

Identificació de l'expedient

Resolució del procediment sancionador núm. PS 39/2024, referent a l'Institut Josep Puig i Cadafalch del Departament d'Educació.

Antecedents

1. En data 03/07/2022, va tenir entrada a l'Autoritat Catalana de Protecció de Dades un escrit de denúncia contra l'Institut Josep Puig i Cadafalch del Departament d'Educació (d'ara endavant, l'institut), amb motiu d'un presumpte incompliment de la normativa sobre protecció de dades personals.

En concret, la denunciant exposava que, en data (...) de 2022, no va poder accedir al seu compte de correu electrònic gestionat per l'institut on havia treballat (...), tot i que el coordinador informàtic li va comentar que el seu compte no es tancaria. Un tècnic de la comissió informàtica va poder comprovar que el compte s'havia inhabilitat i li va tornar a activar, però tot i això no hi va poder accedir atès que s'havia canviat la contrasenya. La persona denunciant exposa que, un cop restablerta la contrasenya, va accedir al seu compte de correu electrònic i va comprovar que algú hi havia accedit sense el seu permís, va canviar la contrasenya i va enviar a la paperera un correu d'alerta de seguretat l'1 de juliol, a les 8:14 hores.

Per tal d'acreditar aquests fets, la denunciant aportava una còpia del correu electrònic enviat a l'institut; on s'exposaven els fets; una captura de pantalla del correu d'alerta de seguretat, desat a la paperera; i una captura de pantalla d'un intent d'accés al seu compte, amb l'avís que la contrasenya s'havia canviat feia 11 hores.

2. L'Autoritat va obrir una fase d'informació prèvia (núm. IP 247/2022), d'acord amb el que preveuen 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 (LPAC), per determinar si els fets eren susceptibles de motivar la incoació d'un procediment sancionador.
3. En aquesta fase d'informació, en data 12/01/2024 es va requerir l'entitat denunciada perquè informés si es va inhabilitar el compte de correu, si es va canviar la contrasenya i si es va enviar un correu d'alerta a la paperera, qui va ser la persona autoritzada a fer-ho i per quins motius i amb quina base jurídica. Que informés si es proporciona al personal informació sobre les regles d'ús dels mitjans electrònics i sobre la política de mesures de control, i quin és el protocol i termini per donar de baixa un compte de correu electrònic per cessament de la relació laboral.
4. En data 26/01/2024, l'institut va respondre el requeriment i va exposar el següent:
 - El primer dia de curs sempre es fa un claustre on es facilita i explica la Guia del professorat, i s'hi especifiquen les normes d'organització i funcionament de centre (NOFC).

- Les NOFC són públiques; són a la web del centre i a la plataforma de gestió del professorat iEduca. La denunciante exercia com a (...), càrrec que comporta la revisió constant d'aquests documents i, per tant, n'era coneixedora.
- L'article 60 de les NOFC, en la seva versió aprovada el 20/09/2021, estableix que: "El centre gestionarà el correu corporatiu. En cas de que es requereixi el centre podrà accedir a qualsevol correu corporatiu i a la informació que hi contingui tant de correu com de totes les aplicacions relacionades amb el compte corporatiu."
- El compte de correu és corporatiu i, des del moment que s'assigna a un usuari concret, el centre mai hi accedeix d'acord amb la normativa de protecció de dades. No obstant això, en determinades circumstàncies com ara el cessament de la relació laboral, o indicis d'ús irregular, l'accés pot ser legítim atès que la titularitat del compte és de l'institut, d'acord amb les NOFC i subsidiàriament la instrucció 8/2020, de 24 de novembre, sobre l'ús de les tecnologies de la informació i la comunicació a l'Administració de la Generalitat de Catalunya, tenint com a base la legislació laboral vigent.
- El compte d'usuari engloba l'accés a diferents aplicacions i unitats d'emmagatzematge amb informació. En data (...) de 2022, quan la denunciante ja no formava part de la plantilla de treballadors del centre, un membre de la direcció que també forma part de la comissió informàtica va suspendre el seu compte.
- La suspensió del compte un cop la denunciante ja no era professora del centre, i tenint en compte l'actitud de la professora en les darreres setmanes de treballar al centre, es va fer per evitar la pèrdua de continguts, evitar accessos indeguts a dades sensibles de les quals disposava pel seu càrrec i disposar de l'accés per poder recuperar informació que afectava al centre.
- La contrasenya la va canviar un membre responsable de la comissió d'informàtica en l'exercici de les funcions que té autoritzades, d'acord amb les NOFC i la instrucció 8/2020, de 24 de novembre, sobre l'ús de les TIC a la Generalitat de Catalunya.
- Desconeixem el motiu pel que el correu d'alerta va arribar a la paperera.
- El compte de correu del domini inspuig.org és un correu corporatiu de titularitat del centre, i es facilita al professorat i alumnat perquè en facin ús per a tasques educatives.
- Un cop la docent ja no era treballadora del centre, únicament hi va accedir el responsable TIC per recuperar la informació pertanyent al centre i exercir les funcions ordinàries que li corresponen, cada vegada que hi ha canvis de professorat. No hi ha accedit cap altra persona.
- Poden accedir als comptes d'usuari els membres de direcció, el coordinador informàtic i els membres de la comissió informàtica, sempre en compliment de les NOFC. És responsabilitat de cada docent eliminar dels comptes de correu que han tingut assignats la informació i totes les dades personals que els concerneixen, abans de marxar definitivament del centre.

