Identificació de l'expedient

Resolució del procediment sancionador núm. PS 32/2022, referent a la Fundació de Malalts Mentals de Catalunya.

Antecedents

1. En data 10/12/2020, va tenir entrada a l'Autoritat una denúncia formulada per tres persones ((...), (...)i (...)) contra la Fundació de Malalts Mentals de Catalunya (en endavant, FMMC), amb motiu d'un presumpte incompliment de la normativa sobre protecció de dades personals. En concret, les persones denunciants, (...), exposaven els següents fets que consideraven contraris a la normativa, els quals van tenir lloc al mes de setembre de 2020, en el si d'una auditoria dels sistemes d'informació que l'entitat havia encarregat a una empresa externa contractada a l'efecte ((...)), i que haurien derivat en un "*incident de seguretat (IN-061").*

a) Que (...)(...)((...)) havia proporcionat a finals d'agost a (...) dos usuaris específics (un per cada auditor) amb drets d'administració del sistema, amb els quals podien accedir remotament via VPN als sistemes de l'FMMC per fer les feines d'auditoria encomanades; però aquests usuaris es van inhabilitar quan el citat responsable va marxar de vacances. Les persones denunciants es queixen que, davant d'aquesta circumstància, la gerència de l'FMMC, en comptes de procedir a tornar a habilitar els usuaris específics que s'havien proporcionat al seu dia als auditors, va facilitar, sense coneixement de les persones responsables de (...)(...)de l'FMMC, "l'usuari genèric administrador" de domini a (...), per tal que poguessin accedir amb els màxims privilegis als sistemes, com així va fer.

b) Que (...), sense coneixement dels responsables de (...), i saltant-se la seguretat perimetral de l'FMMC, va instal·lar un "*maquinari a les instal·lacions per connectar-se des de l'exterior saltant-se la seguretat de l'FMMC, i, mitjançant la contrasenya de l'usuari Administrador, cedida per (...), poder realitzar les tasques que necessitessin"*. Els denunciants manifesten que el protocol de seguretat de l'FMMC prohibeix expressament que mitjançant l'usuari genèric administrador es pugui accedir remotament al sistema, és a dir, que *"aquest usuari especial només pot ser usat des de dins de la xarxa de la Fundació: per seguretat no pot ser usat per entrar des de fora als sistemes de la Fundació"*. En definitiva, els denunciants afirmen que, en la mesura que el sistema de seguretat implementat per l'FMMC no permetia que a través de l'usuari administrador es pogués accedir remotament -a través d'VPN (que era el sistema d'accés remot previst)- als sistemes d'informació, (...) va instal·lar el mencionat maquinari per poder connectar-se remotament mitjançant l'usuari administrador.

c) Que, arran *"les intrusions als sistemes d'informació"* detectades (pels denunciants) per haver constatat accessos amb l'usuari administrador genèric, la gerència, sense la intervenció dels responsables (...)*"ordena a l'empresa que realitza l'auditoria (i presumptament l'autora de les intrusions) a realitzar una investigació i a canviar les claus de tots els usuaris de l'organització (...) gestionant així totes les credencials de l'organització i bloquejant l'accés dels usuaris als sistemes almenys durant el cap de setmana"*. A la vista d'aquest bloqueig, les persones treballadores de l'FMMC van haver de trucar a (...) per tal que aquesta empresa els facilités una nova contrasenya per poder accedir als sistemes. Les persones denunciants afirmen que en cap moment es va avisar al personal que per

seguretat havien de procedir de forma immediata a canviar la contrasenya proporcionada per (...). És més, manifesten que quan van advertir a (...) d'aquest fet, se'ls hi va dir *que "ells no tenien aquesta pràctica, que cadascú la podia canviar (la contrasenya) quan volgués, que ells eren professionals i evidentment no entrarien mai al compte d'un usuari".*

d) Que, durant el període durant el qual el Sr. (...)no va disposar d'accés als sistemes (als voltants de la segona quinzena de setembre de 2020 i fins el 01/10/2020 en què el recupera), *"hi ha proves d'inicis de sessió al seu equip de treball i d'accessos a programari de gestió usant les seves credencials".*

Les persones denunciants afegien que la gerència de l'FMMC va adreçar al "Codi Tipus" de la Unió Catalana d'Hospitals (UCH) -al qual està adherit la Fundació-, una consulta sobre els fets succeïts per tal de procedir a tancar la incidència, però que la gerència va ometre informació rellevant en exposar el cas a la UCH.

Les persones denunciants, junt amb la seva denúncia aportaven la següent documentació:

- *"Informe incidència de seguretat de data 18/09/2020",* elaborat el 29/09/2020 pel (...) qui, (...). Aquest informe conté una cronologia dels fets que al seu entendre, haurien derivat en un incident de seguretat ("*IN-061*"). Aquest informe, entre d'altres, inclou la còpia de diversos correus electrònics intercanviats entre els responsables de (...)(...)((...) i (...)) i entre aquests i la gerència de l'FMMC.

- Còpia de la resposta que la UCH (Codi tipus) va donar a l'FMMC en relació amb la consulta que l'entitat li plantejà relativa a l'incident de seguretat. En aquest informe es recull el literal següent:

"CONSULTA:
Arrel d'uns fets succeïts tinc dubte sobre l'adequació de donar per tancada la incidència de seguretat.
Es va procedir a fer una auditoria (...)per valorar la idoneïtat de fer una inversió en infraestructures (...). Per tal de que els auditors poguessin realitzar la seva feina se'ls hi van habilitar uns usuaris amb accés d'administrador. Aquests usuaris es van deshabilitar, i davant la necessitat de prosseguir amb l'auditoria jo com a (...)els hi vaig donar els codis per accedir i que poguessin seguir fent l'auditoria.
Davant d'aquests fets des de (...)(...)es va enviar un mail d'alarma a tota l'FMMC comunicant possibles ingressos indeguts a la nostra Xarxa. Automàticament vaig aclarir que no eren accessos indeguts, sinó accessos autoritzats per mi, amb l'autorització també del Patronat, per tal de poder prosseguir amb l'auditoria no intrusiva.
Per més seguretat vaig ordenar a l'empresa d'auditoria que iniciessin una investigació i procedissin a canviar totes les contrasenyes tant d'administrador com de tots els usuaris. Un cop finalitzada la investigació es va corroborar que no hi havien hagut accessos no autoritzats, sinó els autoritzats per mi com a gerent.
Correctament (...)analitza la situació, però requereix un informe tant per part de Gerència com de l'empresa (...) i una possible comunicació a l'Agència.
La consulta és si, havent comprovat que no hi han hagut accessos indeguts ni per tant, fuites d'informació, és suficient amb la meva informació per tancar la incidència i no haver de destinar

