File identification

Resolution of sanctioning procedure no. PS 32/2022, referring to the Mentally Ill Foundation of Catalonia.

Background

1. On 10/12/2020, the Authority received a complaint made by three people ((...), (...) and (...)) against the Mentally Ills Foundation of Catalonia (in hereinafter, FMMC), due to an alleged breach of the regulations on the protection of personal data. Specifically, the complainants, (...), exposed the following facts that they considered contrary to the regulations, which took place in the month of September 2020, as part of an audit of the information systems that the 'entity had commissioned an external company hired for the purpose ((...)), and which would have resulted in a " *security incident (IN-061").*

a) That (...)(...)((...)) had provided at the end of August to (...) two specific users (one for each auditor) with system administration rights, with which they could remotely access the FMMC's systems via VPN to carry out the assigned audit work; but these users were disabled when the person responsible went on vacation. The complainants complain that, faced with this circumstance, the management of the FMMC, instead of proceeding to re-enable the specific users that had previously been provided to the auditors, facilitated, without the knowledge of the persons responsible for (...)(...)of the FMMC, "the generic administrator user" of the domain in (...), so that they could access the systems with the highest privileges, as he did.

b) That (...), without the knowledge of those responsible for (...), and bypassing the perimeter security of the FMMC, installed a " *hardware in the facilities to connect from the outside bypassing the security of the FMMC, and, through the password of the Administrator user, given by (...), to be able to perform the tasks they needed"* . The complainants state that the security protocol of the FMMC expressly prohibits remote access to the system through the generic administrator user, that is to say that *"this special user can only be used from within the Foundation's network : for security reasons it cannot be used to enter the Foundation's systems from the outside"* . In short, the complainants claim that, to the extent that the security system implemented by the FMMC did not allow remote access through the administrator user - through VPN (which was the remote access system foreseen)- in the information systems, (...) installed the mentioned hardware to be able to connect remotely through the administrator user.

c) That, as a result *of "the intrusions into the information systems"* detected (by the whistleblowers) for having noted access with the generic administrator user, the management, without the intervention of those responsible (...) *"orders the company to performs the audit (and presumably the author of the intrusions) to carry out an investigation and to change the keys of all the users of the organization (...) thus managing all the credentials of the organization and blocking the access of users on the systems at least during the weekend"* . In view of this blockage, FMMC workers had to call (...) so that this company could provide them with a new password to be able to access the systems. The complainants state that at no time was the staff informed that for security reasons they had to proceed immediately to change the password provided by (...). Moreover, they state that

when they warned (...) of this fact, they were told *that "they did not have this practice, that everyone could change it (the password) whenever they wanted, that they were professionals and obviously they would never enter a user's account".*

d) That, during the period during which Mr. (...)he did not have access to the systems (around the second half of September 2020 and until 01/10/2020 when he regained it), *"there is evidence of logins on his computer of work and access to management software using their credentials".*

The complainants added that the management of the FMMC addressed the "Type Code" of the Unió Catalana d'Hospitals (UCH) -to which the Foundation is a member-, a query about the events that happened in order to proceed to close the incidence, but that the management omitted relevant information when exposing the case to the UCH.

The complainants, along with their complaint, provided the following documentation:

- *"Security incident report dated 18/09/2020",* drawn up on 29/09/2020 by (...) who, (...). This report contains a chronology of the events that, in his opinion, would have resulted in a security incident (" *IN-061* "). This report, among others, includes the copy of several emails exchanged between the managers of (...)(...)((...) and (...)) and between them and the management of the FMMC.

- Copy of the response that the UCH (Type Code) gave to the FMMC in relation to the query that the entity raised regarding the security incident. This report contains the following text:

"CONSULT:
Due to some events that happened, I have doubts about the appropriateness of closing the security incident.
An audit was carried out (...) to assess the suitability of making an investment in infrastructure (...). In order for the auditors to be able to carry out their work, users with administrator access were enabled. These users were disabled , and given the need to continue with the audit, I as (...) gave them the access codes so that they could continue doing the audit.
email was sent from (...)(...) to the entire FMMC communicating possible improper income to our Network. I automatically clarified that they were not improper accesses, but accesses authorized by me, with the authorization of the Board of Trustees, in order to be able to proceed with the non-intrusive audit.
To be on the safe side I instructed the audit firm to start an investigation and proceed to change all passwords for both admin and all users. Once the investigation was completed it was confirmed that there had been no unauthorized accesses, but those authorized by me as manager.
Correctly (...)analyzes the situation, but requires a report from both Management and the company (...) and a possible communication to the Agency.
The query is whether, having verified that there have been no improper accesses or, therefore, leaks of information, is it sufficient with my information to close the incident and not have to allocate

ANSWER:
(...)