- El motiu de l'accés al compte va ser exclusivament obtenir materials i continguts dels cursos de *classroom* de batxillerat de l'assignatura de tecnologia i robòtica, per poder-los facilitar al nou professorat. L'(...)de 2022, un membre responsable de la comissió d'informàtica va accedir al compte per traspasar la informació de les *classrooms* de batxillerat, però per raons de servei va haver de posposar el traspàs de la informació per al dilluns següent. Durant el cap de setmana, un altre membre de la comissió d'informàtica, de manera unilateral i sense consultar, va tornar a donar accés al compte a la persona denunciada, la qual va entrar de manera irregular al compte del centre podent accedir a totes les dades. Es va demanar que no es fessin accions sobre aquest compte i ja no s'hi va accedir mai més, ni s'ha recuperat el material didàctic de batxillerat.
 - Els comptes no es donen de baixa. Inicialment no s'eliminen, sinó que se suspenden per si cal accedir-hi per recuperar informació, bàsicament *classrooms*. Donar de baixa el compte implicaria esborrar-lo totalment, i en casos concrets el professorat marxa temporalment i quan torna es reactiva.
5. En data 11/03/2024, es va tornar a requerir l'entitat denunciada perquè precisés la seva resposta en relació amb:
- Si hi ha alguna altra norma o document que estableixi expressament i concretament que el correu corporatiu és exclusivament professional.
 - Si hi ha alguna altra norma o document que estableixi les actuacions que es duen a terme sobre els comptes corporatius, per raó de cessament de la relació laboral.
 - Si es va informar la denunciada que el centre accediria al seu compte corporatiu i l'abast i els motius de l'accés.
 - Si, després del cessament, es va donar a la denunciada l'opció de recuperar contingut personal del seu compte.
 - Els motius que van impedir que s'accedís als materials i continguts de *classroom* de batxillerat en presència de la denunciada i prèviament al seu cessament.
6. En data 22/03/2024, l'institut va respondre el requeriment a través d'un escrit en què exposava el següent:
- A part de l'article 60 de les NOFC, quan arriba el professorat nou se li donen les claus per accedir a la part digital; es verbalitza que el correu és estrictament professional i també es concreta al correu genèric de benvinguda. S'aporta còpia d'un correu de data 28/09/2022 de benvinguda a un nou professor, on s'exposa expressament que el correu corporatiu "serà d'ús estrictament professional."
 - A les NOFC queda especificat que el centre pot accedir als comptes corporatius, si ho necessita.
 - El cap d'estudis i el coordinador pedagògic li van demanar reiteradament a la denunciada que, abans de marxar, deixés els *classrooms* que tenia sobre robòtica, per poder valorar-ne el contingut i designar el professorat més adient. L'(...), quan la

denunciant ja no era treballadora del centre i no havia atès les reiterades peticions del centre, es va suspendre el compte per:

- a) Evitar la pèrdua de continguts.
 - b) Evitar accessos indeguts a dades sensibles als que disposava pel seu càrrec.
 - c) Disposar de l'accés, per part del centre, per recuperar la informació.
- La denunciante ha tingut i té accés al compte actualment; pot obtenir informació propietat del centre i dels alumnes que ha quedat en aquest correu.
 - Res impedia accedir als materials i continguts del compte corporatiu en presència de la denunciante i abans del seu cessament. Però, creient que és la manera més correcta d'actuar, es demana al professorat la informació (la qual cosa es va fer verbalment, en reiterades ocasions) i, si esgotat el termini i la relació amb el centre no ho facilita, com a última instància el centre es veu obligat a accedir-hi.
7. En data 25/04/2024, la directora de l'Autoritat Catalana de Protecció de Dades va acordar iniciar un procediment sancionador contra l'Institut Josep Puig i Cadafalch del Departament d'Educació, per una presumpta infracció prevista a l'article 83.4.a, en relació amb els articles 25 i 32; tots ells 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 (RGPD). Aquest acord d'iniciació es va notificar a l'entitat imputada en data 03/05/2024.
8. 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 convenientes per defensar els seus interessos. El termini s'ha superat amb escreix i no s'han presentat al·legacions.

Fets provats

Un cop finalitzada la relació laboral amb la denunciante, l'institut va accedir al seu compte de correu corporatiu sense la seva presència, per recuperar materials i continguts de *classroom* de batxillerat.

No es va utilitzar cap procediment ni es van aplicar garanties que estiguessin previstes normativament. Res impedia accedir als materials i continguts del compte corporatiu en presència de la denunciante i prèviament al seu cessament, que hauria estat una mesura més moderada per aconseguir el propòsit de recuperar material amb la mateixa eficàcia.

Igualment, un membre de la comissió d'informàtica, unilateralment i sense consultar, va tornar a donar accés al compte a la persona denunciante, quan ja no era treballadora del centre. Actualment encara hi té accés i pot obtenir informació propietat del centre i dels alumnes que ha quedat en aquest compte.

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.

2. D'acord amb l'article 64.2.f de l'LPAC i de conformitat amb el que s'indica a l'acord d'iniciació d'aquest procediment, escau dictar aquesta resolució sense una proposta de resolució prèvia, atès que l'entitat imputada no ha formulat alegacions a l'acord d'iniciació. Aquest acord contenia un pronunciament precís sobre la responsabilitat imputada.
3. En relació amb la conducta descrita a l'apartat de fets provats, cal acudir a l'article 25.1 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 dades (RGPD), que estableix que el responsable ha d'aplicar i integrar les garanties necessàries en el tractament, a fi de complir els requisits del Reglament i de protegir els drets dels interessats. L'article 32 de l'RGPD estableix que el responsable i l'encarregat del tractament han d'aplicar les mesures tècniques i organitzatives adequades, per garantir un nivell de seguretat adequat als riscos de probabilitat i gravetat variables per als drets i les llibertats de les persones físiques; a l'hora d'avaluar l'adequació del nivell de seguretat, cal tenir en compte especialment la comunicació o l'accés no autoritzats a aquestes dades.

En relació amb l'accés que un membre de la comissió d'informàtica al compte corporatiu va tornar a donar a la denunciant quan aquesta ja no era treballadora del centre docent, unilateralment i sense consultar, l'article 32.4 de l'RGPD estableix que el responsable i l'encarregat del tractament han de prendre mesures per garantir que qualsevol persona que actua sota l'autoritat del responsable i que té accés a dades personals només pot tractar aquestes dades seguint instruccions del responsable, tret que hi estigui obligada en virtut del dret de la Unió o dels estats membres.

Cal circumscriure aquest cas al fet que ens trobem davant d'un correu corporatiu de titularitat de l'institut, el qual es va inhabilitar per causa del cessament de la persona treballadora. Posteriorment, l'institut hi va accedir per recuperar continguts pel funcionament eficient del centre, sense disposar d'un procediment concret i conegut, amb totes les garanties, per accedir a comptes de persones que han cessat la seva relació laboral. I, d'acord amb el que manifesta l'institut, la ex treballadora va tornar a accedir al compte i actualment encara té accés.

