apdcat
Autoritat Catalana de Protecció de Dades

Opinion in relation to the consultation formulated by a town council on the policy of using the council's information and communication systems

Background

A letter from a town council is presented to the Catalan Data Protection Authority, in which it raises several questions related to the policy for the use of information and communication systems that the council is preparing.

Specifically, in relation to the regulation of access and management of personalized corporate email addresses, as well as corporate applications, the following questions are formulated:

> *" **A.** (...) In the definitive cancellation of a personalized corporate email address when the user assigned to the mailbox stops providing services to the City Council, we have the following inquiries:*
>
> - *It is necessary to draw up an internal procedure that establishes the rules for the use of information systems in which the protocol for blocking the personalized corporate e-mail address and how it will be managed in the event of a definitive cancellation is reported, and it is necessary to inform the users of this procedure?*
> - *It is necessary to create an automatic reply message prior to the blocking of the personalized corporate e-mail address that informs of the cancellation of the user person assigned to the personalized corporate address and that indicates another contact address for the forwarding of mails ?*
> - *Can incoming e-mails from the personalized corporate e-mail address of the person who ceases to provide services to the City be automatically redirected to a new address?*
> - *Can the City Council retrieve, if appropriate, the messages necessary to guarantee the proper functioning of the service prior to the user ceasing to provide services to the City Council and in their presence? If this is not possible, can the messages be recovered and how should it be done?*
> - *The person using the personalized corporate address who will stop providing services to the City may be allowed to retrieve personal messages before the email account is blocked and the person no longer provides services.*
> - *How long must the active account of the personalized corporate email address of the user who has ceased to provide services be retained so that it cannot be considered an unreasonable and disproportionate period of time?*
> - *Can the account of the personalized corporate e-mail address be left inactive from the day following the date on which the user ceases to provide services to the City Council?*
> - *It could be considered suitable for data protection regulations that the personalized corporate email address can be active for a period of one month and an automatic response message is recorded in which reference is made*

that the person is no longer provides services to the corporation and that for any issue they can contact the City Council, stating the corresponding telephone number or email address.

- *Once a custom corporate email address can be active, should it be deleted or kept locked, and if so, for how long?*
- *From the date on which the user ceases to provide services, could the content of the email box be downloaded and kept locked, at the same time as the personalized corporate email address is canceled? If so, how long should this information be kept locked?*

***B.** (...) Regarding access to a personalized corporate email address for email users who are temporarily suspended from providing services, we have the following queries:*

- *When a user of the mail service is on temporary leave, in what situations and how can the City Council access the content of their personalized corporate email address?*

***C.** (...) Prior to the telecommuting situation when a person using the applications was on leave, they did not go to work in the municipal facilities and, therefore, did not access the assigned applications from their computer desktop. With telecommuting, this has changed and users can access the applications while they are off the phone using the assigned corporate devices or via the internet. This means that improper accesses can occur during this situation of leave and that it is necessary to monitor the accesses made to avoid possible leaks of information and we have the following queries:*

- *When a user of the applications is temporarily out of service, in what situations and how can the City Council monitor a period of time and access the access register of the applications to which the user is authorized to access?*

***D.** (...) When a user stops providing services to the City Council, can he request a copy of the emails from his personalized corporate email address?"*

Having analyzed the query and the documentation that accompanies it, in view of the applicable regulations in force, and in accordance with the report of the Legal Adviser, I issue the following opinion.

Legal Foundations

I

(...)

II

The consultation raises several questions related to the policy for the use of the information and communication systems of the City Council, which is in the drafting phase.

From the point of view of data protection, it is important to bear in mind that the City Council, as responsible for the processing of personal information at its disposal (Article 4.7) of Regulation (EU) 2016/679, of the Parliament and of the Council European, of April 27, 2016, General of Data Protection (hereinafter, RGPD)), it is responsible for the task of guaranteeing and being able to demonstrate that the data treatments carried out through its information systems and devices that it provides to its staff for the exercise of their professional functions are adapted to the data protection regulations (article 5.2 RGPD, relating to the principle of proactive responsibility).

