apdcat
Autoritat Catalana de Protecció de Dades

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

File identification

Resolution of sanctioning procedure no. PS 28/2020, referring to the Provincial Council of Barcelona.

Background

1. On 31/07/2019, the Catalan Data Protection Authority received a letter from an employee of the Temporary and Temporary Housing Services and RESPIR (hereinafter, Respir) and from a trade union , for which they filed a complaint against the Diputació de Barcelona (hereafter, DIBA), on the grounds of an alleged breach of the regulations on the protection of personal data. Specifically, the complainants stated the following:

- That, on 09/21/2018, Respir's (...) sent an email to 65 recipients in which a claim was attached that had been submitted by the daughter of a Respir user that contained , among other personal data, data relating to the latter's health and which also identified certain people employed by Respir.

- That this shipment was made without encrypting the data contained in the claim. This action would contravene the manual for the use of DIBA's information systems.

ÿ That the email was sent to the corporate address of two people who
they were retired and at the non-corporate address of an external psychiatrist
- That on 10/12/2018 a face-to-face training action was held on data protection in which there were staff who could not attend or who had to be absent due to not having covered their duties.
- That on 05/25/2018, the DIBA temporarily appointed a certain person as data protection delegate, an appointment that was not communicated to the Authority. Neither would the appointment of a new person as DIBA's data protection delegate, which took place on 02/18/2019, be communicated within the 10-day period provided for that purpose.

The complainants provided various documentation, including the 1/2019 report drawn up by the data protection officer in relation to the sending of the aforementioned email.

2. The Authority opened a preliminary information phase (no. IP 225/2019), in accordance with the provisions of article 7 of Decree 278/1993, of November 9, on the sanctioning procedure of application to the 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 they were likely to motivate the initiation of a sanctioning procedure, the identification of the person or persons who could be responsible and the relevant circumstances involved.

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

3. In this information phase, on 15/10/2019 the reported entity was required to report, among others, on the reasons for which the claim was forwarded to several people linked to Respir; if, prior to 09/21/2018, a risk analysis had been drawn up regarding the sending of emails; as well as the measures that were implemented on 09/21/2018, to guarantee the security of the data that was communicated via email, and in particular, when these were related to health.

4. On 10/28/2019, the DIBA responded to the above-mentioned request in writing, in which it set out, among others, the following:

- That the working procedure for the management of complaints determines that when a claim is received from a user, it will be informed and channeled to the responsible person who belongs depending on the professional field that is related to it, with communication to the management team of the affected residential program, to the Head of the Care Management Office and to the Management, as well as to the person responsible for the service provided in order to initiate investigations into the facts and make a report to give an answer to the person who requested the complaint, claim or suggestion.
- That the purpose is always to find out the facts that are exposed, detecting and contacting them professionals who have had some intervention in them.
- That the disputed claim revealed possible malpractice by the medical and health team of the care center (including in some paragraphs the team of auxiliaries was pointed out) and was addressed to the health managers.
- That whoever assumed the management of this complaint considered it necessary to make the claim known to the health care personnel likely to have attended to the person to whom the claim referred (with different shifts and time distributions of work). To this end, 64 people out of the 500 employees were identified as those who could have potentially had healthcare and/or clinical contact with the user.

ÿ That the email addresses in the email message came from a distribution list that included the email addresses of professionals from the health support functional unit, people assigned to different jobs (doctors and nurses), different work shifts, and different legal regimes, who were likely to have information regarding the case to be resolved and who could provide evidence or arguments to address it and prevent a conflict situation with the family. This communication channel is very efficient when it comes to sharing information with a large number of people who work in the center.

- That in cases of retirement, the current corporate protocol normally keeps the operational electronic address only for a period of 15 days following the end of the employment relationship. Analyzed these two cases, despite sending the mail to their corporate electronic addresses, these were not valid and therefore the recipients did not receive the reference email.