A aquests efectes, resulten d'especial interès la Recomanació 1/2013 de l'Autoritat Catalana de Protecció de Dades, sobre l'ús del correu electrònic en l'àmbit laboral, així com el "Manual de bon ús del correu electrònic. Guia per a les persones treballadores per a la protecció de la privacitat en l'ús del correu electrònic". També, els dictàmens CNS 36/2022 i 7/2023 d'aquesta Autoritat, disponibles al web www.apdcat.cat.

D'acord amb el punt 4 de l'apartat III de la Recomanació 1/2013, quan una persona treballadora deixa de prestar els seus serveis l'òrgan competent en matèria de gestió de personal ha de comunicar-ho immediatament al responsable de seguretat, per tal que es revoquin els codis d'usuari i les contrasenyes del treballador. En aquest mateix sentit, el dictamen núm. CNS 36/2022 exposa al fonament jurídic III que, des del punt de vista de la protecció de dades, **l'extinció de la relació laboral ha de comportar que l'ocupador**

cessi en el cessament en el tractament de la informació personal de la persona treballadora i, per tant, també de l'adreça del compte de correu corporatiu que se li hagi facilitat per desenvolupar les seves tasques professionals. Això, ja que en extingir-se la relació laboral s'extingeix alhora la finalitat que va justificar-ne el tractament, d'acord amb els principis de limitació de la finalitat i del termini de conservació de l'article 5.1, lletres *b* i *e*, de l'RGPD.

Per altra banda, de l'article 87.3 de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD), es desprèn per a aquest cas que l'institut ha de comptar amb una política o manual que reculli **els criteris o normes clares** sobre les condicions d'ús dels sistemes d'informació i dispositius digitals proporcionats al seu personal. Aquesta política ha d'advertir dels mecanismes de control sobre el seu ús que pugui afectar la privacitat de les persones treballadores, les conseqüències que se'n poden derivar i les garanties per a les persones treballadores, en especial el dret d'informació.

D'aquesta manera, l'institut només pot accedir als comptes de correu electrònic facilitats als seus treballadors quan aquest accés estigui justificat **i no hi hagi cap altre mecanisme que permeti assolir l'objectiu perseguit sense necessitat d'accedir-hi**. I aquest accés s'ha de dur a terme d'acord amb les normes d'ús del correu electrònic aprovades prèviament per l'institut. La informació prèvia d'aquestes normes a les persones treballadores resulta cabdal per poder considerar legítim que l'institut controli les eines digitals i l'ús que se'n fa (art. 5.1.a i 6 RGPD).

En els mateixos termes amb què s'exposa al dictamen CNS 7/2023 d'aquesta Autoritat, la jurisprudència ha admès que l'ocupador pot establir controls sobre l'ús de les eines que posa a disposició dels treballadors, per coordinar i garantir la continuïtat de l'activitat laboral en els supòsits d'absències dels treballadors, per protegir els sistemes d'informació; també, per prevenir les responsabilitats que es puguin derivar per a l'ocupador de formes il·lícites d'ús enfront de terceres persones. Ara bé, **l'ens ha de concretar aquestes normes d'ús de les eines i informar-ne adequadament els treballadors**.

Es constata que l'institut disposa de les normes d'organització i funcionament del centre (NOFC), les quals són públiques i estan disponibles a la web del centre, així com a la plataforma de gestió del professorat iEduca. A l'article 60 del capítol 13 de les NOFC_convivència, sobre el correu electrònic corporatiu, s'estableix que "el centre gestionarà el correu corporatiu. En cas que es requereixi el centre podrà accedir a qualsevol correu corporatiu i a la informació que hi contingui tant de correu com de totes les aplicacions relacionades amb el compte corporatiu."