This, in practical terms, requires, among other actions (article 24 RGPD):

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

Aspects that, it must be said, must be considered not only with respect to the personal data of citizens available to the City Council for the exercise of their powers, but also with respect to the personal data of municipal employees who use the information systems and other corporate tools to carry out the professional tasks entrusted to them.

This obliges the City Council to also take into consideration the implications that, for the privacy and data protection of these municipal employees, the establishment of control measures on the use of the aforementioned tools by the council may entail , in application of the current regulatory framework.

Regarding these issues, mention should be made of article 87 of Organic Law 3/2018, of December 5, on the protection of personal data and the guarantee of digital rights (hereafter, LOPDGDD), which provides the following:

> *"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 may access the content derived from the use of digital media provided to workers for the sole purpose of controlling 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 all cases the minimum standards of protection of their privacy in accordance with social customs and constitutionally and legally recognized rights. The representatives of the workers must participate in its elaboration.*

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."

It is also necessary to take into account several provisions of the regulations in the field of employment, in relation to the lawfulness of the control measures by the employer - in this case, the City Council - of the compliance by the working people 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 assigned to them and to 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 surveillance and control measures he deems most appropriate to verify the employee's compliance with his obligations and labor duties, keeping in its adoption and application the consideration due to its dignity (...)".*

Point out that the jurisprudence (for example, the STS of September 26, 2007 or the most recent STC 61/2021 to which we refer) has admitted that the employer can establish controls on the use of the tools that makes available to workers for the need to coordinate and guarantee the continuity of work activity in the event of worker absences, for the protection of information systems, which may be negatively affected by certain uses, and for the prevention of the responsibilities that the employer may derive from illicit forms of use vis-à-vis third parties.

Particularly relevant is, in this sense, the Judgment of the European Court of Human Rights (ECtHR), *Barbulescu case* , of 5 September 2017, in which the ECtHR establishes certain elements that should be applied in this context. In summary, the ECtHR refers to the information that must be given to working people regarding the measures that the employer can take to supervise these tools, in particular, the communications of the workers; what is the scope of supervision; or if the employer has assessed the existence of less intrusive control measures for workers , among others (section 210 of the STEDH of September 5, 2017, to which we refer).

It should also be noted that this Authority has issued Recommendation 1/2013, on the use of e-mail in the workplace (available on the Authority's website), in which different considerations are made that are of particular interest in the case examined, and those we will mention throughout this opinion.

III

Focusing on the specific questions raised in the consultation, many of them are related with the regulation of access and management of corporate e-mail accounts, with a

personalized address, when the address assigned to a working person is canceled in order to stop providing services to the City Council definitively.

At the outset, it is considered whether "it *is necessary to draw up an internal procedure that establishes the rules for the use of information systems in which information is provided on the protocol for blocking the personalized corporate email address and how it will be managed in the event of definitive cancellation"* , as well as if "it *is necessary to inform the users of this procedure".*

As can be seen from article 87.3 of the LOPDGDD, transcribed in the previous section, the City Council must have a policy or manual that includes the criteria or clear rules on the conditions of use of the information systems and digital devices that it makes available to its workers to carry out their professional duties, who must warn about the control mechanisms on their use that may affect the privacy of workers, the consequences that may arise from this control and guarantees for workers, especially the right to be informed.

Prior information to workers on these matters is essential in order to be able to consider control by the employer as legitimate regarding the tools mentioned and their use (articles 5.1.a and 6 RGPD), as has been amply recalled by the jurisprudence in this regard, such as, among others, the STS of September 26, 2007 (FJ III):

> *"It is necessary to remember what has already been said about the existence of a widespread social habit of tolerance with certain moderate personal uses of the computer and communication media provided by the company to the workers. This tolerance also creates a general expectation of confidentiality in those uses; This expectation cannot be ignored, although it cannot become a permanent impediment to company control, because, although the worker has the right to respect for his privacy, he cannot impose that respect when he uses a means provided by the company against the established instructions. by it for its use and outside the controls provided for that use and to guarantee the permanence of the service. For this reason,* ***what the company must do*** *in accordance with the requirements of good faith* ***is to previously establish the rules for the use of these means*** *-with the application of absolute or partial prohibitions-* ***and inform the workers that there will be control and of the means*** *that must be applied in order to verify the correctness of the uses, as well as the measures that must be adopted, where appropriate, to guarantee the effective labor use of the medium when necessary, without prejudice to the possible application of other preventive measures. , such as the exclusion of certain connections. In this way, if the medium is used for private purposes contrary to these prohibitions and with knowledge of the controls and applicable measures, it cannot be understood that, when carrying out the control, "a reasonable expectation of privacy" has been violated in the terms established by 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 its part, the National Security Scheme, approved by Royal Decree 311/2022, of May 3, which is applicable to the City Council in accordance with the first additional provision of

the LOPDGDD, provides, as as a security measure, the establishment of e-mail usage rules for the organization's staff (section 5.8).