RESPOSTA:
(...)
De l'anàlisi anterior es pot concloure que:
1) L'Entitat disposa de mecanismes que permeten detectar quan es produeixen incidències.
2) S'ha obert una incidència amb la voluntat de saber-ne l'origen i l'abast.
Les explicacions i actuacions dutes a terme confirmen que no s'han produït accessos indeguts i per tant, la incidència ocorreguda no tindria consideració de bretxa de seguretat susceptible d'haver-se de comunicar a l'autoritat de control doncs no s'ha ocasionat ni destrucció, ni pèrdua, ni comunicació o accés no autoritzat a dades personals.
3) Les explicacions i actuacions dutes a terme permeten descriure la incidència i que aquesta quedi documentada de forma suficient en el registre intern de l'Entitat, no essent requerits informes addicionals excepte que els protocols de l'organització així ho disposin específicament.
4) En cas que l'Entitat valori reforçar alguna política de seguretat arran de la incidència succeïda, poden presentar-se propostes per part de la Delegada de Protecció de Dades, les quals hauran de ser aprovades p(...)del tractament".

2. L'Autoritat va obrir una fase d'informació prèvia (núm. IP 388/2020), d'acord amb el que preveu l'article 7 del Decret 278/1993, de 9 de novembre, sobre el procediment sancionador d'aplicació als àmbits de competència de la Generalitat, i l'article 55.2 de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques (d'ara endavant, LPAC), per determinar si els fets eren susceptibles de motivar la incoació d'un procediment sancionador.

3. En aquesta fase d'informació, en data 21/01/2021 es va requerir l'entitat denunciada perquè donés compliment al següent:

a) Informés si, tal com s'afirmava en la denúncia, la gerència de l'FMMC va facilitar a (...) l'usuari genèric administrador, que permet accedir als sistemes amb els màxims privilegis. En cas afirmatiu, indiqués quines raons organitzatives i d'urgència haurien justificat que es facilités a (...) l'"usuari genèric administrador", en comptes de procedir a tornar a habilitar els usuaris específics (que també tenien privilegis d'administrador) que s'havien proporcionat al seu dia als auditors.

b) Informés si la gerència de l'FMMC va autoritzar la instal·lació per part d'(...) d'un maquinari a la xarxa de l'FMMC. En cas afirmatiu, indiqués si es va autoritzar l'ús d'aquest maquinari per accedir a la xarxa de la FMMC remotament sense utilitzar la VPN.

c) Informés si és cert que, tal com afirmen les persones denunciants, el sistema de seguretat perimetral de l'FMMC no permetia l'accés remot per VPN mitjançant l'usuari genèric administrador.

d) Aportés el document d'avaluació de riscos elaborat per l'FMMC, i qualsevol altre document relatiu a la seguretat de la informació, vigent en les dates en que van ocorre els fets denunciats (setembre 2020).

e) En cas d'haver contestat afirmativament les preguntes a/ i b/, certifiqués que la gerència de l'FMMC podia autoritzar aquestes actuacions (facilitar a (...) l'usuari genèric administrador i autoritzar la instal·lació i ús del maquinari esmentat).

f) Confirmés o desmentís el fet denunciat referent a que durant el període en què el (...) no va tenir accés al sistema, algú va iniciar la sessió al seu equip de treball i va accedir al programari de gestió usant les seves credencials. En cas de confirmar-ho, indiqués amb detall les raons que haurien justificat aquest accés.

g) Aportés el contracte d'encarregat de tractament i qualsevol document que, a aquests efectes, regís la relació contractual entre l'FMMC i l'empresa (...).

h) Aportés qualsevol informació addicional que considerés procedent en relació amb els fets denunciats.

4. En data 31/01/2021 l'entitat denunciada va sol·licitar una ampliació de termini per donar resposta al requeriment, la qual li fou concedida mitjançant acord de 01/02/2021, notificat aquell mateix dia.

5. En data 09/02/2021, l'FMMC va respondre el requeriment esmentat a través d'escrit en què exposava el següent:

- Que, efectivament la Gerència *"va facilitar a (...) l'usuari genèric administrador que permet accedir a sistemes amb els màxims privilegis".*

- Que *"(...)(...)va donar accessos als auditors però els va deshabilitar contravenint les instruccions que explícitament i per escrit se li havien indicat des de la Direcció".* Es detalla seguidament la successió de fets que, segons l'FMMC, van propiciar que als auditors se'ls facilités l'usuari genèric administrador: la Gerència *"va informar al responsable (...)de l'FMMC ((...)) de l'auditoria que es realitzaria i se li demanava de forma precisa que fos facilitador amb els auditors en el marc deis serveis que tenien encomanats (...). Degut a un imprevist, es va haver de modificar la data fixada de realització de part deis treballs contractats per (...) i per tant, les actuacions serien dutes a terme mentre (...)(...)es trobava de vacances. Conscients d'aquest fet, la (...)ho comunica per escrit al responsable (...)precisant-li que no havia de treure als auditors els usuaris (...), instrucció que (...)(...)no acompleix malgrat contestar-la afirmativament. (...) Malgrat l'anterior, la realitat és que (...)(...)va contravenir la instrucció donada i va deixar sense accés als auditors (...) La resposta a la qüestió de perquè no es va sol·licitar «tornar a habilitar els usuaris específics que també tenien privilegis d'administrador» és clara: (...) les raons organitzatives i d'urgència que motiven facilitar als auditors l'usuari genèric d'administrador responen a la desobediència d(...)(...)juntament amb la necessitat de que els auditors contractats poguessin realitzar la seva tasca. Sobre aquest punt convé indicar que l'FMMC tenia a 3 persones incloses en l'usuari genèric d' administrador: la (...), (...)(...)i (...)(...). Per tant, essent la (...)una de les persones amb aquest usuari, va optar per fer-lo extensiu també als auditors que necessitaven els màxims accessos per a poder desenvolupar la prestació encomanada en les dates acordades. És clar que aquest usuari genèric d'administrador se'ls facilitava amb caràcter temporal (únicament durant els treballs que es realitzaven) i amb caràcter excepcional i urgent (degut a la manca d'accés a través deis usuaris que s'havien deshabilitat)".*