ÿ That all the professionals who received the message were those who identified themselves as likely to have intervened at some point in their clinical practice in the

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

situations presented in the claim, as detailed in the same in the "reason for claim/complaint" section.
- That the recipients were 64, even though 65 electronic addresses were sent, since there was one recipient to whom it was sent to two addresses.
- That a risk analysis had not been drawn up on this matter before 21/09/2018.
- That the only reference in relation to the sending of e-mails is the regulation of the use of institutional information and communication systems. Specifically, articles 11 and 17 of the Barcelona Provincial Council's Information and Communication Systems User Manual (MUSICDB). This Manual establishes guidelines for the Corporation's staff on the use of corporate systems.
- That all DIBA e-mail boxes are encrypted and the protocol is used cryptographic TLS to have secure communications over the network.
- That when it is necessary to transmit data relating to users to agents of external organizations, they are encrypted in order to protect them.

The reported entity attached various documentation to the letter.

5. As part of the previous information, it was verified through the Authority's data protection delegate register, that the first communication from a data protection delegate by the DIBA was on 03/12 /2019, communication that the DIBA amended on 03/20/2019 given that he had not used the form provided for the purpose.

6. On 08/06/2020, the director of the Catalan Data Protection Authority agreed to start a disciplinary procedure against the DIBA for 2 alleged infringements: an infringement provided for in article 83.5.a), in relation to articles 5.1.a, 6 and 9; and another offense provided for in article 83.4.a) in relation to article 32; all of them from Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, relating to the protection of natural persons with regard to the processing of personal data and the free movement thereof (hereinafter, RGPD). This initiation agreement was notified to the imputed entity on 07/01/2020.

7. The initiation agreement explained the reasons why no imputation was made with respect to other facts reported.

Firstly, with respect to the training action of 10/12/2018, given that it was not observed that the impossibility of several people to participate in a specific training action on data protection resulted in an infringement of the regulations on data protection.

Secondly, with regard to the communication of the designations of a data protection delegate, although the DIBA did not communicate to the Authority the designation of the person who was to exercise the functions of the data protection delegate data with effect from 05/25/2018,

this eventual non-compliance was considered not to have the entity sufficient to impute it as such an infringement in a sanctioning procedure taking into account that, on 03/12/2019, the DIBA notified the Authority of the appointment of a new data protection officer. And, in any case, the eventual violation provided for in article 83.4 RGPD, which typifies as such the violation of "the obligations of the person in charge and of the person in charge pursuant to articles 8, 11, 25 to 39, 42 and 43 " (among which there is the one provided for in article 37 RGPD) was already prescribed.

And, thirdly, regarding DIBA's designation of another person as data protection delegate on 02/16/2019, it was indicated that DIBA did not notify the Authority of this new designation until 12/03/2019, breaching the 10-day deadline set for the purpose by Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (LOPDGDD). However, the LOPDGDD has only classified as an infringement, the breach of the obligation to notify the control authority of the appointment of the data protection delegate, but not the breach of the 10-day period provided for in the effect if this communication has already been made, which is why no type of responsibility could be demanded from DIBA for having delayed this communication beyond this deadline, especially if you take into account that the deadline established only it was exceeded in a few days.

8. On 14/07/2020, the DIBA made objections to the initiation agreement. The accused entity provided various documentation with its letter that has been included in the file.

9. On 14/10/2020, the person instructing this procedure formulated a proposed resolution, by which it proposed that the director of the Catalan Data Protection Authority admonish DIBA as responsible, in the first place, for an infringement provided for in article 83.5.a) in relation to the article 5.1.c); and secondly, of an infringement provided for in article 83.4.a) in relation to article 32, all of them of the RGPD.

This resolution proposal was notified on 10/20/2020.

10. On 09/11/2020, the accused entity presented a statement of allegations and provided various documentation.

proven facts

1. On 09/21/2018, Respir's Customer Service Area sent by email the complaint (Complaint (...)) that the daughter of a Respir user submitted on 20/09/2018. In that complaint, which referred to the eventual "malpractice of the team that took care of my father during the first two weeks of his stay in the residence (doctor, nurse, auxiliaries) and especially the nurse with whom tengo la entrevista de ingreso", identified certain people employed by Respir who had served both the person making the complaint and the user. In turn,

this complaint contained data of the person making the complaint (name and surname, ID, telephone, email address or handwritten signature) and of the user (in particular, data relating to their health - including images of a sore or ulcer-).

