En aquesta resolució s'han ocultat les mencions a l'entitat afectada per tal de donar compliment a l'art. 17.2 de la Llei 32/2010, atès que en cas de revelar el nom de l'entitat afectada, es podrien identificar també les persones físiques afectades.

Identificació de l'expedient

Resolució del procediment sancionador núm. PS 42/2024, referent a (...) del Departament d'Educació i Formació Professional.

Antecedents

1. En data 04/03/2023, va tenir entrada a l'Autoritat Catalana de Protecció de Dades una denúncia contra (...) del Departament d'Educació i Formació Professional (d'ara endavant, l'institut), amb motiu d'un presumpte incompliment de la normativa sobre protecció de dades personals. El Sr. (...) (d'ara endavant, el denunciant) exposava el següent:

a. Que una persona de l'institut en què treballava li va suplantar la identitat en el seu compte de "Google Workspace G Suites", amb domini "@(...)".

b. Que l'administrador dels comptes de Google Workspace G Suites de l'institut, que alhora és el coordinador informàtic, Sr. (...)(d'ara endavant, l'administrador), va modificar la seva contrasenya d'accés al seu compte. Això li va permetre accedir a totes les seves eines de Google, entre d'altres el seu compte de Gmail, i a tota la documentació emmagatzemada al núvol.

(Google Workspace G Suites –abans anomenat Google Apps- és un conjunt d'aplicacions ofimàtiques allotjades al núvol de Google, que té per objecte millorar l'operativa de les empreses).

c. Que el dia 07/12/2022 un professor acabat d'incorporar a l'institut, Sr. (...) (d'ara endavant, el professor substitut), li va enviar un correu electrònic en què li demanava que compartís amb ell unes "pràctiques d'aquest mòdul".

d. Que el dia 08/12/2022 el denunciant va donar accés als documents que el professor substitut li havia demanat i que el mateix dia, a les 12:25 hores, va rebre un correu electrònic d'aquest professor, creu que per error. Aquest correu anava adreçat a l'administrador i deia, literalment: "Hola (...) [administrador], ja no fa falta que facis res amb el correu del (...) [denunciant], ja que m'ha donat accés a totes les pràctiques. Gràcies."

e. Que disposava d'un missatge Google en què se l'informava que el dia 09/12/2022, a les 09:09 hores, l'administrador sol·licitava una petició de compartició de fitxer i que aquest és el darrer missatge que va rebre, abans del canvi de contrasenya.

f. Que, amb posterioritat al dia 09/12/2022, va intentar accedir al seu compte, sense èxit. Manifestava que, quan intentava accedir-hi, es mostrava un missatge de Google que deia que la contrasenya s'havia modificat feia 25 hores.

Juntament amb la denúncia aportava un dossier documental en què hi ha diverses captures d'imatge, entre d'altres les següents:

- El correu electrònic de 07/12/2022, referit en el punt 1.c.

- El correu electrònic de 08/12/2022, referit en el punt 1.d.

- El missatge de Google, referit en el punt 1.e.

- El missatge de Google, referit en el punt 1.f.

2. L'Autoritat va obrir una fase d'informació prèvia (núm. IP 122/2023), per determinar si els fets eren susceptibles de motivar la incoació d'un procediment sancionador, 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).

En aquesta fase d'informació, en data 29/02/2024 es va requerir l'institut perquè informés sobre els punts següents:

- Que confirmés o desmentís si des de l'institut es va canviar la contrasenya del compte d'usuari de Google Workspace G Suites del denunciant.

- Que, en cas de confirmar el punt anterior, indiqués en quina data i hora es va fer el canvi, especifiqués les raons per les quals es va modificar i quina seria la base jurídica que legitimaria aquesta acció per part de l'institut. Així mateix, se li demanava que indiqués si, atès que l'administrador es va atribuir accés a un compte d'un usuari individual, es van adoptar les mesures compensatòries adients en relació amb els riscos que implicava aquesta acció i que, en aquest cas, especifiqués quines.

- Que informés sobre si els empleats de l'institut signaven algun document o rebien instruccions en relació amb l'ús del compte de Google Workspace G Suites i que, en aquest cas, n'aportés un exemplar.