- Que *"les polítiques de seguretat i protocols de l'entitat estableixen que l'usuari genèric d'administrador no té accés a l'FMMC via VPN. Aquesta previsió obeeix a la definició de mesures de seguretat en escenaris quotidians, que per situacions excepcionals o degudament motivades, poden veure's alterades. S'han descrit abans les raons que condueixen a la realització de l'auditoria deis experts i les dificultats en que aquests puguin desenvolupar-la, explicant tot plegat la no normalitat del moment que es vivia i que fa entendre fàcilment que l'aplicació del protocol es veiés modificada. A tot això, s'hi suma la situació generada per la pandèmia de coronavirus en la que s'estava i s'està immers i la recomanació de dur a terme el màxim de les actuacions de forma no presencial, que exigeix modular aspectes del dia a dia a la nova realitat. L'anterior justifica doncs que els auditors busquessin alternatives d'accés, davant la impossibilitat de fer-ho via VPN. En aquest sentit, instal·laren una màquina per fer un escaneig de la xarxa i detectar vulnerabilitats, tasca que es recorda que estava dins de la prestació contractada. La Direcció i el Patronat estaven assabentats de les actuacions, les quals autoritzaven perquè, tal i com havien explicat els auditors "el nou sistema d'accés remot mantenia igualment totes les garanties de seguretat, dones el tràfic viatjava de forma xifrada punt a punt".*

- Que "*es confirma que l'usuari genèric d'administrador no permetia l'accés remot per VPN. Aquest punt va estretament lligat a les explicacions donades"* al punt precedent.

- Que "*en quant a la seguretat de la informació i en general, l'acompliment de la normativa de protecció de dades, interessa destacar que la Fundació sempre ha estat proactiva i ha tingut especial sensibilitat en aquesta matèria (...) . En aquest sentit, l'FMMC ja disposa de l'anàlisi de riscos deis tractaments descrits en el RAT, també de les avaluacions d'impacte d'alguns d'ells".*

- Que la gerència *"podia autoritzar les actuacions descrites en els punts"* a/ i b/ del requeriment d'aquesta Autoritat (antecedent 3r), d'acord amb el que *"es disposa en els articles 17 i 24 dels estatuts, i en els poders que li foren atorgats. Annex 6, s'aporta còpia dels estatuts i escriptura d'agost de 2020"* atorgada davant notari.

- *Que "les actuacions dutes a terme per part dels auditors externs van provocar una alerta al responsable (...) ((...)). En efecte, l'alerta va comportar que el (...) creués comunicacions amb (...)(...)(que en aquells moments estava de vacances) en relació als accessos als servidors de la Fundació però en canvi, no va contactar en cap moment amb la (...)(que no estava de vacances, sinó plenament operativa), malgrat ser una qüestió de seguretat de màxima rellevància.(...). En paral·lel, també el 18 de setembre a les 8:48h el (...) envia un comunicat a tota la Fundació sota el títol «intrusions als sistemes de la Fundació» en el qual s'informa dels accessos desconeguts als servidors de la Fundació.(...) Immediatament després d'això, la (...)a les 10:06 envia a tota la Fundació un missatge en el qual explica que els accessos havien estat previstos i autoritats per ella en el marc de !'auditoria (...)que s'estava realitzant a l'FMMC. (...) Malgrat que des de la Direcció es creia que els accessos produïts al servidor només eren els autoritzats als auditors, per a confirmar-ho i gestionar correctament la incidència, s'obre una investigació. Dins de les actuacions, com a mesura de seguretat es procedeix a canviar les contrasenyes de tots els usuaris. Això s'explica en el correu electrònic que la (...)envia a les 14:49h a tothom. (...) És justament durant el procés de bloqueig de totes les comunicacions, fruit del suposat atac i a requeriment de la direcció*

de l'FMMC, que els auditors externs detecten almenys dues màquines amb programes de control remot residents accessibles des d'internet. Un dels equips es troba ubicat al despatx del departament (...), per tant, es creu oportú accedir a l'equip del (...) responent a la necessitat de certificar la inexistència d'aquests tipus de programari instal·lat en el seu propi perfil que pogués suposar una vulneració de la seguretat al permetre connexions remotes. Per tant, es conclou que temporalment els accessos que el (...) té suspesos queden en mans deis auditors perquè tenen la instrucció de verificar que no s'hagin produït accessos no autoritzats ni s'hagi posat en risc la informació o seguretat de la Fundació".

- Que s'aporta el contracte d'encarregat del tractament amb l'empresa auditora.

- Que *"des de l'FMMC entenem que estem davant d'una situació de conflicte aliè a la normativa de protecció de dades. Efectivament aquesta denúncia es produeix en un context lligat a la pèrdua de confiança de l'entitat FMMC amb determinats comandaments intermedis ((...), (...)i (...)(...)) (...)…). (...)(…)"*

- Que *"s'ha de fer referencia a que gran part del contingut de la denúncia gira entorn de si les decisions foren adoptades per part de qui tenia aquesta competència i/o encomanada la funció (...). Per tant, en el marc de la gestió i correcte desenvolupament de l'activitat fundacional, queda sota el control de la Direcció General l'execució de les decisions del Patronat (màxim òrgan de govern) i l'adopció de les ordres o contraordres sobre accions que comandaments intermedis poguessin realitzar. A l'anterior se suma que en els darrers temps hi havia desconfiança en la persona que ostentava el rol de responsable (...)*

- Que, *"per últim però no menys important, incidir en l'època de coronavirus en que vivim. Des de la declaració d'estat d'alarma el març de 2020, les entitats han hagut de seguir endavant adaptant-se de forma imprevista a nous reptes sense deixar en cap moment l'activitat, sobretot en institucions amb caràcter assistencial com ho és l'FMMC".*