Among the different aspects to be dealt with in these rules or policy of use, it would certainly be advisable to collect the measures that will be adopted to manage the personalized corporate email account of working people in the event of the termination of their employment relationship with the City Council.

It should be borne in mind that, from the point of view of data protection, the termination of the employment relationship must entail the cessation of the processing of the employee's personal information by the City Council and, therefore, also of the address of the personalized e-mail account that has been provided to him for the development of his professional tasks, when the purpose justifying its treatment ceases at the same time (articles 5.1 b) and i) RGPD, principles of limitation of the purpose and the term of conservation, respectively).

This can have implications both for the working person, who could be interested in having private or personal messages from their corporate account, and for the City Council itself, which could affect the continuity of municipal activity to a greater or lesser extent.

Point out that, although it is not known whether in the usage policy that is being drawn up the City Council plans to admit a certain private use of personalized corporate email accounts, it must be borne in mind, as this Authority points out in Recommendation 1/ 2013, previously cited, that even with respect to e-mail accounts for which an exclusively professional use is established, the working person will not always be able to avoid, for example, the use by third parties of this e-mail, to send personal messages.

For the purposes of guaranteeing a correct treatment of the information in these cases, it is important to have an internal procedure relating to the use of corporate email that takes this and other circumstances into account, and where information is provided prior to blocking of the employee's account of the management that will be carried out by the City Council and, therefore, of the specific measures that can be adopted in this regard.

Remember that the determination and adoption of these measures is, in any case, a decision that corresponds to the City Council, in consideration of its needs when dealing with the personal information for which it is responsible (articles 4.7 and 26 GDPR).

IV

In relation to the possible measures to be adopted, the consultation considers whether *"it is necessary to create an automatic response message prior to the blocking of the personalized corporate e-mail address that informs of the termination of the user who has been assigned the address personalized corporate and that indicates another contact address for the forwarding of mails"* and whether *"incoming e-mails can be automatically redirected from the personalized corporate e-mail address of the person who ceases to provide services to the City Hall to a new address".*

In section III.4 of Recommendation 1/2013, referring to access to e-mail by the company (in this case, the City Council), some actions are identified that the employer can take to

term to correctly manage the information due to the termination of the employment relationship of the working person.

Specifically, it is pointed out that in these situations it is necessary to immediately notify the person responsible for the management of the email accounts so that *"the worker's user codes and passwords are not used and, where appropriate, 'include an auto-reply message for incoming mail indicating the new address to which messages can be addressed for professional reasons.'*

Therefore, in attention to the specific needs that may arise in the specific case (for example, according to the position and/or position of the working person and the functions he has been performing), it may be an appropriate measure to schedule an automatic response message for all incoming mail to the mailbox of the employee who ceases to provide services to the City, indicating that the account in question is no longer in use and the new corporate mail address where mail can be addressed for professional reasons.

This action is preferable to automatically forwarding incoming e-mails to another corporate e-mail address, given that, in these cases, there is a lack of control over the e-mails in question, so the private information that eventually could be included, it could end up being known by people not foreseen by the person sending the communication, potentially contravening not only the data protection regulations (Article 5.1.e) RGPD, principle of integrity and confidentiality), but also other constitutional rights protected (privacy and secrecy of communications (article 18.1 and 3 EC)).

V

The consultation also raises the issue of whether *"the City Council can retrieve, if appropriate, the messages necessary to guarantee the proper functioning of the service prior to the user ceasing to provide services to the City Council and in their presence "* and if this is not possible *"if the messages can be recovered and how it should be done".*

As indicated by this Authority in Recommendation 1/2013, one of the objectives that could justify access to the corporate email of employees by the employer, in this case the City Council, and whenever there is adequately informed, is to guarantee the continuity of the company's normal activity, given that this could be affected if certain professional information is not available (article 87 LOPDGDD, in connection with labor regulations and existing jurisprudence) .

