data of third parties is used, as has been pointed out, for the development of the proper and usual scope of labor relations, and without prejudice to the margin that, for private use or particular of the communication tools, the company has been able to establish, a matter to which we have also referred.

For all of the above, corporate email addresses, as professional contact data, may be processed for the purpose of communications related to the workplace, as long as there is an enabling legal basis (art. 6.1 RGPD) , and its use is respectful of the rest of the principles and guarantees of the data protection regulations, specifically, the purpose principle, according to which personal data must be collected for specific, explicit and legitimate purposes, in or must be subsequently treated in a manner incompatible with these purposes (art. 5.1.b) RGPD).

This, without prejudice to the forecasts that the City Council, in this case, has previously determined in relation to the appropriate use of the tools it makes available to workers, which they must know in the terms of the aforementioned regulations.

It will therefore be based on the reason and circumstances in which a specific communication of contact data of municipal workers occurs to a third party external to the council, that it will be possible to determine whether this communication is authorized or, where appropriate, whether it can be incurred in inadequate treatment of these professional contact data.

v

In this context, given the terms in which the query is formulated, it should be noted that the mere fact of including a recipient who is not part of the City Council itself would not, per se, be contrary *to* data protection regulations.

On the contrary, as an example, it may even be common for a shipment to be copied by other employees of the council or other administrations, public or private bodies involved in the provision of a service, addresses of citizens or other external recipients, etc.

A different matter would be, for example, the inclusion of an address (not only of an external recipient, but of a recipient of the corporation itself, for example, or of another administration or entity), in an erroneous form, or without it responding to a legitimate purpose, and more so, if this involves bringing to the attention of third parties certain personal information to which all or some of the recipients should not have had access, in view of the content of the message in question.

For illustrative purposes, we note that this Authority has examined on several occasions cases relating to the sending of email messages, from the perspective of data protection, in which the particular circumstances of each case have been analyzed , for the purposes of determining both the possible concurrent infringement of data protection regulations, as well as the determination of possible responsibilities (as an example, we mention the Resolution of the sanctioning procedure PS 33/2019, or the Resolution of file IP 340/2018, which can be consulted on the website www.apdcat.cat , both relating to the use of corporate mail). Analysis that does not correspond to carry out in this opinion in relation to the assumption of the consultation, which is set out in general terms.

In any case, given the terms in which the query is formulated, it cannot be determined whether a specific breach of data protection regulations would occur, for the mere fact that an email has been sent to a recipient outside the council.

It will be necessary to examine in each case whether the inclusion of an external recipient is lawful for the purposes of the principle of purpose (art. 5.1.b) RGPD) and whether there is a legal basis enabling said treatment (art. 6 RGPD).

Finally , the query also refers to the same case, but in the case of using a private e-mail address of the worker (different from the corporate address provided by the company).

With regard to this circumstance, and based on the considerations already made, we cannot rule out that, in the workplace, circumstances may arise that justify the sending of an email by an employee , not through the corporate address (which would be the usual assumption given that it is the tool that the company provides to the worker for this purpose), but from a private or personal address of the worker.

Thus, merely as an example, circumstances may arise in which the worker is unable to use the corporate address, and must send a certain message through other means (due to technical difficulties, unavailability of the usual work tools for various reasons, to be on vacation, in a telework situation, etc.).

This fact, in itself, does not seem to constitute in any case a violation of the data protection regulations, as long as the data protection principles and guarantees we have referred to are complied with.

This, without prejudice to the fact that a prohibition in this regard has been previously and transparently stated by the company (in this case, the City Council), through the regulations for the use of corporate tools and other tools of communication by the staff.

In any case, to determine this end it will be necessary to take into account the specific guidelines or indications that the City Council has specified in relation to this possibility. Guidelines that, as has been said, the City Council must necessarily have brought to the attention of the workers, according to the aforementioned regulations.

VI

Without prejudice to the fact that, as can be seen from the considerations made, this opinion does not correspond to determine whether or not there is an infringement of the data protection regulations in the specific case, beyond the general indications that have been made, it is appropriate to point out the next.