L'institut considera que, d'acord amb les NOFC i subsidiàriament la Instrucció 8/2020, de 24 de novembre, sobre l'ús de les tecnologies de la informació i la comunicació a l'Administració de la Generalitat de Catalunya, tenint com a base la legislació laboral vigent, l'accés al correu corporatiu de l'extreballadora pot ser legítim, atès que la titularitat del compte és de l'institut. En la seva resposta, el centre docent manifesta que "és responsabilitat de cada docent eliminar la informació i totes les dades personals que els concerneixen dels comptes de correu que han tingut assignats abans de marxar definitivament del centre". No obstant això, no hi ha cap norma interna que estableixi un procediment concret i amb totes les garanties on es concreti el que manifesta l'institut en la seva resposta.

El punt 8 de la Instrucció 8/2020, de 24 de novembre, estableix que en l'àmbit professional s'han d'utilitzar les eines de comunicació digital corporativa, com ara el correu electrònic, d'acord amb les guies d'ús disponibles i les regles de seguretat previstes de cada eina. El mateix apartat també estableix que el personal pot fer un ús privat de les eines de comunicació digital corporatives, sempre que es faci de manera excepcional, no abusiva i circumstancial. També cal tenir en compte que, **fins i tot respecte dels comptes de correu dels quals s'estableixi un ús exclusivament professional, la persona treballadora no sempre podrà evitar que terceres persones li trametin missatges de caràcter personal.**

I en relació amb la pèrdua de la vinculació del personal amb l'Administració: el punt 12.3 de la Instrucció esmentada estableix que "l'Administració de la Generalitat podrà recuperar la informació dels serveis informàtics que la Generalitat de Catalunya va posar a la disposició del personal per a l'exercici de les seves funcions **mitjançant procediments i garanties previstos en la normativa vigent.**"

En els mateixos termes en què s'exposen en el dictamen CNS 36/2022 d'aquesta Autoritat, i tenint en compte l'apartat 14.5 de la Recomanació CM/REC (2015) 5, d'1 d'abril de 2015, del Comitè de Ministres del Consell d'Europa, relativa al tractament de dades personals en el context de la relació de treball, en els casos de cessament de la relació laboral en què calgui recuperar informació vinculada a l'activitat professional de la persona treballadora que causa baixa, **sempre que sigui possible l'accés s'ha de dur a terme abans del dia en què se cessa efectivament la relació laboral, davant la presència de la persona treballadora i, si escau, d'un tercer.**

En aquest cas, a l'efecte de garantir que la informació es tracta correctament, és important **tenir un procediment intern sobre l'ús del correu corporatiu, que tingui en compte aquesta i altres circumstàncies**, on prèviament s'informi els treballadors de les **mesures concretes** que es poden adoptar en aquest sentit.

Per tot el que s'ha exposat, es constata que l'institut no disposa d'un procediment concret per accedir a comptes corporatius de persones extreballadores, amb totes les garanties. Per contra, **res no impedia a accedir a la informació que es volia extreure del compte de correu corporatiu de la treballadora, en la seva presència i abans del seu cessament.**

En aquest sentit, és especialment rellevant la sentència del Tribunal Europeu de Drets Humans (TEDH), cas Barbulescu, de 5 de setembre de 2017. En aquesta sentència, s'exposa que un dels factors a tenir en compte en la ponderació obligada d'interessos, en un cas com el que ens ocupa, és la inexistència o existència de mitjans menys intrusius per aconseguir el mateix objectiu. Això sintonitza completament amb el "judici de necessitat" que estableix la doctrina jurisprudencial sobre el principi de proporcionalitat (per totes, la sentència del Tribunal Suprem de 02/07/2007 i la interlocutòria del Tribunal Constitucional de 26/02/2007), en el sentit que no hi hagi cap altra mesura més moderada per aconseguir el propòsit amb eficàcia idèntica.

En definitiva, l'accés de l'institut al compte corporatiu de l'extreballadora no ha estat proporcionat, no hi ha hagut cap procediment ni garanties per accedir-hi i hi havia mesures menys restrictiva de drets, com ara la d'accedir al compte en presència de la treballadora i abans del seu cessament.

Per altra banda, l'acció unilateral i sense consultar amb el responsable del tractament del membre de la comissió d'informàtica que li va donar accés al compte corporatiu, quan ja no era treballadora de l'institut, i el fet que actualment la persona extreballadora encara té accés al compte, comporta una vulneració en relació amb la seguretat del tractament que estableix l'article 32 de l'RGPD.