Also in this case, as pointed out in said Recommendation, it is advisable to plan and define in the policy for the use of the information systems - and inform the workers - the measures that will be adopted in this regard in case of 'absence of working people and also in the case of termination of the employment relationship (section III. 2 and 4).

Point out that, in application of the principle of proactive responsibility (article 5.2 RGPD), the person responsible, in this case, the City Council, must answer for compliance with data protection principles and, for this reason, it is not enough to allege a purpose for access that in general terms may be lawful, but it must be motivated based on the circumstances of each case.

Thus, in the case of termination of the employment relationship, and following the considerations formulated in Recommendation 1/2013, as well as in Recommendation CM/REC (2015) 5, of April 1, 2015, of the Committee of Ministers of the Council of Europe, regarding the processing of personal data in the context of the employment relationship, it could be established in the policy of use that access to the corporate e-mail account of working people that could be justified in order to guarantee the continuity of the normal activity of the City Council, the purpose is to recover the information strictly linked to the professional activity of the working person who causes definitive leave from the City Council when this is essential to continue with the City Council normal municipal activity; that access will be carried out, whenever possible, prior to the day on which the employment relationship with the City is effectively terminated, in the presence of the working person and, where appropriate, of a third party; that, when this is not possible, the former employee's superior body will have to assess the necessity of the intervention in a motivated way and will have to identify the specific information to which it is necessary to access, and that the access will be communicated, if possible, to the former employee; and that, in no case, access will cover messages that can be clearly identified as private or personal, or those that the employee himself indicates of this nature.

It should be borne in mind that, given the purposes provided for in article 87 of the LOPDGDD, in connection with the labor regulations examined, which can enable access and monitoring of the equipment that the company makes available to its workers, the access to private information would be neither provided nor justified.

VI

The consultation also considers whether *"the user of the personalized corporate address who will stop providing services to the City Council can be allowed to retrieve personal messages before the email account is blocked and the person no longer provides services. "*

As stated in Recommendation 1/2013 (apparatus II.4), it is important to establish in the usage policy a maximum retention period for private messages, after which they must be deleted, as well as encouraging the creation of folders to store emails of this nature that allow for easy identification in case of eventual access by the employer to the corporate email account.

It is also agreed in said Recommendation (section III.4) that, given the case of termination of the employment relationship, the company (the City Council) must make it easier for the employee to obtain the private messages from said account of corporate mail, as long as they do not exceed the maximum retention period established in the usage policy. And that, in this case, access must occur in the presence of the employee in order to identify messages of an exclusively personal nature, who could decide to delete these private messages or transfer them to another account mail

VII

The consultation also raises some questions related to the fact of keeping active for a certain time the personalized corporate email address of the working person who stops providing services to the City Council. Specifically:

- *"For how long must the active account of the personalized corporate email address of the user person who has stopped providing services be kept so that it cannot be considered an unreasonable and disproportionate period of time."*
- *"The account of the personalized corporate e-mail address can be left inactive from the day following the date on which the user ceases to provide services to the City Council"*
- *"It could be considered appropriate to the data protection regulations that the personalized corporate e-mail address can be active for a period of one month and an automatic response message is recorded in which reference is made to the fact that the person already does not provide services to the corporation and that for any issue they can contact the City Council, stating the corresponding telephone number or email address."*
- *"Once the period in which the personalized corporate e-mail address can be active has passed, it must be deleted or it must be kept blocked and, if applicable, for how long ."*

As has been advanced in section III of this opinion, from the point of view of data protection, the termination of the employment relationship must entail the cessation of the processing of the employee's personal information for part of the City Council and, therefore, also of its corporate email account, when the purpose that justifies its treatment ceases.