In specific cases, the commission of an infringement of data protection regulations may be materially attributable to a specific person who provides services in an organization.

However, according to the liability system provided for in the RGPD, responsibility for breaches of data protection regulations falls, among others, on those responsible for the processing, and not on their employees.

Thus, according to article 70.1 of the LOPDGDD:

> *" They are subject to the sanctioning regime established in Regulation (EU) 2016/679 and in this organic law:*
>
> *a) Those responsible for the treatments.*
> *b) Those responsible for the treatments.*
>
> *(...).”*

As this Authority has decided, among others, in the Resolutions of the sanctioning procedures PS 46/2021, PS 23/2020, or PS 33/2019, available on the Authority's website (www.apdcat.cat) , d ' in accordance with the liability regime provided for in the data protection regulations, the attribution of responsibility, if applicable, for the commission of an offense classified in said regulations by an entity's own staff (articles 71 and ss . LOPDGDD), would fall to the person in charge of data processing.

In this regard, it is necessary to take into account the repeated doctrine of the Supreme Court on the attribution of responsibility when the infringement is committed by the personnel of a legal entity, based on the existence of a fault *in eligendo* or *in vigilando ,* between others, the STS of 196/2021, of February 15, or the STS188/2022, of February 15, both regarding the protection of personal data, to which we refer for illustrative purposes.

Obviously, in each case, it will be necessary to examine, taking into account the concurrent circumstances, whether the principle of culpability applies, that is to say, the need for there to be intent or fault in the punitive action, which is applicable to the penal administrative law, in accordance with the liability regime provided for in article 28 of Law 40/2015, of October 1, on the legal regime of the public sector, to which we refer.

Likewise, we recall that, according to article 77 of the LOPDGDD, relating to the regime applicable to the treatment for which certain categories of persons in charge or in charge are responsible, among others, the entities that make up the local administration (section 1 .c):

> *"(...).*
>
> *2. When the managers or managers listed in section 1 committed*
> *any of the infractions referred to in articles 72 to 74 of this organic law, the competent data protection authority will issue a resolution sanctioning the same with notice. The resolution will also establish the measures to be adopted so that the conduct ceases or the effects of the offense that had been committed are corrected.*
>
> *The resolution will be notified to the person in charge or in charge of the treatment, to the body of which*
> *it depends hierarchically, in his case, and the affected people who would have the condition of*
> *interested, if so.*
>
> *3.* ***Without prejudice to what is established in the previous section, the data protection authority will also propose the initiation of disciplinary proceedings when there are sufficient indications*** *for this. In this case, the procedure and the sanctions to be applied will be those established in the legislation on the disciplinary or sanctioning regime that results from application."*

Thus, it cannot be ruled out that, in the event that the sending of an email by an employee may lead (due to the circumstances of the transmission or the content of the message) to an infringement of the data protection regulations that would in principle be attributable to the person in charge, disciplinary consequences could be derived from it, in relation to the worker who may have acted negligently or contrary to compliance with said regulations.

As a last resort, remember that, in the event that the City Council detects misuse of the equipment provided to staff that could constitute a crime or misdemeanor, the Public Prosecutor's Office should be notified.

conclusion

The corporate email address of a City Council, which uses in its format the first surname, the initial of the second surname and the initial of the first name, as well as the identification of the corporation, given that it allows the identification of the account holder, it is personal data protected by data protection regulations.

The processing of personal data that occurs as a result of the sending of e-mail messages by a public employee, in particular, the inclusion of third-party corporate e-mail addresses and the transmission to an external recipient, may be lawful if there is a legal basis (art. 6.1 RGPD) and the purpose principle is complied with (art. 5.1.b) RGPD).

According to the liability system provided for in the RGPD, responsibility for breaches of the data protection regulations rests with those responsible for the treatment, without prejudice to the fact that consequences may arise from a breach of the data protection regulations of a disciplinary nature, in relation to the worker who may have acted negligently or contrary to compliance with said regulations.

Barcelona, April 25, 2023