From the above analysis it can be concluded that:
1) The Entity has mechanisms to detect when incidents occur.
2) An incident has been opened with the desire to know its origin and scope.
The explanations and actions carried out confirm that there have been no improper accesses and therefore, the incident that has occurred would not be considered a security breach likely to have to be communicated to the control authority because it has not been caused no destruction, no loss, no unauthorized communication or access to personal data.
3) The explanations and actions carried out allow the incidence to be described and for it to be sufficiently documented in the Entity's internal register, additional reports not being required unless the organization's protocols specifically provide for it.
4) In the event that the Entity considers strengthening some security policy following the incident that has occurred, proposals may be submitted by the Data Protection Officer, which must be approved for (...)the treatment" .

2. The Authority opened a preliminary information phase (no. IP 388/2020), in accordance with the provisions of article 7 of Decree 278/1993, of November 9, on the sanctioning procedure applied to areas of competence of the Generalitat, and article 55.2 of Law 39/2015, of October 1, on the common administrative procedure of public administrations (henceforth, LPAC), to determine whether the facts were susceptible to motivate the initiation of a sanctioning procedure.

3. In this information phase, on 01/21/2021 the reported entity was required to comply with the following:

a) Report if, as stated in the complaint, the management of the FMMC provided (...) with the generic administrator user, which allows access to the systems with maximum privileges. If so, indicate which organizational and urgent reasons would have justified enabling (...) the " generic administrator user", instead of proceeding to re-enable specific users (who also had administrator privileges) that had previously been provided to the auditors.

b) Report if the management of the FMMC authorized the installation by (...) of a hardware in the network of the FMMC. If yes, please indicate whether the use of this hardware was authorized to access the FMMC network remotely without using VPN.

c) Please report if it is true that, as claimed by the whistleblowers, FMMC's perimeter security system did not allow remote VPN access via the generic admin user.

d) Provide the risk assessment document drawn up by the FMMC, and any other document relating to information security, valid on the dates when the events reported occurred (September 2020).

e) If you answered affirmatively to questions a/ib/, certify that the management of the FMMC could authorize these actions (facilitate (...) the generic administrator user and authorize the installation and use of the aforementioned hardware).

f) Confirm or deny the reported fact that during the period in which the (...) did not have access to the system, someone logged into his work team and accessed the management software using his credentials. In case of confirmation, indicate in detail the reasons that would have justified this access.

g) Provide the data processor contract and any document that, for these purposes, governs the contractual relationship between the FMMC and the company (...).

h) Provide any additional information you consider appropriate in relation to the events reported.

4. On 01/31/2021, the reported entity requested an extension of time to respond to the request, which was granted through an agreement dated 02/01/2021, notified that same day.

5. On 02/09/2021, the FMMC responded to the above-mentioned request in writing in which it stated the following:

- That, indeed, the Management *"gave (...) the generic administrator user that allows access to systems with maximum privileges".*

- That *"(...)(...) gave access to the auditors but disabled them in contravention of the instructions explicitly and in writing given to him by the Management".* The sequence of events that, according to the FMMC, led to the auditors being given the generic administrator user is detailed below: the Management *"informed the person in charge (...) of the FMMC ((...)) of the audit that would be carried out and he was specifically asked to be a facilitator with the auditors within the framework of the services they were entrusted with (...). Due to an unforeseen event, the fixed date of completion of part of the works contracted by (...) had to be modified and therefore, the actions would be carried out while (...)(...)was in holidays Aware of this fact, the (...) communicates it in writing to the person in charge (...), specifying that he should not remove the users from the auditors (...), an instruction that (...)(. ..) does not comply despite answering it affirmatively. (...) Despite the above, the reality is that (...)(...)contradicted the instruction given and left the auditors without access (...) The answer to the question of why it is not requested to "re-enable specific users who also had administrator privileges" is clear: (...) the organizational and urgent reasons for providing auditors with the generic administrator user respond to disobedience d(...)(...)together with the need for the contracted auditors to be able to carry out their work. On this point it should be noted that the FMMC had 3 people included in the generic administrator user: the (...), (...)(...)and (...)(...). Therefore, being (...) one of the people with this user, she chose to make it extensive also to the auditors who needed maximum access to be able to carry out the assigned service on the agreed dates. It is clear that this generic administrator user was provided to them on a temporary basis (only during the work being carried out) and on an exceptional and urgent basis (due to the lack of access through users who had been disabled)" .*