This is a requirement that derives from the principle of purpose limitation (article 5.1.b) RGPD), according to which *"personal data will be collected for specific, explicit and legitimate purposes, and will not be subsequently processed in a manner incompatible with said purposes ; in accordance with article 89, paragraph 1, the subsequent processing of personal data for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes will not be considered incompatible with the initial purposes".*

Principle that must be put in line with the principle of limiting the retention period (Article 5.1.e) RGPD), according to which *"personal data will be kept in a way that allows the identification of the interested parties for no longer than necessary for the purposes of processing personal data; the personal data may be retained for longer periods as long as processed exclusively for archiving purposes in the public interest, research purposes scientific or historical or statistical purposes, in accordance with article 89, paragraph 1, without prejudice to the application of appropriate technical and organizational measures that imposes this Regulation in order to protect the rights and freedoms of the interested".*

About això, according to recital 39 of the GDPR: "(...) *Personal data must be adequate, pertinent and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that their retention period is limited to a strict minimum. Personal data should only be processed if the purpose of the processing cannot reasonably be achieved by other means. To ensure that personal data is not retained for*

longer than necessary, the data controller must establish deadlines for its deletion or periodic review. (…).”

A banda d'questes principis, it is especially relevant the deletion law regulated by article 17 of the GDPR, according to which:

> *"one. The interested party shall have the right to obtain without undue delay from the data controller the deletion of the personal data that concerns them, which shall be obliged to delete the personal data without undue delay when any of the following circumstances occur:*
> *a) the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;*
> *b) the data subject withdraws the consent on which the processing is based in accordance with Article 6, paragraph 1, letter a) or Article 9, paragraph 2, letter a), and this is not based on another legal basis;*
> *c) the data subject objects to the processing pursuant to Article 21, paragraph 1, and no other legitimate grounds for the processing prevail, or the data subject objects to the processing pursuant to Article 21, paragraph 2;*
> *d) the personal data have been unlawfully processed;*
> *e) the personal data must be deleted to comply with a legal obligation established in the Law of the Union or of the Member States that applies to the data controller;*
> *f) the personal data have been obtained in relation to the offer of information society services mentioned in article 8, section 1.*
> *(...).”*

It follows from this that the controller (article 4.7 RGPD) must keep personal data for the shortest possible time and that, in determining this retention period, the purpose for which requires the processing of the data, in such a way that, once the purpose is achieved, the personal data must be deleted. It would also be necessary to take into account the obligations to retain the data for a certain period of time that may establish applicable provisions, in such a way that, once these terms have been met, that is when the personal data will have to be deleted.

As provided by the data protection regulations themselves, deletion, when relevant, does not necessarily equate to the erasure or destruction of personal information, but to its blocking.

Specifically, article 32 of the LOPDGDD establishes the following:

> *"one. The person in charge of the treatment will be obliged to block the data when it proceeds to its rectification or deletion .*
> *2. The blocking of the data consists of the identification and reservation of the same, adopting technical and organizational measures, to prevent its treatment, including its visualization, except for the provision of the data to judges and courts, the Public Prosecutor or the competent Public Administrations, in particular the data protection authorities, for the requirement of possible responsibilities derived from the treatment and only for the limitation period thereof. After this period, the data must be destroyed.*

3. The blocked data may not be processed for any purpose other than that indicated in the previous section.
4. When in order to comply with this obligation, the configuration of the information system does not allow blocking or an adaptation that implies a disproportionate effort is required, a secure copy of the information will be made so that digital or other evidence is recorded. nature, which allows to prove the authenticity of the same , the date of the blocking and the non-manipulation of the data during it.
(...).”

Therefore, personal data must be deleted once they are no longer necessary or relevant for the purpose for which they were collected or, where applicable, once the retention periods established by law have ended, which will result in its blocking during the limitation periods in which some type of liability derived from the treatment can be demanded. Upon completion of this period, which may vary depending on the information processed and the responsibilities that may be generated, the personal information must be effectively deleted.

This transferred to the case at hand, and thus answering the questions posed, implies that, in general, the deletion (and, therefore, blocking) of the personalized corporate email address of the employee who leaves rendering services to the City Council should be carried out at the time when the termination of the employment relationship occurs (it could be the day after the date on which it ceases to provide services).

However, with the aim, when appropriate, of guaranteeing the continuity of the service, it may be permissible to keep the corporate address in question "active", despite the fact that the person in charge no longer provides services to the City Council, for a certain period of time. Noting that not all jobs could justify keeping the operational address, it will depend on the position or the functions assigned to the ex-employee.