- Que especifiqués a quina documentació i/o informació allà desada es va accedir i que ho acredités mitjançant una evidència tècnica de traçabilitat. Així mateix, se li demanava que informés sobre si, a banda d'accedir a la documentació de Google Workspace G Suites, havia accedit a alguna altra aplicació del compte d'usuari del denunciant. En relació amb això, se li demanava que aportés una evidència.

- Que respongués les qüestions següents: a) quines persones podrien haver accedit a la informació; b) si, abans de l'accés, es va informar el denunciant que s'accediria al seu compte; i c) si es va oferir al denunciant ser present en el moment de l'accés i/o, en el seu defecte, fer-ho en presència d'un representant de les persones treballadores.

- Que expliqués les funcionalitats que aquest compte de Google Workspace G Suites prestava als seus empleats.

- Que, en cas de contestar negativament al punt 1, exposés quina explicació podia tenir el missatge de Google rebut pel denunciant, referent al canvi de contrasenya (punt 1.f), així com el contingut del correu del professor substitut de 08/12/2022 que, per error, va enviar al denunciant (punt 1.d).

3. En data 05/04/2024, atès que s'havia superat amb escreix el termini concedit sense que l'institut respongués el requeriment de 29/02/2024, aquesta Autoritat el va reiterar perquè en el termini de 5 dies hi donés resposta, amb l'advertència que si no ho complia podria incórrer en una infracció de la normativa de protecció de dades.

El termini es va superar amb escreix i l'institut no va respondre el requeriment.

4. En data 13/05/2024, la directora de l'Autoritat Catalana de Protecció de Dades va acordar iniciar un procediment sancionador contra (...) del Departament d'Educació i Formació Professional, per dues presumptes infraccions previstes a l'article 83.4.*a*, en relació amb els articles 25, 31 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 dades (RGPD)..

5. Aquest acord d'iniciació es va notificar a l'entitat imputada en data 16/05/2024 i 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.

6. En data 27/05/2024, en fase d'al·legacions a l'acord d'iniciació, la directora de l'institut va presentar un escrit d'al·legacions en el qual responia cadascuna de les qüestions incloses en el requeriment de 29/02/2024. En el seu escrit exposa el següent (la negreta és de l'APDCAT):

- Com a qüestió prèvia, pel que fa a la manca de resposta del requeriment durant el termini concedit en la fase d'informació prèvia, manifesta que no va tenir coneixement de la tramitació de la IP 122/2023 fins que no se li va notificar l'obertura del procediment sancionador PS 42/2024, el dia 16/05/2024. Exposa que el Departament d'Educació i Formació Professional, a qui correspon informar el centre implicat sobre els fets denunciats i notificacions d'aquesta Autoritat, no el va informar. Manifesta també que el departament li va dir que la manca d'informació es va produir degut a "un error de coordinació i malentès amb el Consorci d'Educació de Barcelona referent a la reassignació d'algunes funcions que en matèria de dades es va produir per aquelles dates entre ambdós organismes."

  Per aquest motiu, sol·licita que es tingui en compte aquesta al·legació i es descarregui de responsabilitat el centre, pel que fa a la manca de col·laboració amb aquesta Autoritat i la desatenció als seus requeriments. Així mateix, manifesta que des del moment en què va tenir coneixement d'aquest procediment, ha respost totes les qüestions abans que s'exhaurís el termini concedit.

- Pel que fa a si des de l'institut es va canviar la contrasenya del compte d'usuari de Google Workspace G Suites del denunciant, confirma que aquest fet es va produir. Però, per justificar el fet, explica que el personal de l'institut va insistir en reiterades

ocasions al denunciant per accedir al seu compte amb el seu permís i que, atès que no va donar cap resposta i que l'institut necessitava disposar dels materials didàctics per impartir el mòdul, el coordinador d'informàtica **va haver de fer "aquesta intervenció**, de manera proporcionada i limitada, per poder accedir a una carpeta i poder recuperar uns arxius de material de classe." Així mateix, afirma que aquest fet es va produir el 09/12/2022 a les 9:00 hores, aproximadament.

- Referent a quines eren les raons per les quals es va modificar la contrasenya i quina era la base jurídica que legitima aquesta acció, l'institut considera que la normativa de la funció pública i a la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD), preveuen que "l'ocupador pugui accedir als continguts derivats de l'ús dels mitjans digitals facilitats als treballadors per al control del compliment de les obligacions laborals i per garantir la integritat dels dispositius." I justifica que, en el cas que ens ocupa, **l'accés es va produir per assegurar "el bon funcionament dels sistemes d'informació i comunicació i dispositius digitals, fer un seguiment de la seva adequada utilització, així com detectar i respondre als possibles incidents de seguretat**."