The email was sent to 65 email addresses corresponding to 64 people who, according to the DIBA, could have had healthcare and/or clinical contact with the user.

Among the recipients of said mail was even a psychiatrist (to whom said mail was sent to two different non-corporate addresses) despite the fact that there was no element in the content of the complaint that would allow it to be inferred that it referred to some performance of this professional.

2. For an indeterminate period, but in any case until 09/21/2018, a risk analysis had not been carried out to determine the appropriate technical and organizational measures to guarantee the security of the data sent through e-mail.

Fundamentals of law

1. The provisions of the LPAC, and article 15 of Decree 278/1993, according to the provisions of DT 2a of Law 32/2010, of October 1, of the Catalan Data Protection Authority. In accordance with articles 5 and 8 of Law 32/2010, the resolution of the sanctioning procedure corresponds to the director of the Catalan Data Protection Authority.

2. The accused entity has made allegations both in the initiation agreement and in the resolution proposal. The first ones were already analyzed in the proposed resolution, but even so it is considered appropriate to mention them here, given that they are partly reproduced in the second ones.
The set of allegations made by the accused entity are then analysed.

2.1. About the fact imputed first.

In the 1st section of its statement of objections, the accused entity reiterates that all of the people to whom the mail containing the disputed complaint was sent (64 people) were health personnel who could have been in contact with the user and their relatives, but points out that finally 18 health professionals participated directly in the investigation and resolution of the complaint. In this sense, the DIBA accepts in its letter of allegations, that the scope of the communication of this data could have been minimized, so that the full complaint could have been sent to these 18 health professionals. However, he considers that the fact that the complaint was sent to only 64 health professionals out of a total of 500 professionals (of which 259 are health professionals) instead of sending it exclusively to the 18 health professionals who participated in the investigation of the complaint, it should not be a reason for reprimand, especially taking into account the measures taken by the DIBA after the fact.

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

As indicated by the instructing person in the resolution proposal, and as the accused entity also acknowledges, in order to achieve the purpose of handling the complaint it was not necessary to send a copy of the written complaint to the entire health team (64 people) that could potentially have served the user or his daughter. More if you take into account that the complaint, among others, contained data relating to the user's health, identification and contact data of the person who made the complaint and in which certain people employed by Respir were identified who had served both the person making the complaint and the user.

Indeed, this purpose could have been achieved by simply informing the Respir staff who could have attended to the user, that a complaint had been submitted in relation to the assistance provided to the user and the attention to his daughter , without the need to send the full content of the complaint to the center's 64 health professionals. Another thing is that once the employees involved in the action that is the subject of the complaint have been identified, they can access all the content, if this becomes necessary to achieve the intended purpose.

It is worth noting that in the report issued by the data protection representative regarding the claim addressed to him in relation to the facts that were the subject of a complaint, he recommended that, in cases where a complaint is received, "use only the data strictly necessary for the identification of the episode or clinical-care course of the user and, once the care personnel who have effectively intervened have been identified, proceed, if necessary, with their sending (...)" .

Also, as highlighted in the resolution proposal, in the procedure for handling complaints, claims, suggestions and thanks, approved by the DIBA's Customer Service Area, it was only contemplated (in the current version at the time of the events) the communication of the complaint to the person in charge of the service provided in order to initiate investigations into the events that occurred and make a report to give an answer to the person who has urged the complaint, but at no time was it foreseen no further referral of the complaint.

In this regard, in its statement of objections to the proposed resolution, the DIBA admits that the sending of the full complaint could have been limited to only 18 health professionals (instead of the 64 to which it was sent) . Indeed, if these 18 people were involved in the action of the complaint, this would have been adjusted to the principle of data minimization.

Having said that, it should be noted that the penalty for these facts that are considered to violate the principle of data minimization does not depend on the number of people to whom the full complaint was sent and who were not involved in the facts that are the subject of the complaint . In any case, this circumstance that the DIBA invokes (that the full complaint was sent to 64 health professionals, instead of the 500 professionals that the center claims to have) could be taken into account in order to graduate the economic amount of the penalty in case this

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

consisted in the imposition of an administrative fine, in accordance with what is established in article 83.4 of the RGPD.