- That *"the entity's security policies and protocols establish that the generic administrator user does not have access to the FMMC via VPN. This provision complies with the definition of security measures in everyday scenarios, which may be altered due to exceptional or duly motivated situations. The reasons that lead to the carrying out of the expert audit and the difficulties in which they can develop it have been described before, explaining all together the non-normality of the moment that was lived and that makes it easy to understand that the application of the protocol was modified. Added to all this is the situation generated by the coronavirus pandemic in which it was and is immersed*

and the recommendation to carry out the maximum number of actions in a non-face-to-face manner, which requires modulating aspects of the day up to date with the new reality.
The above justifies that the auditors looked for alternative access, given the impossibility of doing so via VPN. In this sense, they installed a machine to scan the network and detect vulnerabilities, a task that is remembered as part of the contracted service. The Management and the Board of Trustees were aware of the actions, which they authorized because, as the auditors had explained, "the new remote access system still maintained all security guarantees, since the traffic traveled point-to-point in an encrypted form" .

- That " *it is confirmed that the generic administrator user did not allow remote VPN access. This point is closely linked to the explanations given"* in the previous point.

- That " *in terms of information security and, in general, compliance with data protection regulations, it is interesting to note that the Foundation has always been proactive and has had special sensitivity in this matter (...) . In this sense, the FMMC already has the risk analysis of the treatments described in the RAT, also the impact assessments of some of them".*

- That the management *"could authorize the actions described in points"* a/ ib/ of this Authority's request (antecedent 3rd), in accordance with what *"is provided in articles 17 and 24 of the statutes, and in the powers that were granted to him. Annex 6, a copy of the statutes and deed of August 2020"* granted before a notary is provided.

- *That "the actions carried out by the external auditors caused an alert to the person in charge (...) ((...)). Indeed, the alert led to the (...) crossing communications with (...)(...)(who was on vacation at the time) in relation to access to the Foundation's servers but instead, at no time did he contact the (...) (which was not on vacation, but fully operational), despite being a matter of maximum relevance.(...). In parallel, also on September 18 at 8:48 a.m. the (...) sends a statement to the entire Foundation under the title "intrusions into the Foundation's systems" in which it is reported about unknown access to the servers of the Foundation.(...) Immediately after this, the (...) at 10:06 a.m. sends a message to the entire Foundation in which it explains that the accesses had been planned and authorized by it in the framework of the audit (...) that was being carried out at the FMMC. (...) Despite the fact that the Management believed that the accesses made to the server were only those authorized to the auditors, in order to confirm this and manage the incident correctly, an investigation is opened. Within the actions, as a security measure, the passwords of all users are changed. This is explained in the e-mail that the (...) sends at 14:49 to everyone. (...) It is precisely during the process of blocking all communications, the result of the alleged attack and at the request of the FMMC management, that the external auditors detect at least two machines with resident remote control programs accessible from the Internet . One of the teams is located in the office of the department (...), therefore, it is considered appropriate to access the team of (...) responding to the need to certify the non-existence of these types of installed software in your own profile that could pose a security breach by allowing remote connections. Therefore, it is concluded that temporarily the access that the (...) has suspended remains in the hands of the auditors because they have the*

instruction to verify that no unauthorized access has occurred or that the information or security of the Foundation".

- That the contract of the person in charge of the treatment with the auditing company is provided.

- That *"from the FMMC we understand that we are dealing with a conflict situation unrelated to data protection regulations. Indeed, this complaint occurs in a context linked to the loss of confidence of the FMMC entity with certain intermediate commands ((...), (...) and (...)(...)) (.. .) …). (...)"*

- That *"reference should be made to the fact that a large part of the content of the complaint revolves around whether the decisions were adopted by the person who had this competence and/or was entrusted with the function (...). Therefore, within the framework of the management and correct development of the foundation's activity, the execution of the decisions of the Board of Trustees (highest governing body) and the adoption of orders or counter-orders on actions that intermediate commands could perform. In addition to the above, in recent times there has been distrust in the person who held the role of responsible (...)*

- That, *"last but not least, affect the time of the coronavirus in which we live. Since the declaration of a state of alarm in March 2020, the entities have had to move forward adapting in an unforeseen way to new challenges without ceasing activity at any time, especially in institutions with a welfare nature such as the "FMMC".*

The reported entity provided various documentation with its letter, among others:

i. Copy of several emails sent by management to (...): 1) email of 08/28/2020 in which management informs you that an internal audit has been ordered in the company (...), as as of the dates on which it takes place, 2) mail dated 02/09/2020 informing you that the audit is delayed by one week and asking you not to disable the users initially assigned to the auditors.

ii. Copy of the email sent on 14/09/2020 by one of the auditors to the management in which he reported that he could not enter the system because his user was disabled.