L'entitat denunciada aportava amb el seu escrit diversa documentació, entre d'altra:

i. Còpia de diversos correus electrònics enviats per la gerència al (...): 1) correu de 28/08/2020 en què gerència l'informa que s'ha encarregat una auditoria interna a l'empresa (...), així com de les dates en què es dura a terme, 2) correu de 02/09/2020 en què l'informa que l'auditoria es retarda una setmana i li demana que no inhabiliti els usuaris inicialment assignats als auditors.

ii. Còpia del correu electrònic enviat el 14/09/2020 per un dels auditors a la gerència en què informava que no podia entrar al sistema perquè el seu usuari estava inhabilitat.

iii. Còpia del correu electrònic que el 18/09/2020 a les 8:48 el (...) hauria enviat a tot el personal exposant que *"s'han constatat accessos no autoritzats als servidors de la Fundació. Això ha originat una incidència de seguretat. Sembla ser que no hi ha danys (...)".*

iv. Còpia dels correus electrònics que la gerència hauria enviat el 18/09/2021 a tot el personal: 1) correu de les 10:06 en què, fent referència al correu electrònic que havia

enviat el (...) aquell mateix dia, informava que *"les intrusions estaven previstes i autoritzades per mi per tal de finalitzar l'Auditoria (...)visual i no intrusiva que s'està realitzant (...)",* 2) correu de les 14:49 en què s'informava al personal que es procediria a canviar els passwords i les contrasenyes de VPN, que no podrien accedir amb la contrasenya actual, i que calia trucar a l'empresa d'auditoria (...) per obtenir una de nova.

v. Contracte entre la FMMC i(...), datat el 28/08/2020 i signat per les parts en la mateixa data, per a la realització d'una auditoria interna preventiva, que contindria les previsions establertes a l'article 28 de del Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes (en endavant, RGPD), pel que fa a l'encàrrec del tractament.

vi. Certificat emès pel Codi Tipus de la UCH, en què certifica que durant el 2020 l'FMMC ha dut a terme diverses actuacions que acrediten que l'entitat compleix els requisits bàsics exigits per estar adherits a l'organització. En concret, certifica l'assistència a sessions formatives plenàries i monogràfiques ofertes a entitats adherides al Codis Tipus, realització de sessions formatives als seus professionals, realització de dues avaluacions d'impacte i realització d'auditories en protecció de dades.

vii. Còpia dels estatuts de l'FMMC, quin article 23 disposa que el Patronat *"nomenarà a un Director-Gerent de la Fundació, (...) al qual li seran assignades les funcions que s'estableixin a l'acord de nomenament, referides principalment a l'administració i gestió de la Fundació".*

viii. Còpia de l'escriptura d'atorgament de poders per part de l'FMMC a l'actual gerència, de data 05/08/2020. En aquest document es recull l'acord adoptat per Patronat de la Fundació de data 22/06/2020 mitjançant el qual es confereix poder a favor de (...)*"perquè en nom i representació de la Fundació, pugui exercir les facultats que consten a la certificació protocol·litzada a la que em remeto".* Aquesta certificació, unida a l'escriptura, recull de forma detallada els amplis poders atorgats per l'FMMC a la (...), entre d'altres, les *"facultats de gestió i administració"* entre les quals s'inclou *"1) Administrar els béns de la fundació i portar la direcció i gestió de les activitats pròpies de la Fundació, els seus drets i obligacions, amb facultat per realitzar i atorgar tota classe d'actes, operacions, contractes i altres documents (...) 5) Nomenar i acomiadar treballadors, fixant les seves atribucions, sous i emoluments (...)"*.

6. En dates 09/03/2021 i 24/03/2022, encara en el si d'aquesta fase d'informació prèvia, es van dirigir sengles requeriments a l'FMMC per tal que ampliessin alguna de les respostes que van donar mitjançant el seu escrit de 09/02/2021; en concret:

- Informés de les circumstàncies que explicarien que els auditors externs coneguessin les credencials personals d'accés del (...) al sistemes d'informació de l'FMMC, i mitjançant les quals els auditors haurien accedit al seu equip de treball.

- Confirmés si, tal com afirmaven les persones denunciants, quan les persones treballadores de l'FMMC van accedir al sistema per primera vegada mitjançant la nova contrasenya proporcionada per (...), el sistema no els va forçar a canviar-la.

7. En dates 19/03/2021 i 05/04/2022 l'FMMC va donar resposta als anteriors requeriments d'informació, exposant el següent:

a) Que "*es confirma que els auditors tenien usuari genèric d'administrador. Fou amb aquest usuari d'administrador que canviaren la contrasenya del (...) per tal de poder accedir al seu perfil d'usuari. Per tant, els auditors no coneixien les credencials personals d'accés del (...), de les quals mai en feren ús, sinó que actuaren sempre amb les credencials d'administrador per accedir als sistemes d'informació de la Fundació.*
Es vol tornar a destacar que l'accés a l'equip del (...) era necessari per poder verificar que no hi hagués cap software d'accés remot instal·lat com s'havia detectat ja en 2 altres equips (el de la sala de juntes i el de la sala (...)d'informació), els quals es deshabilitaren per minimitzar riscos".

b) Que "*Es confirma que per fer el canvi de la contrasenya, els treballadors trucaven a (...) i els donava una nova contrasenya. En el moment de donar-los-la, (...) informava de la necessitat de que la primera vegada que accedissin calia fer el canvi de la contrasenya i que aquesta no coincidís amb una d'antiga.*
El canvi de la contrasenya per part del treballador però només venia imposat pel sistema per aquells treballadors que en aquell moment estaven a les oficines de la Fundació. En canvi, per als treballadors que estaven teletreballant, aquest canvi l'havia de fer el propi treballador perquè tècnicament a través de la VPN no era possible que fos obligatori. És justament per aquest motiu que (...) explicava a cada treballador la necessitat de fer el canvi de contrasenya en el moment que se'ls trucava per telèfon per demanar la contrasenya".

8. A petició de l'Àrea d'Inspecció, la Coordinació de Tecnologia i Seguretat de la Informació de l'Autoritat va analitzar els fets objecte de denúncia, anàlisi que es recull en un document de data 22/04/2022.