However, in the present case the sanctioning regime applicable to the DIBA does not provide for the imposition of a financial penalty, but rather a warning in accordance with the provisions of article 77 of the LOPDGDD, which by its very nature is not subject to graduation.

Next, for the specific case of the referral of the complaint via e-mail to a psychiatrist, the DIBA indicates that this person was a professional who was part of the medical team and describes some of her duties.

As the instructing person pointed out in the resolution proposal, the complaint focused on the care given to the father of the person making it during the first two weeks of his stay at Respir. And specifically, in the fact of not having given his father "personalized attention in accordance with his needs (difficulties in voluntary mobility and passive mobilization due to spastic paraparesis disease)". And the person making the complaint focused on the performance of a certain doctor, the
auxiliary staff who cared for his father, and nursing staff (and in particular, a certain nursing professional). Specifically, in the complaint the person who formulated it identified 5 Respir professionals.

Thus things, neither the circumstances of the case nor any of the extremes set out in the complaint allowed us to infer that this referred to an action by the psychiatrist.

Proof of the above is that, in its statement of objections to the proposed resolution, the DIBA also does not consider that the psychiatrist was one of the 18 health professionals involved in the action complained of.

On the other hand, the DIBA also highlights in its statement of objections to the proposed resolution that, in the report issued by the DIBA's data protection officer on 04/05/2019 the previous claim contained a series of recommendations that were implemented on 05/20/2019; as well as that on 10/30/2020 the corrective measures proposed by the instructing person in the resolution proposal were also implemented.

In this respect, it is appropriate to highlight and positively assess the diligent action of the DIBA, in particular, when implementing the corrective measures that were proposed to correct the effects of the infringement regarding the principle of data minimization.

Without prejudice to the above, it is necessary to point out that the adoption of measures to correct the effects of the infringement do not distort the imputed facts, nor do they modify their legal qualification.

In the last one, the DIBA also refers to the legality of the treatment consisting of managing that, as indicated in the resolution proposal, would be legal. And for this reason, the investigating person already estimated in the resolution proposal that it was necessary to modify the legal classification of the fact proven first, which in the initiation agreement was incardinated in the violation of the principle of legality, to qualify it as a violation of the minimization principle.

2.2. About risk analysis.

In relation to the 2nd fact that was imputed in the initiation agreement, the DIBA states that it has located the risk analysis carried out on 04/19/2015 "at the time" of the Manual of Use of the Systems Information and Communication of the Provincial Council of Barcelona (MUSICDB).

In advance, it should be noted that the DIBA admitted in its statement of objections to the initiation agreement that "a risk analysis has not been formalized" to determine the appropriate technical and organizational measures to guarantee the safety of the data that was sent via email, as I had already explained in writing dated 10/25/2019, in response to this Authority's request in the framework of the prior information phase.

As has been advanced, in the hearing process before the resolution proposal, the DIBA has provided a risk analysis carried out on 04/19/2015.

The first thing to highlight is that this risk analysis is part of the DIBA's adaptation to the National Security Scheme (hereafter, ENS) approved by Royal Decree 3/2010, of 8 January.

It must be admitted that the first additional provision of the LOPDGDD (norm that was not in force during the period of time to which proven fact 2n refers) has determined that the responsible persons listed in article 77.1 of the LOPDGDD (among which there is the DIBA) must apply to the processing of personal data the security measures that correspond to those foreseen by the ENS. But the LOPDGDD (in force since 07/12/2018) has also provided for the revision of the ENS (which has not yet taken place) in order to include the measures that must be implemented in case of treatment of personal data to avoid its loss, alteration or unauthorized access, with the adaptation of the risk determination criteria in the processing of data to that established in article 32 of the RPGD. This need to review the ENS that contemplates the LOPDGDD due to the fact that the ENS is not adapted to the criteria for determining the risk of personal data in accordance with article 32 of the RGPD, already allows progress that with the risk analysis in accordance with the ENS that has been provided, does not comply with the provisions of article 32 of the RGPD.

The ENS (art. 27) establishes that the security measures indicated in Annex II must be applied by the Public Administrations taking into account the following: a) the assets that make up the system; b) the category of the system (in accordance with art. 43 ENS) and; c) the decisions taken to manage the risks identified.