iii. Copy of the e-mail that on 09/18/2020 at 8:48 a.m. the (...) would have sent to all staff stating that *"unauthorized access to the Foundation's servers has been detected. This has caused a security incident. It seems that there is no damage (...)".*

iv. Copy of the e-mails that the management would have sent on 18/09/2021 to all staff: 1) e-mail from 10:06 in which, referring to the e-mail he had sent on (...) that same day, he informed that *"the intrusions were planned and authorized by me in order to complete the (...)visual and non-intrusive Audit that is being carried out (...)",* 2) email from 14:49 in which it informed staff that passwords and VPN passwords would be changed , that they would not be able to access with the current password, and that they needed to call the audit firm (...) to get a new one.

v. Contract between the FMMC and(...), dated 08/28/2020 and signed by the parties on the same date, for the performance of a preventive internal audit, which would contain the forecasts established in article 28 of of Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, relating to the protection of natural persons with regard to the processing of personal data and the free circulation thereof (hereinafter, RGPD) , regarding the order of the treatment.

vi. Certificate issued by the UCH Type Code, in which it certifies that during 2020 the FMMC has carried out several actions that certify that the entity meets the basic requirements required to be a member of the organization. Specifically, it certifies attendance at plenary and monographic training sessions offered to entities adhering to the Type Code, holding training sessions for its professionals, carrying out two impact assessments and conducting data protection audits.

vii. Copy of the statutes of the FMMC, which article 23 states that the Board of Trustees *"will appoint a Director-Managing Director of the Foundation, (...) who will be assigned the functions established in the appointment agreement, referred to mainly in the administration and management of the Foundation"*.

viii. Copy of the deed granting powers by the FMMC to the current management, dated 08/05/2020. This document contains the agreement adopted by the Board of Trustees of the Foundation dated 22/06/2020 by means of which power is conferred in favor of (...) *"so that in the name and representation of the Foundation, it can exercise the powers that they are contained in the protocolized certification to which I refer".* This certification, together with the deed, contains in detail the broad powers granted by the FMMC to the (...), among others, the *"management and administration powers"* which include *"1) Administer the assets of the foundation and carry out the direction and management of the activities of the Foundation, its rights and obligations, with the power to carry out and grant all kinds of acts, operations, contracts and other documents (...) 5) Appoint and dismiss workers, fixing their attributions, salaries and emoluments (...)"* .

6. On dates 03/09/2021 and 03/24/2022, still in the midst of this preliminary information phase, individual requests were addressed to the FMMC in order for them to expand some of the answers they gave through their written on 09/02/2021; specifically:

- Report on the circumstances that would explain the external auditors knowing the personal access credentials of (...) to the FMMC information systems, and through which the auditors would have accessed his work team.

- Confirm whether, as claimed by the complainants, when FMMC workers first accessed the system using the new password provided by (...), the system did not force them to change it.

7. On 19/03/2021 and 05/04/2022 the FMMC responded to the previous information requirements, setting out the following:

a) That " *it is confirmed that the auditors had a generic administrator user. It was with this administrator user that they changed the password of (...) in order to be able to access their user profile. Therefore, the auditors did not know the personal access credentials of*

(...), which they never used, but always acted with administrator credentials to access the Foundation's information systems.
We would like to point out again that access to the equipment of (...) was necessary to be able to verify that there was no remote access software installed as had already been detected on 2 other equipment (the one of the meeting room and that of the (...) information room), which were disabled to minimize risks".

b) That " *It is confirmed that to change the password, the workers called (...) and gave them a new password. At the time of giving it to them, (...) it informed of the need to change the password the first time they access and that it does not match an old one.*
The change of the password by the worker, however, was only imposed by the system for those workers who were in the Foundation's offices at that time. On the other hand, for workers who were teleworking, this change had to be made by the worker himself because technically through the VPN it was not possible for it to be mandatory. It is precisely for this reason that (...) explained to each worker the need to change the password when they were called by phone to ask for the password".

8. At the request of the Inspection Area, the Authority's Technology and Information Security Coordination analyzed the facts that were the subject of the complaint, an analysis that is contained in a document dated 04/22/2022.

9. On 26/05/2022, the director of the Catalan Data Protection Authority agreed to initiate a sanctioning procedure against the FMMC for an alleged infringement provided for in article 83.4.a), in relation to article 32; both of Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, relating to the protection of natural persons with regard to the processing of personal data and the free movement thereof (hereinafter, RGPD).. This initiation agreement was notified to the imputed entity on 05/30/2022.