9. En data 26/05/2022, la directora de l'Autoritat Catalana de Protecció de Dades va acordar iniciar un procediment sancionador contra l'FMMC per una presumpta infracció prevista a l'article 83.4.a), en relació a l'article 32; ambdós del Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes (en endavant, RGPD).. Aquest acord d'iniciació es va notificar a l'entitat imputada en data 30/05/2022.

10. L'acord d'iniciació explicitava els motius pels quals no es va efectuar cap imputació respecte d'altres fets denunciats. En primer lloc, pel que fa a l'accés a l'equip de treball d'una de les persones denunciants per part dels auditors, es va arxivar en la mesura que en el marc de les investigacions no es va poder constatar que, ateses les circumstàncies concurrents, el dit accés no fos necessari per tal de garantir la seguretat del sistema informàtic de l'FMMC. I, en segon lloc, pel que fa a la facilitació per part de de la gerència als auditors externs d'un usuari genèric administrador i que se'ls autoritzés la instal·lació en els sistemes d'informació de l'entitat d'un maquinari que permetés la connexió remota sense fer servir l'VPN, es va arxivar ja que aquests fets per si mateixos no tindrien l'entitat suficient com per encabir-se en una vulneració de mesures de seguretat. A més, es va posar en relleu que els auditors van seguir en tot moment les instruccions donades per la gerència qui, d'acord amb la documentació proporcionada per l'entitat en el marc de les

investigacions, tenia la facultat per prendre aquest tipus de decisions, d'acord amb els amplis poders que li havia conferit l'FMMC.

11. A l'acord d'iniciació es concedia a l'entitat imputada un termini de 10 dies hàbils per formular al·legacions i proposar la pràctica de proves que considerés convenients per defensar els seus interessos.

1**2.** En data 07/06/2022 l'FMMC va sol·licitar l'ampliació del termini per tal de formular al·legacions, el que se li va concedir mitjançant acord de 07/06/2022 notificat el mateix dia.

13. En data 17/06/2022, l'FMMC va presentar un escrit en el que reconeixia la seva responsabilitat en els fets imputats, i reiterava allò que havia exposat en el marc de la informació prèvia en relació amb les circumstàncies que havien propiciat els fets imputats. En el mateix escrit l'FMMC relacionava aquelles circumstàncies que al seu parer justificarien *"una minoració al màxim de la sanció que correspongui imposar".*

Junt amb aquest escrit, l'entitat imputada aportava el document acreditatiu de la seva adhesió al Codi Tipus de la Unió Catalana d'Hospitals.

14. En data 12/07/2022, la instructora d'aquest procediment va formular una proposta de resolució, per la qual proposava que la directora de l'Autoritat Catalana de Protecció de Dades imposés a l'FMMC amb una multa administrativa de 2.500 euros (dos mil cinc-cents euros) com a responsable d'una infracció prevista a l'article 83.4.a) en relació amb l'article 32, ambdós de l'RGPD.

Aquesta proposta de resolució es va notificar en data 15/07/2022 i es concedia un termini de 10 dies per formular al·legacions.

15. En data 19/07/2022 l'FMMC ha presentat un escrit en què no formula al·legacions i acredita el pagament per avançat de la quantitat de 1.500 euros (mil cinc-cents euros), corresponents a la sanció pecuniària proposada per la instructora en la proposta de resolució, una vegada aplicades les reduccions previstes a l'article 85 de l'LPAC (en aquest punt cal recordar que en l'escrit de 17/06/2022 -antecedent 13- l'entitat va reconèixer la seva responsabilitat en els fets imputats). D'altra banda, junt amb el seu escrit, l'FMMC aporta un certificat emès per la gerència de l'FMMC en què manifesta que *"tot aquell personal a qui els auditors van facilitar una contrasenya d'accés als sistemes d'informació de l'entitat, el sistema informàtic els ha forçat a canviar-la per una altra personal i intransferible"*, certificat que havia estat proposat per la instructora com a mesura correctora a la proposta de resolució.

Fets provats

En el marc de la realització d'una auditoria interna dels sistemes d'informació, les persones auditores contractades per l'FMMC, amb el coneixement i autorització de la gerència, en una data indeterminada, però en tot cas compresa entre el 18/09/2020 i el 30/09/2020, van dur a terme les actuacions següents:

- Per raons de seguretat, es va procedir a inhabilitar les contrasenyes del personal de l'FMMC per accedir als sistemes d'informació. Per tal d'obtenir les noves credencials d'autenticació, el personal havia de contactar amb l'empresa auditora, qui era l'encarregada de proporcionar-les. El procés d'assignació de les noves contrasenyes -descrit per la mateixa entitat (apartat b/ de l'antecedent 7è) era el següent*: "(...) els treballadors trucaven a (...) i els donava una nova contrasenya. En el moment de donar-los-la, (...) informava de la necessitat de que la primera vegada que accedissin calia fer el canvi de la contrasenya i que aquesta no coincidís amb una d'antiga. El canvi de la contrasenya per part del treballador però només venia imposat pel sistema per aquells treballadors que en aquell moment estaven a les oficines de la Fundació. En canvi, per als treballadors que estaven teletreballant, aquest canvi l'havia de fer el propi treballador perquè tècnicament a través de la VPN no era possible que fos obligatori. És justament per aquest motiu que (...) explicava a cada treballador la necessitat de fer el canvi de contrasenya en el moment que se'ls trucava per telèfon per demanar la contrasenya"*.

En aquest procés descrit d'assignació de les noves contrasenyes, no es van establir les mesures de seguretat oportunes que garantissin que la contrasenya fos coneguda únicament per l'usuari corresponent (com seria forçar a l'usuari al canvi de contrasenya en el seu primer accés al sistema).

- Un cop es van inhabilitar les credencials del (...), Responsable (...) -com a la resta del personal-, els auditors, amb l'usuari genèric administrador, van procedir a assignar-li unes noves credencials, i fou mitjançant aquestes noves credencials vinculades al (...) que els auditors van accedir al seu equip de treball. Aquest accés, segons ha informat l'FMMC, es va limitar a verificar que en el dit equip no s'havia instal·lat cap software d'accés remot que posés en perill la seguretat del sistema.

Fonaments de dret

1. Són d'aplicació a aquest procediment el que preveuen l'LPAC, i l'article 15 del Decret 278/1993, segons el que preveu la DT 2a de la Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades. De conformitat amb els articles 5 i 8 de la Llei 32/2010, la resolució del procediment sancionador correspon a la directora de l'Autoritat Catalana de Protecció de Dades.