By virtue of the above, the ENS risk analysis that has been provided focuses on the security of information systems (specifically software applications, hardware platforms and other infrastructure), but it does not take into account all the risks that arise specifically from the processing of personal data (such as from the sending of e-mails containing special categories of data).

As an example, in the ENS risk analysis of 04/19/2015, it is indicated that one of the events (E.19) that can cause a risk of disclosure of information on the Exchange platform are errors and unintentional failures. And with regard to the confidentiality dimension of this event, it is pointed out that the impact is "M" (medium), without it being noted that the type of personal data that was used as a criterion for determining the risk may be affected. In this regard, the data that have the status of special categories cannot have the same impact on confidentiality as those that do not. Indeed, if the disclosure affected special categories of data, its impact would be high (that is, it should have an approximate value of "9" or "10" according to the risk map used in said analysis).

At this point, it should be noted that also article 27 of the ENS contemplates that "When a system affected by this royal decree handles personal data it will be applied as provided for in Organic Law 15/1999, of 13 of December, and development regulations, without prejudice to the requirements established in the National Security Scheme."

And section 5.7.1 on protection measures affecting personal data of Annex II of the ENS (regarding security measures) provides that "When the system processes data of a personal nature, se estará a lo dispuéto in Organic Law 15/1999, of December 13, and development rules, without prejudice to complying, in addition, with the measures established by this royal decree."

Therefore, the ENS refers to the regulations on data protection (referral that must be understood as made to the RGPD) when the system processes personal data, regulations that provide for the need to carry out an analysis of the risks that present the processing of personal data based on the determination criteria contemplated in article 32 of the RGPD.

That being the case, the guarantee of the security of personal data is not limited exclusively to the area of information security to which the ENS currently refers, but it is also necessary to take into account the criteria for determining the risk in the processing of the data (art. 32.2 RGPD).

In accordance with the above, aside from applying the security measures that derive from the ENS, the DIBA also had to assess what are the appropriate measures to guarantee the security of personal data. Indeed, in order to determine whether to ensure data security, additional measures should be implemented to those that apply in accordance with

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

the ENS, or, if these measures are already adequate, the said risk analysis must take into account the risks presented by the treatment, as established in article 32 of the RGPD.

Regarding the risk analysis referred to in article 32 of the RGPD, in opinion CNS 7/2019, this Authority stated the following:

> "From the point of view of information security, a risk analysis requires identifying the threats (for example, unauthorized access to personal data), assessing the probability that it will occur and the impact it would have on people affected
>
> The type of risk and, in short, its probability and severity, varies according to the types of treatment, the nature of the data being treated, the number of interested persons affected, the amount and variety of treatments, the technologies used, etc.
>
> In the case of treatments of little complexity, this analysis can be the result of a documented reflection on the implications of the treatments on the rights and freedoms of the persons concerned. This reflection must analyze the context in which the treatment is carried out (media, facilities, users, etc.) and must answer questions such as the type of data they deal with (special categories of data, col· vulnerable groups, of a large number of people, which allow the creation of profiles), if the disclosure, alteration or loss of the data may have significant consequences for the people affected, if the data is processed outside the equipment or installation locations of the person in charge, if third parties who provide services on behalf of the person in charge have access to the data, and technologies that are particularly invasive to privacy are used (geolocation, video surveillance, internet of things, etc.)."

So, from the perspective of the regulations on data protection, the risk analysis must take into account, among others, the threats to the treatment, the impact on the people affected (the ENS has taking into account the impact on the security of information or services) or the type of risk, taking into account the type of data, the number of people affected or the variety of treatments, among others.

Without prejudice to what has been explained so far, it is worth saying that after the date on which it was approved (19/04/2015) the risk analysis according to the ENS that is now provided, the ENS it was modified by Royal Decree 951/2015, of 23 October. This rule, among others, updated Annex II of the ENS referring to security measures. Therefore, this risk assessment carried out in compliance with the ENS, would even have become obsolete. Indeed, the measures determined to adapt to the ENS on 04/19/2015 have not been subject to periodic reassessment and updating, in order to adapt their effectiveness to the constant evolution of risks and protection systems, as required by article 9 of the ENS.