10. The initiation agreement explained the reasons why no imputation was made with respect to other facts reported. Firstly, with regard to the access to the work team of one of the whistleblowers by the auditors, it was filed to the extent that in the framework of the investigations it could not be established that, given concurrent circumstances, said access was not necessary in order to guarantee the security of the FMMC computer system. And, secondly, with regard to the facilitation by the management to the external auditors of a generic administrator user and that they be authorized to install in the entity's information systems a hardware that allowed remote connection without using the VPN, was shelved as these facts by themselves would not have sufficient entity to fit into a breach of security measures. In addition, it was highlighted that the auditors followed at all times the instructions given by the management who, according to the documentation provided by the entity as part of the investigations, had the faculty to take this type of decisions, in accordance with the broad powers conferred on him by the FMMC.

11. In the initiation agreement, the accused entity was granted a period of 10 working days to formulate allegations and propose the practice of evidence that it considered appropriate to defend its interests.

1 **2.** On 07/06/2022 the FMMC requested an extension of the deadline in order to formulate allegations, which was granted by means of an agreement of 07/06/2022 notified on the same day.

13. On 06/17/2022, the FMMC submitted a letter in which it acknowledged its responsibility for the alleged events, and reiterated what it had stated in the framework of the previous information in relation to the circumstances that had led to the alleged facts. In the same letter, the FMMC related those circumstances which in its opinion would justify *"a reduction to the maximum of the penalty that should be imposed".*

Along with this letter, the accused entity provided the document certifying its adherence to the Type Code of the Catalan Union of Hospitals.

14. On 12/07/2022, the instructor of this procedure formulated a resolution proposal , by which proposed that the director of the Catalan Data Protection Authority impose an administrative fine of 2,500 euros (two thousand five hundred euros) on the FMMC as responsible for an infringement provided for in article 83.4.a) in in relation to article 32, both of the RGPD.

This resolution proposal was notified on 07/15/2022 and a period of 10 days was granted to formulate allegations.

15. On 19/07/2022 the FMMC has submitted a letter in which it does not formulate allegations and accredits the payment in advance of the amount of 1,500 euros (one thousand five hundred euros), corresponding to the monetary penalty proposed by the instructor in the resolution proposal, once the reductions provided for in article 85 of the LPAC have been applied (at this point it should be remembered that in the letter of 06/17/2022 - antecedent 13 - the entity recognized the his responsibility in the alleged acts). On the other hand, along with its letter, the FMMC provides a certificate issued by the management of the FMMC in which it states that *"all those personnel to whom the auditors provided a password to access the information systems of the entity, the computer system has forced them to change it for another personal and non-transferable one"* , certificate that had been proposed by the instructor as a corrective measure to the resolution proposal.

proven facts

In the framework of carrying out an internal audit of the information systems, the auditors hired by the FMMC, with the knowledge and authorization of the management, on an undetermined date, but in any case between 18/09 /2020 and on 30/09/2020, carried out the following actions:

- For security reasons, the passwords of the FMMC staff to access the information systems were disabled. In order to obtain the new authentication credentials, the staff had to contact the auditing company, which was responsible for providing them. The process of assigning new passwords - described by the same entity (section b/ of precedent 7th) was as follows *: "(...) the workers called (...) and he gave them a new password . At the time of giving it to them, (...) it informed of the need to change the password the first time they access and that it does not match an old one. The change of the password by the worker, however, was only imposed by the system for those workers who were in the Foundation's offices at that time. On the other hand, for workers who were teleworking, this change had to be made by the worker himself because technically through the VPN it was not possible for it to be*

mandatory. It is precisely for this reason that (...) he explained to each worker the need to change the password at the time they were called by phone to ask for the password" .

In this described process of assigning new passwords, the appropriate security measures were not established to ensure that the password was known only by the corresponding user (as would be forcing the user to change the password in his first access to the system).

- Once the credentials of (...), Responsible (...) -as well as the rest of the staff- were disabled, the auditors, with the generic administrator user, proceeded to assign him new credentials, and it was through these new credentials linked to (...) that the auditors gained access to their work team. This access, as reported by the FMMC, was limited to verifying that no remote access software had been installed on said equipment that would endanger the security of the system.

Fundamentals of law

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

The reported data processing falls within the competence of the Authority under the provisions of article 156.b) of the Statute of Autonomy of Catalonia (EAC) and article 3.h) of the Law 32/2010, since the FMMC is an entity provider of the Public Care Social Services Network, i provides public services on behalf of the Department of Social Rights of the Generalitat of Catalonia.

2. In accordance with article 85.3 of the LPAC, both the recognition of responsibility and the voluntary advanced payment of the proposed monetary penalty lead to the application of reductions. The effectiveness of these reductions is conditional on the withdrawal or renunciation of any action or appeal through the administrative route against the sanction. For both cases, sections 1 and 2 of article 85 of the LPAC provide for the termination of the procedure.