  Explica que el coordinador informàtic va accedir als mòduls i materials que havia demanat el professor substitut i va poder comprovar que, realment, no es tenia accés als materials necessaris per poder impartir la matèria, que recalcava que eren del centre. Així, el coordinador va seguir les instruccions del sistema per sol·licitar l'accés al material i, seguidament, "**va canviar la contrasenya del compte del professor (...) [el denunciant] per poder entrar al seu compte**." I, un cop dins del compte, va acceptar les peticions de compartició de fitxers efectuades pel professor substitut i per la cap d'estudis. Afegeix que "també va identificar la carpeta de materials dels mòduls i **va atorgar accés a tot el professorat del centre**."

  A continuació, afirma que el coordinador va manifestar que **no va tornar a entrar** al compte.

- Pel que fa a si es van adoptar mesures compensatòries en relació amb l'accés al compte del denunciant, afirma que **no tenia constància que se n'hagués adoptat cap**. Així mateix, apunta que va tenir coneixement dels fets a través del denunciant, que va presentar un escrit per e-valisa en data 10/12/2022, amb l'assumpte "Apropiació indeguda compte Google (...)@(...) mitjançant canvi de contrasenya". En aquest escrit, exposava el següent (la negreta és de l'APDCAT):

  > "Soc (...) [el denunciant], l'any passat vaig impartir (...) i actualment exerceixo com a (...) adscrit a (...).
  >
  > El passat dijous vaig rebre per correu (...)@(...) una sol·licitud de part de (...) [el professor substitut], que actualment cursa el mòdul (...) per tal que compartís uns documents de pràctiques que tinc al Drive i que fins al moment compartia amb els alumnes dels meus antics grups. També vaig rebre una altra petició de (...) [l'administrador].
  >
  > Molt gentilment **vaig respondre al company i vaig accedir a compartir tots els documents que em va sol·licitar per tal que en fes una còpia i els fes servir a la seva practica docent.**

Hores després he rebut una notificació de Google alertant d'un canvi de contrasenya en el meu compte de informacions de caràcter sensible corresponents a alumnes que he tutoritzat, incloses dades mèdiques, documents de tutoria, calendaris, etc.

Val a dir que la conservació de les dades personals es troba regulada a la Llei 3/2018 de la LOPDGDD. En ella es defineix que ja es consideren dades personals les que continguin informació en text, imatge o àudio que permeti la identificació d'una persona. **Òbviament conservo documentació al meu compte email i compte Drive de gestions al centre, amb Secretaria i amb el Departament d'Educació que actualment es troben exposades a qui hagi fet el canvi de contrasenya que Google m'ha notificat, persona/es que desconec.**

Sense fer judicis previs sobre com s'ha dut a terme aquesta apropiació d'un compte personal existent, en lloc del seu esborrat, que és el que pertocaria, val a dir que és una pràctica il·legal que pot comportar seriosos problemes a les persones responsables de tal acte i a la institució que representen. A l'espera de què facis les investigacions oportunes sobre com s'ha dut a terme aquesta apropiació indeguda, poso en còpia de seguretat a la inspectora (...).

Es per això que sol·licito en primera instància als administradors del domini Google de (...), de (...) del qual ets Directora:

- L'eliminació del meu compte Google (...)@(...) i de totes les seves dades associades al seus serveis donat que conté dades personals pròpies i d'alumnes en exercici de les meves funcions docents, sense cap mena de còpia de seguretat. (...)."

- En relació amb si els empleats de l'institut signaven algun document o rebien instruccions sobre l'ús del compte de Google Workspace G Suites, exposa que s'informa oralment el professorat "que tots els documents que es treballen en els moodles de les assignatures han d'estar ubicats al drive corporatiu del centre, que el material dels mòduls professionals són de propietat del centre i han d'estar a disposició de tots els docents que en puguin necessitar fer ús", però que **no disposen de cap informació escrita**.