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

And, in particular, once the RGPD became applicable (from 25/05/2018) the DIBA did not carry out any assessment to determine if the security measures it had implemented until then were adequate to the risks presented by the treatments.

On the other hand, the DIBA states in its statement of objections to the proposed resolution that the MUSICDB, approved in 2015 (before the RGPD was approved), "was designed and approved from in accordance with the regulations in force in the field of data protection (Royal Decree 1720/2007, of December 21, which approves the Regulations for the development of Organic Law 15/1999, of December 13, on the protection of data of a nature personal [hereafter, RLOPD]) and security (Royal Decree 3/2010, of January 8, which regulates the National Security Scheme in the field of Administration
Electronics)". Likewise, the DIBA also claims that the MUSICDB incorporates, among others, rules on the use of e-mail.

Well, regardless of whether the rules described in the MUSICDB can be considered to be appropriate security measures to guarantee the security of personal data, as already explained, a risk analysis must be carried out in the terms provided for in article 32 of the RGPD, which must be documented, in order to determine if these measures are sufficient or if there is any deficiency.

As the DIBA indicates in its statement of objections, it must also be taken into account that the MUSICDB was approved taking into account the RLOPD, which established a series of security measures which, in the nature of required minimums, were to be applied to the treatments depending on the level of security applicable to them (basic, medium or high).
With the application of the RGPD, it is left to the discretion of the person responsible for the treatment and the person in charge, after assessing the risks, to determine which security measures need to be implemented in each case.

In accordance with the above, as has been advanced, from the application of the RGPD the DIBA had to analyze in each case, if the security measures implemented were sufficient or if it was necessary to modify them , through an analysis of risks derived from the treatment as established in article 32 of the RGPD, an analysis that the DIBA did not carry out.

Finally, in its statement of objections to the proposed resolution, DIBA informs that in March 2020 it awarded two companies certified in the ENS, a contract to review the adaptation to the ENS and to carry out a new risk analysis of services related to Respir centers.

In this regard, as the instructing person did in the resolution proposal, the action of the DIBA must be highlighted in order to carry out the corresponding actions that must end with the completion of a risk analysis and therefore, correcting the effects of this infringement. However, in order for the risk analysis that is the subject of the contract to consider that the effects of the infringement are corrected, the

provided by article 32 of the RGPD and, in particular, the risks presented by the treatments of personal data.

For all the above, the allegations made by the DIBA against the proposed resolution must be rejected.

3. In relation to the facts described in point 1 of the proven facts section, it is necessary to refer to article 5.1.c) of the RGPD, which regulates the principle of data minimization determining that personal data will be " adequate, relevant and limited to what is necessary in relation to the purposes for which they are treated".

As indicated by the person instructing, during the processing of this procedure the fact described in point 1 of the proven facts section, which is constitutive of the infraction provided for in article 83.5.a) of l 'RGPD, which typifies the violation of the "basic principles of treatment, including the conditions for consent pursuant to articles 5, 6, 7 and 9", among which the principle of minimization is contemplated.

4. With regard to the fact described in point 2 of the proven facts section, it is necessary to go to article 5.1.f) of the RGPD, which regulates the principle of integrity and confidentiality, according to which personal data will be "treated in such a way as to guarantee adequate security of personal data, including protection against unauthorized or illegal processing and against accidental loss, destruction or damage, through the application of appropriate technical or organizational measures".

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

> "1. Taking into account the state of the art, the costs of application, and the nature, scope, context and purposes of the treatment, as well as risks of variable probability and severity for the rights and freedoms of natural persons, the person responsible and the treatment manager will apply appropriate technical and organizational measures to guarantee a level of security adequate to the risk (...).
> 2. When evaluating the adequacy of the level of security, particular consideration will be given to the risks presented by data processing, in particular as a result of the accidental or unlawful destruction, loss or alteration of personal data transmitted, stored or otherwise processed, or unauthorized communication or access to said data. (...)"

This implies that, since the RGPD is applicable, an assessment of the risks involved in each treatment must be carried out, to determine the security measures that need to be implemented.