As has been advanced in the antecedents, the imputed entity has not formulated allegations in this sanctioning procedure, and has adopted the two options to reduce the amount of the sanction, recognizing its responsibility in the imputed facts and paying in advance the amount of the sanction proposed by the instructor in the resolution proposal (with the corresponding reduction of 40%).

Nevertheless, it is considered appropriate to reiterate here the assessments made by the instructor on the circumstances that, according to the FMMC, would have led to the events alleged in the procedure, invoking especially the pandemic situation that was experienced at the time, which led to that the organization had to adapt to new human resource management situations that had never been experienced until then, and emphasizing that at all times its action had been aimed at avoiding eventual vulnerabilities in its information systems.

In this regard, it is worth saying that this Authority is aware of the difficult circumstances that occurred in entities, such as the one imputed here, on the dates when the reported events occurred (September 2020), in the midst of the COVID pandemic; and understands that, this situation required additional over-effort on the part of all organizations; but having said that, it should also be noted that this exceptional situation cannot protect the violation of data protection regulations, in this case, the lack of implementation of security measures appropriate to the risk.

3. In relation to the conduct described in the "Proven Facts" section, relating to data security, it is necessary to refer to article 32 of the RGPD, which provides that :

> *"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 physical persons, (.. .) and the person in charge of the treatment will apply appropriate technical and organizational measures to guarantee a level of security adequate to the risk, which if applicable includes, among others:*
>
> a) *the pseudonymization and encryption of personal data;*
> b) *the ability to guarantee the confidentiality, integrity, availability and permanent resilience of the treatment systems and services;*
> c) *the ability to quickly restore availability and access to personal data in the event of a physical or technical incident;*
> d) *a process of regular verification, evaluation and assessment of the effectiveness of the technical and organizational measures to guarantee the security of the treatment.*
> 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 the unauthorized communication or access to said data.*
> 3. *Adherence to a code of conduct approved in accordance with article 40 or a certification mechanism approved in accordance with article 42 may serve as an element to demonstrate compliance with the requirements established in section 1 of this article.*
> 4. *(...) and the person in charge of treatment will take measures to ensure that any person who acts under the authority of (...) or the person in charge and has access to personal data can only process said data following the instructions of the person in charge, unless they are obliged to do so by virtue of the Law of the Union or of the Member States".*

As has been said, with respect to the conduct described in the imputed facts section, it is considered that the FMMC has violated the security measures detailed below:

In accordance with the provisions of the first additional provision of Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (hereinafter, LOPDGDD), it is necessary to mention what is established in sections 4.2. 1 and 4.2.5 of Annex II ("Security Measures") of Royal Decree 3/2010, of January 8, which regulates the National Security Scheme (ENS), in force when the events occurred:

"4.2.1 Identification [op.acc.1]_

dimensions	AT		
level	low	average	tall
	apply	=	=

The identification of system users will be carried out according to what is indicated below:

1. The identification systems provided for in the applicable regulations may be used as a unique identifier.

2. When the user has different roles in front of the system (for example, as a citizen, as an internal employee of the organization and as an administrator of the systems) he will receive unique identifiers for each of the cases so that privileges and activity records are always delimited .

3. Each entity (user or process) that accesses the system will have a unique identifier in such a way that:
a) You can know who receives it and what access rights it receives.
b) You can know who did something and what he did.

4. User accounts will be managed as follows:
a) Each account will be associated with a unique identifier.
b) Accounts must be disabled in the following cases: when the user leaves the organization; when the user stops the function for which the user account was required; or, when the person who authorized it, gives an order to the contrary.
c) The accounts will be retained for the period necessary to meet the traceability needs of the activity records associated with them. This period will be called the retention period.
(…)

4.2.5 Authentication mechanisms [op.acc.5]_

dimensions	ICAT		
level	low	average	tall
	apply	+	++

The authentication mechanisms against the system will be adapted to the system level, taking into account the following considerations, and the following authentication factors can be used:
– "something known": agreed passwords or keys.
– "something you have": logical components (such as software certificates) or physical devices (in English, tokens).
– "something that is": biometric elements.

The above factors can be used in isolation or combined to generate strong authentication mechanisms.

The CCN-STIC guides will develop the appropriate concrete mechanisms for each level.

The instances of the authentication factor or factors that are used in the system will be called credentials.

Before providing authentication credentials to users, they must have identified and registered in a reliable manner before the system or before an electronic identity provider recognized by the Administration. Several possibilities for user registration are contemplated:
- Through the physical presentation of the user and verification of his identity in accordance with current law, before an official authorized to do so.
– Electronically, by means of an electronic ID card or a qualified electronic certificate .
- In telematic form, using other legally admitted systems for the identification of the citizens of those contemplated in the applicable regulations.