It should be borne in mind that, in any case, this action should be limited to the programming of the automatic reply message mentioned in section IV of this opinion, in which the senders of the mails are informed incoming messages that the account in question is no longer in use and the address to which messages should be addressed in the event of wanting to contact the relevant department or municipal area.

Regarding the time in which the e-mail address could be kept active for this purpose, note that there is no regulatory provision in this regard, although, in application of the principle of limitation of data conservation (article 5.1.e) RGPD), should not extend beyond the time strictly necessary to achieve the purpose of not losing relevant information for the City Council.

As a guide, please note that the Belgian Data Protection Authority recommends a period of one month in general, which could, depending on the context and the functions or position held by the former employee, be extended up to a maximum of three months (Decision issued on September 29, 2020, available on its website).

In view of this, the option proposed in the consultation consists of keeping the address active for a period of one month and recording an automatic response message informing

about the new address or contact telephone number of the person to whom to address- would be appropriate to the data protection regulations.

During this period in which the automatic reply message is in operation, the e-mail box should remain locked in such a way that its contents cannot be accessed.

In addition to all this, the inquiry asks if *"from the date on which the user ceases to provide services, the contents of the e-mail box could be downloaded and kept blocked, at the same time as unsubscribing the personalized corporate email address"* and, if yes, *"for how long this information should be kept blocked."*

The data protection regulations oblige the controller (the City Council) to block the data when it carries out its deletion (article 32.1 LOPDGDD).

In a case like the one proposed, in which it is necessary to deregister the personalized corporate e-mail address due to the termination of the employment relationship of the working person, with respect to the contents of the mailbox (the set of messages that can be contain), in order to be able to comply with this blocking obligation, it would be reasonable that for this purpose this information could be downloaded or saved by the person responsible and keep it properly blocked.

Considering that this is a tool facilitated for the development of the professional tasks of working people and given the guidelines and recommendations that these people must follow when a private use of this tool is allowed (configuration of messages, organization in folders, respecting the fixed retention period, periodically verifying those that must be deleted, possibility of recovering messages before the termination of the employment relationship, etc.), a priori in the corporate e-mail box there is no they should contain messages of a private or personal nature from the person now ex-employee, although it is also not possible to rule this out with complete certainty. The same could happen despite the fact that the corporate email account was facilitated for exclusively professional reasons.

For this reason, as an additional guarantee for the respect of the rights of the ex-employee, it would be advisable that before downloading the contents of the mailbox, a review of this was carried out in order to detect mails that, in consideration of the subject, lead to think that these are private or personal messages, or to locate mail storage folders that may have been identified as private or personal, and delete them (without accessing their content).

Having done this, and once the information has been downloaded, it must be kept properly blocked and may not be processed for any purpose, except for making the data available to judges and courts, the Public Prosecutor's Office or the competent public administrations , in particular from the data protection authorities, for the requirement of possible responsibilities derived from the treatment (article 32.3 LOPDGDD).

The period during which the blocked information must be kept may vary depending on its nature and the responsibilities that may be generated and, once fulfilled, the effective elimination of this information must be carried out (article 32.2 LOPDGDD).

VIII

The query also raises *"when a person using the mail service is temporarily disabled, in which situations and how the City Council can access the content of their personalized corporate email address."*

As highlighted in section III.2 of Recommendation 1/2013, the absence of a worker, especially if it is of long duration, can lead to problems for the continuity of the normal activity of the company, if a certain account cannot be accessed
of mail

The Authority emphasizes the need to plan - and record in the usage policy - the measures that will be adopted to guarantee continuity during the absence of this person, in such a way that it is not necessary to the employer's access to his email account due to the risk that this may entail for the rights of the working person.

Among these measures, it can be foreseen, as an example, that the working person can delete or transfer to a personal folder all private or personal messages, and authorize access to another worker, adopting the relevant changes, both at the beginning as well as at the end of the period in which the cause is removed, with regard to the change of passwords; and/or transfer the information necessary to continue the activity during your absence.

If this is not possible, for example in the case of an unforeseen absence of the worker, it is necessary that the superior body of the absent worker evaluates in a motivated way the need for the intervention for the continuity of the service (non-extendable need linked to work activity).