El tractament de dades denunciat recau dins l'àmbit competencial de l'Autoritat en virtut del previst a l'article 156.b) de l'Estatut d'Autonomia de Catalunya (EAC) i l'article 3.h) de la Llei 32/2010, atès que l'FMMC és una entitat proveïdora de la Xarxa de Serveis Socials d'Atenció Pública, i presta serveis públics per compte del Departament de Drets Socials de la Generalitat de Catalunya.

2. De conformitat amb l'article 85.3 de l'LPAC, tant el reconeixement de responsabilitat com el pagament voluntari avançat de la sanció pecuniària proposada comporten l'aplicació d'unes reduccions. L'efectivitat d'aquestes reduccions està condicionada al desistiment o la renúncia de qualsevol acció o recurs per la via administrativa contra la sanció. Per a ambdós casos, els apartats 1 i 2 de l'article 85 de l'LPAC preveuen la terminació del procediment.

Tal com s'ha avançat als antecedents, l'entitat imputada no ha formulat al·legacions en el si d'aquest procediment sancionador, i s'ha acollit a les dues opcions per reduir l'import de la sanció, reconeixent la seva responsabilitat en els fets imputats i pagant per avançat l'import de la sanció proposada per la instructora a la proposta de resolució (amb la reducció corresponent del 40%).

Tot i això, es considera oportú reiterar aquí les apreciacions fetes per la instructora sobre les circumstàncies que, segons l'FMMC, haurien propiciat els fets imputats en el procediment, invocant especialment la situació de pandèmia que es vivia en aquells moments, que va comportar que l'organització es tingués que adaptar a noves situacions de gestió de recursos humans fins aquells moments mai viscudes, i posant en relleu que en tot moment la seva actuació havia estat destinada a evitar eventuals vulnerabilitats en els seus sistemes d'informació.

Al respecte val a dir que aquesta Autoritat es coneixedora de les difícils circumstàncies que es van donar en entitats, com l'aquí imputada, en les dates en què van ocorre els fets denunciats (setembre de 2020), en plena pandèmia de COVID; i entén que, aquesta situació va requerir un sobreesforç addicional per part de totes les organitzacions; però dit això cal també remarcar que aquesta situació d'excepcionalitat no pot emparar la vulneració de la normativa de protecció de dades, en aquest cas, la manca d'implementació de mesures de seguretat adequades al risc.

3. En relació amb les conductes descrites a l'apartat "Fets Provats", relatives a la seguretat de les dades, cal acudir a l'article 32 de l'RGPD, el qual disposa que:

> *"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, (...)y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:*
>
> a) *la seudonimización y el cifrado de datos personales;*
> b) *la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
> c) *la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;*
> d) *un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*
> 2. *Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.*
> 3. *La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.*

> 4. *(...)y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad d(...)o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".*

Com s'ha dit, respecte les conductes descrites a l'apartat de fets imputats, es considera que l'FMMC ha vulnerat les mesures de seguretat que es detallen a continuació:

D'acord amb el que disposa la disposició addicional primera de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (en endavant, LOPDGDD), cal mencionar el que estableixen els apartats 4.2.1 i 4.2.5 de l'Annex II ("Mesures de Seguretat") del Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat (ENS), vigent quan van ocórrer els fets:

"4.2.1 Identificación [op.acc.1]

dimensiones	A T		
nivel	bajo	medio	alto
	aplica	=	=

La identificación de los usuarios del sistema se realizará de acuerdo con lo que se indica a continuación:

1. Se podrán utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación.

2. Cuando el usuario tenga diferentes roles frente al sistema (por ejemplo, como ciudadano, como trabajador interno del organismo y como administrador de los sistemas) recibirá identificadores singulares para cada uno de los casos de forma que siempre queden delimitados privilegios y registros de actividad.

3. Cada entidad (usuario o proceso) que accede al sistema, contará con un identificador singular de tal forma que:
a) Se puede saber quién recibe y qué derechos de acceso recibe.
b) Se puede saber quién ha hecho algo y qué ha hecho.

4. Las cuentas de usuario se gestionarán de la siguiente forma:
a) Cada cuenta estará asociada a un identificador único.
b) Las cuentas deben ser inhabilitadas en los siguientes casos: cuando el usuario deja la organización; cuando el usuario cesa en la función para la cual se requería la cuenta de usuario; o, cuando la persona que la autorizó, da orden en sentido contrario.
c) Las cuentas se retendrán durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas. A este periodo se le denominará periodo de retención.
(…)

4.2.5 Mecanismos de autenticación [op.acc.5]

dimensiones	I C A T		
nivel	bajo	medio	alto
	aplica	+	++

Los mecanismos de autenticación frente al sistema se adecuarán al nivel del sistema atendiendo a las consideraciones que siguen, pudiendo usarse los siguientes factores de autenticación:
– "algo que se sabe": contraseñas o claves concertadas.
– "algo que se tiene": componentes lógicos (tales como certificados software) o dispositivos físicos (en expresión inglesa, tokens).
– "algo que se es": elementos biométricos.

Los factores anteriores podrán utilizarse de manera aislada o combinarse para generar mecanismos de autenticación fuerte.

Las guías CCN-STIC desarrollarán los mecanismos concretos adecuados para cada nivel.

Las instancias del factor o los factores de autenticación que se utilicen en el sistema se denominarán credenciales.

Antes de proporcionar las credenciales de autenticación a los usuarios, estos deberán haberse identificado y registrado de manera fidedigna ante el sistema o ante un proveedor de identidad electrónica reconocido por la Administración. Se contemplan varias posibilidades de registro de los usuarios:
– Mediante la presentación física del usuario y verificación de su identidad acorde a la legalidad vigente, ante un funcionario habilitado para ello.
– De forma telemática, mediante DNI electrónico o un certificado electrónico cualificado.
– De forma telemática, utilizando otros sistemas admitidos legalmente para la identificación de los ciudadanos de los contemplados en la normativa de aplicación.