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

In accordance with what has been presented, as indicated by the instructing person, the fact recorded in point 2 of the section on proven facts constitutes the violation provided for in article 83.4.a) of the RGPD, which typifies the violation of "the obligations of the person in charge and the person in charge pursuant to articles 8, 11, 25 to 39, 42 and 43", among which there is that provided for in article 32 RGPD.

5. Article 77.2 LOPDGDD provides that, in the case of infractions committed by those in charge or in charge listed in art. 77.1 LOPDGDD, the competent data protection authority:

> "(...) must issue a resolution that sanctions them with a warning. The resolution must also establish the measures to be adopted so that the conduct ceases or the effects of the offense committed are corrected.
>
> The resolution must be notified to the person in charge or in charge of the treatment, to the body to which it depends hierarchically, if applicable, and to those affected who have the status of interested party, if applicable."

In terms similar to the LOPDGDD, article 21.2 of Law 32/2010, determines the following:

> "2. In the case of violations committed in relation to publicly owned files, the director of the Catalan Data Protection Authority must issue a resolution declaring the violation and establishing the measures to be taken to correct its effects . In addition, it can propose, where appropriate, the initiation of disciplinary actions in accordance with what is established by current legislation on the disciplinary regime for personnel in the service of public administrations. This resolution must be notified to the person responsible for the file or the treatment, to the person in charge of the treatment, if applicable, to the body to which they depend and to the affected persons, if any".

By virtue of this power, the DIBA should be required to carry out a compliance risk analysis as soon as possible, and in any case within a maximum period of 2 months from the day after the notification of this resolution with article 32 of the RGPD, to determine the appropriate technical and organizational measures to guarantee the security of the data sent by email.

Once the corrective measure described has been adopted, within the specified period, the DIBA must inform the Authority within the following 10 days, without prejudice to the Authority's inspection powers to carry out the corresponding checks.

On the other hand, in relation to proven fact 1, the DIBA has certified that it has modified the procedure for managing complaints, claims, suggestions and thanks, approved by the DIBA's People Service Area, in the terms which were indicated in the resolution proposal in order to collect that in the "case of receiving a complaint regarding a person

user in which it is necessary to identify the personnel who could be responsible (so as not to identify the person making the complaint), the employees who could potentially have intervened in the action that is the reason for the complaint will be notified, the name and surnames of the affected user (without referral of the complaint) and a succinct explanation of the reason for the complaint." As things stand, the DIBA has implemented the measure proposed by the instructing person in the proposed resolution, which is why it is unnecessary to require any other corrective measure in this regard.

resolution

For all this, I resolve:

1. Admonish the Provincial Council of Barcelona as responsible for two infractions: an infraction provided for in article 83.5.a) in relation to article 5.1.c); and another violation provided for in article 83.4.a) in relation to article 32, all of them of the RGPD.

2. To require the DIBA to adopt the corrective measure indicated in the 5th legal basis and certify to this Authority the actions taken to comply with it.

3. Notify this resolution to the DIBA.

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

5. Order that this resolution be published on the Authority's website (apdcat.gencat.cat), in accordance with article 17 of Law 32/2010, of October 1.

Against this resolution, which puts an end to the administrative process in accordance with articles 26.2 of Law 32/2010, of October 1, of the Catalan Data Protection Authority, and 14.3 of Decree 48/2003 , of February 20, by which the Statute of the Catalan Data Protection Agency is approved, the imputed entity can file, with discretion, an appeal for reinstatement before the director of the Catalan Data Protection Authority Data, within one month from the day after its notification, in accordance with what they provide
article 123 et seq. of the LPAC. You can also directly file an administrative contentious appeal before the administrative contentious courts, within two months from the day after its notification, in accordance with articles 8, 14 and 46 of Law 29/1998, of July 13, regulating the administrative contentious jurisdiction.

If the imputed entity expresses to the Authority its intention to file an administrative contentious appeal against the final administrative decision, the decision will be provisionally suspended in the terms provided for in article 90.3 of the LPAC.

Likewise, the imputed entity can file any other appeal it deems appropriate to defend its interests.

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

The director,