It is also necessary to communicate this access to the working person in advance, if possible, or later when it has not been possible (as soon as possible).

This access must be carried out in the presence or under the supervision of the higher body of the working person and, in case it has been possible to communicate with him, with his assistance or the person designated by the interested person, if he so wishes .

For this reason, messages that the employee has designated as private or stored in a folder identified as private or personal cannot be accessed under any circumstances.

IX

On the other hand, the consultation shows that, prior to the telework situation, when a person using the corporate applications was
leave was not going to work in the municipal facilities and, therefore, did not access the assigned applications from their desktop computer, but that, with telecommuting, this has changed and users can access them while on leave through the assigned corporate devices or through the internet.

This, he maintains, means that improper accesses can occur during this situation of leave and that it is necessary to carry out a follow-up of the accesses made to avoid possible leaks of information.

Given this, it raises *"when a person using the applications is in a situation of temporary absence from the provision of services, in which situations and how can the City Council monitor a period of time and access the application's access register to the which the user is authorized to access."*

Remember that it is up to the City Council, as responsible, to establish in the usage policy that it is preparing the general criteria and the appropriate rules for the appropriate use, not only of corporate e-mail, but also of its systems of 'information, which it makes available to its workers so that they act responsibly and are informed of the control that the City Council can exercise in the use of these systems.

Considering that the City Council must be able to demonstrate that the processing of data through its information systems complies with data protection regulations (Article 5.2 RGPD), it must be recognized the possibility of carry out, through the persons designated for this function, the control and monitoring tasks that are necessary in the common infrastructures and in the workstations assigned to their staff in order to check and verify that the use of the information systems and corporate applications conforms to the usage policy and does not generate security incidents.

Point out that this type of control must be proportional to the type of risk that may arise from the misuse of the information systems for the City Council or third parties by all those people who have authorized access to the information systems 'information (it should not be a measure designed only for workers who are providing services in the telework modality and who are absent due to sickness or other reasons).

In view of this, the City Council could establish in the policy of use the limitations on the use of e-mail and in the other information systems that must be introduced during the period in which you are on leave, which, with the purpose to guarantee the proper functioning of the information systems and to monitor their appropriate use by its staff, it has tools and means of control to supervise and monitor this, which, for example, allow to register the 'access to information systems by its users (user identification, day, time, resource accessed and reason for access), and the period of time in which the control information will be reviewed recorded (for example, once a month).

It would also be convenient for the possible consequences in the case of the existence of indications of a misuse of the information systems by the workers, to breach the rules.

X

Finally, the consultation asks if *"when a user stops providing services to the City Council, he can request a copy of the emails from his personalized corporate email address."*

Regarding emails of a private or personal nature, as we have seen, it would be necessary to facilitate the access of the working person before his final departure from the workplace, although, in the face of a subsequent request for access to this information,

there should not, a priori, be any inconvenience from the point of view of data protection, given that it would be information to which he could have access in the exercise of his right of access to the information that it is his own, in the terms of article 15 of the RGPD.

With regard to professional emails, article 15 of the RGPD would allow access to data directly linked to the employee (or better to their status as the person sending or receiving the message) but on the other hand it does not seem to be able to cover the access to information of third parties that may appear in said emails.

With regard to this information, it must be borne in mind that it would be information that would be in the possession of the City Council as a result of the exercise of the functions entrusted to the person requesting access. Therefore, it would be public information for the purposes of article 2.b) of Law 19/2014, of December 29, on transparency, access to public information and good governance (hereafter, LTC), and , consequently, subject to the regime of the right of access (article 18 LTC).

Article 18 of the LTC recognizes the right of people to *"access public information, referred to in article 2.b, individually or in the name and representation of any legally constituted legal person* " (paragraph 1).

However, it should be borne in mind that this right of access is not absolute and may be denied or restricted for the reasons expressly established in the laws. For the relevant purposes, it must be borne in mind that the requested professional emails will contain information belonging to the former employee, to which he could have access on the basis of article 15 of the RGPD, but also and mainly information from third parties people This would oblige to keep in mind the limitations and criteria provided for in the transparency legislation (articles 23 and 24 LTC), and the principles of the regulations for the protection of personal data.