LOW level
a) As a general principle, the use of any authentication mechanism based on a single factor will be accepted.
b) In the case of using "something known" as a factor, the basic quality rules of the same will apply .
c) The security of the credentials will be taken care of so that:
1. Credentials will be activated once they are under the effective control of the user.
2. Credentials will be under the exclusive control of the user.
3. The user will acknowledge that he has received them and that he knows and accepts the obligations implied by his possession, in particular, the duty of diligent custody, protection of his confidentiality and immediate information in case of loss.
4. Credentials will be changed with a frequency marked by the organization's policy, depending on the category of the system accessed.
5. Credentials will be withdrawn and disabled when the entity (person, team or process) that authenticates terminates its relationship with the system.

MEDIUM level
a) The use of at least two authentication factors will be required.
b) In the case of using "something known" as an authentication factor, rigorous quality and renewal requirements will be established.
c) The credentials used must have been obtained after a previous registration:
1. Face-to-face
2. Telematics using a qualified electronic certificate.
3. Telemático by means of an authentication with an electronic credential obtained after a previous registration in person or telemático using a qualified electronic certificate in a qualified signature creation device.

HIGH level
a) Credentials will be suspended after a defined period of non-use.

b) In the case of the use of "algo que se tiene", the use of hardware cryptographic elements using algorithms and parameters accredited by the National Cryptological Center will be required.
c) The credentials used must have been obtained after a previous in-person or telematic registration using a qualified electronic certificate in a qualified signature creation device".

Thus, being able to clearly establish the traceability of accesses (who, when, to what information, etc.), is a necessary measure to ensure the protection of the information subject to treatment; which was not the case in the analyzed case where, as explained in the proven facts section, it was not guaranteed that the system access credentials were always under the exclusive control of the users (measure op.acc .5); since, once the new passwords were provided to the users, no system or protocol was established by which they had to necessarily change them on their first access to the computer system. Also, to the extent that the passwords were not under the exclusive control of the users, the measure specified in op.acc.1 was also affected, since from that moment it would no longer be possible to establish undoubted who, what and when a certain action was taken within the system, which is particularly clear in the case of the person who held the position of Responsible (...), in which the auditors accessed his team of work using new credentials that they assigned him "ex novo ".

During the processing of this procedure, the facts described in the proven facts section, which are considered constitutive of 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 of the person in charge pursuant to articles 8, 11, 25 to 39, 42 and 43",* among which there is the obligation described in article 32 referring to the security of the treatment.

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

> *"f) The lack of adoption of technical and organizational measures that are appropriate to guarantee a level of security adequate to the risk of the treatment, in the terms required by article 32.1 of Regulation (EU) 2016/679 ".*

4. When the FMMC does not fit into any of the subjects provided for in article 77.1 of the LODGDD, the general sanctioning regime provided for in article 83 of the GDPR applies

Article 83.4 of the RGPD provides for a fine up to a maximum of 10,000,000 euros, or in the case of a company, an amount equivalent to a maximum of 2% of the total annual business volume total of the previous financial year, opting for the higher amount. This, without prejudice to the fact that, as an additional or substitute, some other of the measures provided for in article 58.2 RGPD may be applied.

In the present case, as explained by the investigating person in the resolution proposal, the possibility of substituting the sanction of an administrative fine with the sanction of reprimand provided for in article 58.2.b) RGPD should be ruled out, given that the lack of control about passwords affected numerous employees of the entity and, consequently, in relation to all

these people, it was not possible to clearly establish the traceability of the accesses to the information system of the FMMC.

Once it has been ruled out that the penalty of an administrative fine should be replaced by a warning, the amount of the administrative fine to be imposed must be determined. According to the provisions of article 83.2 of the RGPD, and also in accordance with the principle of proportionality enshrined in article 29 of Law 40/2015, as indicated by the instructor in the resolution proposal, the sanction should be imposed of 2,500 euros (two thousand five hundred euros). This quantification of the fine is based on the weighting between the aggravating and mitigating criteria indicated below.

As mitigating criteria, the concurrence of the following circumstances is observed, all of them invoked by the FMMC:

- The nature, seriousness and duration of the infringement, taking into account the nature, scope and purpose of the treatment operation in question, as well as the number of interested persons affected (art. 83.2.a/). It is here in consideration that there is no record of any improper access by the auditors (the only ones who knew the passwords of the employees) to the information systems, and that the facts subject to imputation resulted from a specific action and isolated in time (83.2.a RGPD).
- The lack of intentionality (art.83.2.b RGPD).
- FMMC's adherence to the code of conduct of the Unió Catalana d'Hospitals (art. 83.2.j RGPD).
- The lack of evidence of obtaining benefits as a result of the infringement (art. 83.2.k RGPD and 76.2.c LOPDGDD).
- The nature of the non-profit private Foundation entity - art. 1 of its Statutes - (art. 83.2.k RGPD).
- That in the last two accounting years the FMMC has had losses (art. 83.2.k RGPD).