Durant la tramitació d'aquest procediment s'ha acreditat el fet descrit a l'apartat de fets provats, que és constitutiu de la infracció prevista a l'article 83.4.a de l'RGPD, que tipifica com així la vulneració de "las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43."

La conducta que aquí s'aborda s'ha recollit com a infracció greu a l'article 72.1.i de l'LOPDGDD, de la manera següent: "La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño, así como la no integración de las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25 del Reglamento (UE) 2016/679." I "f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679."

4. L'article 77.2 de l'LOPDGDD disposa que, en el cas d'infraccions comeses pels responsables o encarregats enumerats a l'article 77.1 de la mateixa llei, l'autoritat de protecció de dades competent:

"(...) ha de dictar una resolució que declari la infracció i estableixi, si s'escau, les mesures que convingui adoptar perquè cessi la conducta o es corregeixin els efectes de la infracció que s'hagi comès, a excepció de la que preveu l'article 58.2.i del Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016.

La resolució s'ha de notificar al responsable o l'encarregat del tractament, a l'òrgan del qual depengui jeràrquicament, si s'escau, i als afectats que tinguin la condició d'interessat, si s'escau."

En termes similars a l'LOPDGDD, l'article 21.2 de la Llei 32/2010 determina el següent:

"2. En el cas d'infraccions comeses amb relació a fitxers de titularitat pública, el director o directora de l'Autoritat Catalana de Protecció de Dades ha de dictar una resolució que declari la infracció i estableixi les mesures a adoptar per a corregir-ne els efectes. (...)".

En virtut d'aquesta facultat, escau requerir a l'Institut Josep Puig i Cadafalch perquè al més aviat possible, i en tot cas en el termini màxim de 6 mesos a comptar a partir de l'endemà de la notificació de la resolució que es dicti en aquest procediment:

- Elabori i/o modifiqui les NOFC, per establir una política o manual que reculli els criteris, protocols o normes clares sobre les condicions d'ús dels comptes corporatius, amb uns procediments concrets per als casos en què el centre hagi d'accedir a aquests comptes, ja sigui per cessament de la persona treballadora o per altres circumstàncies.

També, que tots els treballadors coneguin prèviament les mesures concretes que s'adoptin.

- Que es revoquin immediatament els codis d'usuari i les contrasenyes de l'extreballadora, o se li suspengui l'accés al compte corporatiu. Això, sens perjudici de la sol·licitud d'accés que pugui fer l'extreballadora, per poder recopilar la informació estrictament personal que hi pugui haver, amb la supervisió d'un responsable del centre.

Un cop s'hagin adoptat aquestes mesures correctores en el terminis assenyalats, cal que en els 10 dies següents l'institut n'informi l'APDCAT, sense perjudici de la facultat d'inspecció d'aquesta Autoritat per fer les verificacions corresponents.

Resolució

Per tot això, resolc:

1. Declarar que l'Institut Josep Puig i Cadafalch, del Departament d'Educació, ha comès una infracció prevista a l'article 83.4.a en relació als articles 25 i 32, tots ells de l'RGPD.
2. Requerir l'Institut Josep Puig i Cadafalch perquè adopti les mesures correctores assenyalades al fonament de dret 4t i acrediti davant d'aquesta Autoritat les actuacions dutes a terme per complir-les.
3. Notificar aquesta resolució a l'Institut Josep Puig i Cadafalch, del Departament d'Educació.
4. Comunicar la resolució al Síndic de Greuges, de conformitat amb el que preveu l'article 77.5 de l'LOPDGDD.
5. 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 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, amb caràcter potestatiu l'entitat imputada pot interposar un recurs de reposició davant la directora de l'Autoritat Catalana de Protecció de Dades, en el termini d'un mes a comptar a partir de l'endemà de la seva notificació, d'acord amb el que preveuen l'article 123 i següents de la Llei 39/2015. També es pot interposar directament un recurs contenciós administratiu davant els jutjats contenciosos administratius de Barcelona, en el termini de dos mesos a comptar a partir 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