To point out, at this point, that this Authority has had the opportunity to examine the eventual access and obtaining a copy of professional emails by a former employee of a local entity in the IAI report 2/2021 , available on the Authority's website.

As stated in this report, with regard to the functions attributed to the ex-employee, we could find ourselves in front of information that could be of a different nature and affect to a greater or lesser degree the privacy of the people it serves reference

At the outset, the applicant's access and obtaining a copy of professional emails containing specially protected personal data of third parties, once their employment relationship with the City Council has ended, should be in any case limited on the basis of what is provided for in articles 23 of the LTC and 15.1 of *Law 19/2013, of December 9, on transparency, access to public information and good governance* (LTC)).

But beyond that, the content of these professional emails could also contain data deserving of a special reservation or confidentiality in view of the concurrence of certain qualified circumstances (for example, situations of social vulnerability, data of minors, data related to gender violence, etc.) or in attention to the nature of the matters dealt with by the ex-employee according to their assigned tasks or functions (members of the local police, staff of the social services area, etc.).

It should also be borne in mind that the intended access could affect a large volume of people. Although the number of people affected is not actually a decisive criterion when it comes to being able to limit access, it must be taken into account that when the people affected are very numerous, this can lead to a series of problems in being able to attend to the sun request for access with the appropriate guarantees, in particular, grant the hearing procedure provided for in article 31 of the LTC and assess, case by case, whether the protection of personal data or the right to access of the person claiming.

A reasoned weighting between the different rights and interests at stake that would need to be done in accordance with article 24.2 of the LTC, would require taking into account this circumstance that may lead to a denial of access to this information in the event of no the relevance that it may have for the person requesting to have this information is sufficiently proven.

Although it is not mandatory to include in the request the reasons for which access is requested (articles 18.2 and 26.2 LTC), if you do not do so, this element cannot be taken into account when assessing the different rights and interests at stake. Thus, if no specific reason is given, the access should be understood as framed within the purpose of the transparency law itself (article 1.2 LTC).

For all this, in general, it would not appear as justified, from the point of view of data protection, the obtaining in a generalized way by a former employee of a copy of the set of professional e-mails. This, without prejudice to the fact that in some specific case the access and obtaining a copy of certain e-mails could be justified in view of the circumstances or specific reasons that could be alleged (for example, in the case of information necessary for your right of defence).

In addition to all this, it should be noted that the LTC does not establish any time limit regarding the conservation of public information and documentation, for the purposes of guaranteeing the exercise of the right of access (article 18 LTC). Therefore, it is not mandatory to keep the information that is available to respond to eventual requests for access, beyond the retention periods provided for in the provisions that apply to the specific case.

In this case, as we have seen, the termination of the employment relationship must lead to the deletion of the employee's corporate email account, which must lead to its blocking, in the terms of the article 32 of the LOPDGDD and with the particularities indicated in legal basis VII.

As this Authority has highlighted in the IAI 6/2022 report (available on the web), the blocking of personal information should not void the possibility of exercising other rights, such as the right of access to public information, under the terms of the transparency legislation.

The communication of blocked data in this case would have the purpose of complying with an obligation of the person in charge, based on the Constitution (art. 105.b) EC) and the LTC, therefore, as was highlighted in the opinion CNS 76/2016 (available on the web), could be lawful on the legal basis of article 6.1.c) of the RGPD.

Once the relevant information blocking period has been completed, the e-mails must be effectively deleted.

Therefore, to point out that the attention of an eventual right of access (and obtaining a copy) of a former employee in relation to emails can be carried out while the City Council has this information public

Conclusions

The policy for the use of information systems and digital devices that the City Council is preparing must include clear rules on the management of the personalized corporate email account, and on access to the information it contains, both on the grounds of termination of the employment relationship as in case of temporary absence of the working person, taking into account the considerations made in sections III to VIII of this opinion.

It must also include specific provisions regarding the appropriate use of information systems by its staff and the control that the City Council can carry out to guarantee their security and proper functioning.

With regard to requests for access and obtaining copies of e-mails by former employees, the observations made in section X of this opinion must be taken into account.

Barcelona, December 12, 2022