Nivel BAJO
a) Como principio general, se admitirá el uso de cualquier mecanismo de autenticación sustentado en un solo factor.
b) En el caso de utilizarse como factor "algo que se sabe", se aplicarán reglas básicas de calidad de la misma.
c) Se atenderá a la seguridad de las credenciales de forma que:
1. Las credenciales se activarán una vez estén bajo el control efectivo del usuario.
2. Las credenciales estarán bajo el control exclusivo del usuario.
3. El usuario reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida.
4. Las credenciales se cambiarán con una periodicidad marcada por la política de la organización, atendiendo a la categoría del sistema al que se accede.
5. Las credenciales se retirarán y serán deshabilitadas cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.

Nivel MEDIO

a) Se exigirá el uso de al menos dos factores de autenticación.
b) En el caso de utilización de "algo que se sabe" como factor de autenticación, se establecerán exigencias rigurosas de calidad y renovación.
c) Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo:
1. Presencial.
2. Telemático usando certificado electrónico cualificado.
3. Telemático mediante una autenticación con una credencial electrónica obtenida tras un registro previo presencial o telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de firma.

Nivel ALTO
a) Las credenciales se suspenderán tras un periodo definido de no utilización.
b) En el caso del uso de utilización de "algo que se tiene", se requerirá el uso de elementos criptográficos hardware usando algoritmos y parámetros acreditados por el Centro Criptológico Nacional.
c) Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial o telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de firma".

Així, poder establir de forma clara la traçabilitat dels accessos (qui, quan, a quina informació, etc), resulta una mesura necessària per assegurar la protecció de la informació objecte de tractament; cosa que no ocorria en el cas analitzat en què, tal com s'ha exposat a l'apartat de fets provats, no es va garantir que les credencials d'accés al sistema estiguessin sempre sota el control exclusiu dels usuaris (mesura op.acc.5); ja que, un cop subministrades les noves contrasenyes als usuaris, no es va establir un sistema o protocol pel qual aquests l'haguessin de canviar necessàriament en el seu primer accés al sistema informàtic. Així mateix, en la mesura que les contrasenyes no van estar sota el control exclusiu dels usuaris, també resultà afectada la mesura especificada a l'op.acc.1, ja que a partir d'aquell moment ja no seria possible poder establir de forma indubtable qui, què i quan s'ha fet una determinada actuació dins del sistema, el que resulta especialment clar en el cas de la persona que ocupava el càrrec de Responsable (...), en què els auditors van accedir al seu equip de treball utilitzant unes noves credencials que aquests li van assignar "ex novo".

Durant la tramitació d'aquest procediment s'ha acreditat degudament els fets descrits l'apartat de fets provats, que es consideren constitutius de la infracció prevista a l'article 83.4.a) de l'RGPD, que tipifica la vulneració de *"las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43",* entre les quals hi ha l'obligació descrita a l'article 32 referida a la seguretat del tractament.

Les conductes que aquí s'aborden s'han recollit com a infracció greu a l'article 73.f) de l'LOPDGDD), en la forma següent:

> *"f) La falta d'adopció de les mesures tècniques i organitzatives que siguin apropiades per garantir un nivell de seguretat adequat al risc del tractament, en els termes que exigeix l'article 32.1 del Reglament (UE) 2016/679".*

4. En no encabir-se l'FMMC en cap dels subjectes previstos a l'article 77.1 de l'LODGDD, resulta d'aplicació el règim sancionador general previst a l'article 83 de l'RGPD

L'article 83.4 de l'RGPD preveu una sanció de multa fins un màxim de 10.000.000 d'euros, o tractant-se d'una empresa, d'una quantia equivalent al 2% com a màxim del volum de negoci total anual global de l'exercici financer anterior, optant-se per la de major quantia. Això, sens perjudici que, amb caràcter addicional o substitutiu, es pugui aplicar alguna altra de les mesures previstes a l'article 58.2 RGPD.

En el present cas, tal com exposava la persona instructora en la proposta de resolució, escau descartar la possibilitat substituir la sanció de multa administrativa per la sanció d'amonestació prevista a l'article 58.2.b) RGPD, atès que la manca de control sobre les contrasenyes va afectar a nombroses persones treballadores de l'entitat i, en conseqüència, en relació amb totes aquestes persones no es va poder establir de forma clara la traçabilitat dels accessos al sistema d'informació de l'FMMC.

Un cop descartat que procedeixi substituir la sanció de multa administrativa per una amonestació, correspon determinar la quantia de la multa administrativa que correspon imposar. Segons el que estableix l'article 83.2 de l'RGPD, i també de conformitat amb el principi de proporcionalitat consagrat a l'article 29 de la Llei 40/2015, tal com indicava la instructora en la proposta de resolució, escau imposar la sanció de 2.500 euros (dos mil cinc-cents euros). Aquesta quantificació de la multa es basa en la ponderació entre els criteris agreujants i atenuants que a continuació s'indiquen.

Com a criteris atenuants, s'observa la concurrència de les circumstàncies següents, totes elles invocades per l'FMMC:

- La naturalesa, gravetat i duració de la infracció, tenint en compte la naturalesa, abast i propòsit de l'operació de tractament de que es tracti, així com el número de persones interessades afectades (art. 83.2.a/). És té aquí en consideració que no es té constància de cap accés indegut per part dels auditors (únics que coneixien les contrasenyes de les persones treballadores) als sistemes d'informació, i que els fets objecte d'imputació van derivar d'una actuació puntual i aïllada en el temps (83.2.a RGPD).

- La manca d'intencionalitat (art.83.2.b RGPD).

- L'adhesió per part de l'FMMC al codi de conducta de la Unió Catalana d'Hospitals (art. 83.2.j RGPD).

- La manca de constància de l'obtenció de beneficis com a conseqüència de la infracció (art. 83.2.k RGPD i 76.2.c LOPDGDD).

- La naturalesa de l'entitat de Fundació privada sense ànim de lucre -art. 1 dels seus Estatuts- (art. 83.2.k RGPD).

- Que en els dos darrers exercicis comptables l'FMMC ha tingut pèrdues (art. 83.2.k RGPD).