On the contrary, it cannot take into account other extenuating circumstances invoked by the entity, for the reasons set out below:

- Degree of cooperation with the control authority. In this regard, it is worth saying that the mere fact of having responded to the requirements of this Authority in the prior information phase, would not justify the application of the mitigating factor provided for in letter f) of article 83.2; essentially because responding to said requirements is an obligation of the entities subject to their scope of action (article 19 of Law 32/2010) and failure to do so may constitute an infringement.
- Non-continuing nature of the infringement. The FMMC advocates the application of this mitigating factor (76.2.a LOPDGDD) since its action was a "one-off mistake". In this regard, it must be said that the fact that it was a specific action in time is a circumstance

that has already been taken into account in the first of the mitigating factors related to the previous section - art. 83.2.a RGPD-.

- The lack of previous infringements in the field of data protection. Regarding this circumstance, it is worth saying that it cannot be applied as a mitigating criterion, since it is the obligation of the entities that process personal data to comply with the regulations; reason for which if such a circumstance were to occur - which is not the case - it would act as an aggravating criterion.

- Action by the FMMC *"quick and effective",* tending to avoid *"a data leak", a* circumstance that the FMMC falls under the circumstance provided for in article 83.2.c) of the RGPD [" *cualquier medida tomada por el responsible or in charge of the treatment to alleviate the damages and losses suffered by the interested parties"]* . This mitigating criterion would apply when the entity had carried out actions to mitigate the effects or damages of the offense committed, and the FMMC does not refer to actions taken in this regard, but what it does is explain the reason why he is going to carry out the actions that, as we have seen, entailed the violation of security measures which are, precisely, those that have led to the initiation of this sanctioning procedure.

In contrast to the attenuating causes set out, the following criterion operates in an aggravating sense, and which has been taken into account to set the amount of the fine.

- Linking the activity of the FMMC with the processing of personal data (art. 83.2.k of the RGPD and 76.2.b/ of the LOPDGDD).

5. On the other hand, in accordance with article 85.3 of the LPAC and as stated in the initiation agreement and also in the resolution proposal, if before the resolution of the sanctioning procedure the entity accused acknowledges his responsibility or makes voluntary payment of the pecuniary penalty, a 20% reduction should be applied on the amount of the provisionally quantified penalty. If the two aforementioned cases occur, the reduction is applied cumulatively (40%).

As has been advanced, the effectiveness of the aforementioned reductions is conditional on the withdrawal or renunciation of any action or appeal through the administrative route against the sanction (art. 85.3 of the LPAC, *in fine*).

Well, as indicated in the background, by means of a letter dated 06/17/2022, the accused entity acknowledged its responsibility. Likewise, on 19/07/2022 he has paid 1,500 euros (one thousand five hundred euros) in advance, corresponding to the amount of the penalty resulting once the cumulative reduction of 40% has been applied.

6. Given the findings of the violations provided for in art. 83 of the RGPD in relation to files or treatments carried out by entities not included in article 77.1 of the LODGDD, article 21.3 of Law 32/2010, of October 1, of the Catalan Authority of Data Protection, empowers the director of the Authority so that the resolution declaring the infringement establishes the appropriate measures to stop or correct its effects. In the present case, however, it is not necessary to require the adoption of any corrective measure since the entity in the course of this procedure has carried out the measure proposed by the instructor, consisting of certifying that *"all those personnel to whom auditors provided a password to access the*

entity's information systems, the computer system has forced them to change it to another personal and non-transferable one" .

For all this, I resolve:

1. To impose on the Foundation for the Mentally Ill of Catalonia the sanction consisting of a fine of 2,500 euros (two thousand five hundred euros), as responsible for an infringement provided for in article 83.4.a) in relation to article 32 , both of the RGPD.

It is not necessary to require corrective measures to correct the effects of the infringement, in accordance with what has been set out in the 6th legal basis.

2. Declare that the Fundació de Malalts Mentals de Catalunya has effected the advanced payment of 1,500 euros (one thousand five hundred euros), which corresponds to the total amount of the penalty imposed, once the 40% deduction percentage has been applied corresponding to the reductions provided for in article 85 of the LPAC.

3. Notify this resolution to the Mentally Ill Foundation of Catalonia.

4. 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 the provisions of article 123 et seq. of the LPAC. You can also directly file an administrative contentious appeal before the administrative contentious courts, within two months from the day after its notification, in accordance with articles 8, 14 and 46 of Law 29/1998, of July 13, regulating the administrative contentious jurisdiction.

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

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

The director,