Per contra, no pot tenir en compte altres circumstàncies atenuants invocades per l'entitat, per les raons que seguidament s'exposen:

- Grau de cooperació amb l'autoritat de control. Al respecte val a dir que el sol fet d'haver contestat els requeriments d'aquesta Autoritat en la fase d'informació prèvia, no justificaria l'aplicació de l'atenuant prevista a la lletra f) de l'article 83.2; essencialment perquè contestar als dits requeriments és una obligació de les entitats subjectes al seu àmbit d'actuació (article 19 de la Llei 32/2010) i el no fer-ho pot ser constitutiu d'infracció.

- Caràcter no continuat de la infracció. L'FMMC advoca per l'aplicació d'aquest atenuant (76.2.a LOPDGDD) ja que la seva actuació va ser una "errada puntual". Al respecte cal dir que el fet que es tractés d'una actuació puntual en el temps és una circumstància que ja ha estat tinguda en compte en el primer dels atenuants relacionats a l'apartat anterior -art. 83.2.a RGPD-.

- La manca d'infraccions anteriors en matèria de protecció de dades. Respecte a aquesta circumstància val a dir que no es pot aplicar com a criteri atenuant, ja que és obligació de les entitats que tracten dades personals complir amb la normativa; motiu pel qual si concorregués tal circumstància -que no es el cas- actuaria com a criteri agreujant.

- Actuació de l'FMMC *"ràpida i eficaç",* tendent a evitar *"una fuita de dades",* circumstància que l'FMMC encabeix en la circumstància prevista en l'article 83.2.c) de l'RGPD [*"cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados"]*. Aquest criteri atenuant seria d'aplicació quan l'entitat hagués dut a terme actuacions per pal·liar els efectes o perjudicis de la infracció comesa, i l'FMMC no es refereix a actuacions preses en aquest sentit, sinó que el que fa és explicar el perquè va a dur a terme les actuacions que, com s'ha vist, van comportar la vulneració de mesures de seguretat que són, precisament, les que han derivat en la incoació d'aquest procediment sancionador.

En contraposició a les causes atenuants exposades, concorre el següent criteri que opera en sentit agreujant, i que s'ha tingut en compte per fixar l'import de la multa.

- La vinculació de l'activitat de l'FMMC amb la realització de tractaments de dades personals (art. 83.2.k de l'RGPD i 76.2.b/ de l'LOPDGDD).

5. D'altra banda, de conformitat amb l'article 85.3 de l'LPAC i tal com s'avançava a l'acord d'iniciació i també a la proposta de resolució, si abans de la resolució del procediment sancionador l'entitat imputada reconeix la seva responsabilitat o fa el pagament voluntari de la sanció pecuniària, escau aplicar una reducció del 20% sobre l'import de la sanció provisionalment quantificada. Si hi concorren els dos casos esmentats, la reducció s'aplica de forma acumulada (40%).

Com s'ha avançat, l'efectivitat de les reduccions esmentades està condicionada al desistiment o la renúncia de qualsevol acció o recurs per la via administrativa contra la sanció (art. 85.3 de l'LPAC, *in fine*).

Doncs bé, tal com s'ha indicat en els antecedents, per mitjà d'escrit de 17/06/2022, l'entitat imputada va reconèixer la seva responsabilitat. Així mateix, en data 19/07/2022 ha abonat de manera avançada 1.500 euros (mil cinc-cents euros), corresponents a la quantia de la sanció resultant un cop aplicada la reducció acumulada del 40%.

6. Davant la constatació de les infraccions previstes a l'art. 83 de l'RGPD en relació amb fitxers o tractaments efectuats per entitats no incloses a l'article 77.1 de l'LODGDD, l'article 21.3 de la Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades, faculta la directora de l'Autoritat perquè la resolució que declara la infracció estableixi les mesures escaients perquè cessin o se'n corregeixin els efectes. En el cas present però, no cal requerir l'adopció de cap mesura correctora ja que l'entitat en el si d'aquest procediment ha dut a terme la mesura proposada per la instructora, consistent en certificar que *"tot aquell personal a qui els auditors van facilitar una contrasenya d'accés als sistemes d'informació de l'entitat, el sistema informàtic els ha forçat a canviar-la per una altra personal i intransferible"*.

Per tot això, resolc:

1. Imposar a la Fundació de Malalts Mentals de Catalunya la sanció consistent en una multa de 2.500 euros (dos mil cinc-cents euros), com a responsable d'una infracció prevista a l'article 83.4.a) en relació amb l'article 32, ambdós de l'RGPD.

No cal requerir mesures correctores per corregir els efectes de la infracció, de conformitat amb el que s'ha exposat al fonament de dret 6è.

2. Declarar que la Fundació de Malalts Mentals de Catalunya ha fet efectiu el pagament avançat de 1.500 euros (mil cinc-cents euros), que correspon a l'import total de la sanció imposada, un cop aplicat el percentatge de deducció del 40% corresponent a les reduccions previstes a l'article 85 de la LPAC.

3. Notificar aquesta resolució a la Fundació de Malalts Mentals de Catalunya.

4. Ordenar que es publiqui aquesta resolució al web de l'Autoritat (apdcat.gencat.cat), de conformitat amb l'article 17 de la Llei 32/2010, de l'1 d'octubre.

Contra aquesta resolució, que posa fi a la via administrativa d'acord amb els articles 26.2 de la Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades, i 14.3 del Decret 48/2003, de 20 de febrer, pel qual s'aprova l'Estatut de l'Agència Catalana de Protecció de Dades, l'entitat imputada pot interposar, amb caràcter potestatiu, un recurs de reposició davant la directora de l'Autoritat Catalana de Protecció de Dades, en el termini d'un mes a comptar des de l'endemà de la seva notificació, d'acord amb el que preveuen l'article 123 i següents de l'LPAC. També pot interposar directament un recurs contenciós administratiu davant els jutjats contenciosos administratius, en el termini de dos mesos a comptar des de l'endemà de la seva notificació, d'acord amb els articles 8, 14 i 46 de la Llei 29/1998, de 13 de juliol, reguladora de la jurisdicció contenciosa administrativa.

Si l'entitat imputada manifesta a l'Autoritat la seva intenció d'interposar un recurs contenciós administratiu contra la resolució ferma en via administrativa, la resolució se suspendrà cautelarment en els termes previstos a l'article 90.3 de l'LPAC.

Igualment, l'entitat imputada pot interposar qualsevol altre recurs que consideri convenient per defensar els seus interessos.

La directora,