- Referent a quina era la documentació i/o informació específica a què es va accedir i que ho acredités mitjançant una evidència tècnica de traçabilitat, la directora afirma que **només es va accedir als "apunts que es necessitaven al Google Drive, per descarregar-los", però que aquesta aplicació ofimàtica no permet obtenir cap evidència de traçabilitat** de la descàrrega de fitxers. Afirma que "no es va fer cap acció que no fos la de permetre compartir el material sol·licitat del mòdul."

  Així mateix, posa de manifest que abans d'aquest accés **es va demanar al denunciant en reiterades ocasions que permetés ell mateix l'accés** al material i que, degut a la seva desatenció i a la necessitat de l'institut d'utilitzar els materials docents, es va produir el fet controvertit. En aquest sentit, exposa que l'accés del coordinador de l'institut es va fer "amb la intenció clara de compartir un material elaborat col·lectivament que ha d'estar a disposició de tot el professorat del centre." I també ressalta que la informació a la qual es va accedir no contenia dades personals

que esmentessin directament o indirectament cap persona, sinó que es tractava de material didàctic elaborat conjuntament pel professorat del centre educatiu.

- En relació amb quines persones podrien haver accedit a la informació, va respondre que "**per la informació de la que disposo únicament van accedir als materials de l'assignatura i es va fer la tramesa al professor que impartia el mòdul**."

- En relació amb el fet de si es va informar el denunciant prèviament a l'accés i si se li va oferir ser-hi present o, en el seu defecte, fer-ho en presència d'un representant de les persones treballadores, reitera que se li va demanar accés en diverses ocasions i que, en no donar-lo, el coordinador va considerar necessari accedir al seu compte. L'accés es va efectuar sense oferir-li ser-hi present.

- En relació amb quines eren les funcionalitats d'aquest tipus de compte de Google, va manifestar que era d'ús únicament laboral i que en aquest compte s'ubicaven "tots els materials d'elaboració del centre per poder impartir els mòduls professionals."

- Per concloure, manifesta literalment que "**el coordinador va fer una acció que no s'hauria d'haver produït, per això, i després de compartir-ho amb la inspecció, vaig procedir a fer una amonestació escrita** de la que adjunto l'assabentat."

  En aquesta amonestació escrita, de data 21/12/2022, la directora reconeix textualment que un treballador de l'institut "**ha accedit al compte corporatiu d'un company del centre sense el seu coneixement**" i que "**en cap cas havia d'accedir al compte del professor (...) [el denunciant] i s'hauria d'haver realitzat altres accions que no vulnerin la llei de protecció de dades**."

7. En data 29/05/2024, el Departament d'Educació i Formació Professional va presentar un escrit en què exposa que, degut a una confusió, no va remetre els requeriments notificats per aquesta Autoritat en la fase d'investigació prèvia IP 122/2023 (ni el de 29/02/2024, ni tampoc el posterior amb advertiment de 05/04/2024) al centre educatiu implicat. I que, per aquest motiu, l'institut no va respondre l'Autoritat dins del termini concedit. En base a això, demanava que es tingués en compte aquesta circumstància i es descarregués de responsabilitat l'institut, pel que fa a la imputació per la manca de col·laboració amb l'autoritat de control.

8. En data 02/10/2024, la persona 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 declarés que (...) del Departament d'Educació i Formació Professional havia incorregut en una infracció prevista a l'article 83.4.*a* en relació amb els articles 25 i 32, tots ells de l'RGPD.

Aquesta proposta de resolució es va notificar en data 03/10/2024 i es concedia un termini de 10 dies per formular al·legacions.

9. El termini s'ha superat amb escreix i no s'han presentat al·legacions.

Fets provats

Un treballador de (...) del Departament d'Educació i Formació Professional, concretament l'administrador dels comptes de Google Workspace G Suites dels empleats de l'institut (amb el domini "@(...)"), va modificar la clau d'accés del compte del denunciant, també treballador de l'institut, sense el seu permís ni coneixement.

Aquest fet va comportar que l'administrador pogués accedir a totes les aplicacions de Google Workspace G Suites del denunciant i que, de fet, accedís a la documentació emmagatzemada en el núvol del compte del denunciant i sol·licités la compartició de fitxer.

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. L'entitat imputada no ha formulat al·legacions a la proposta de resolució, però sí que ho va fer a l'acord d'iniciació. Respecte d'això, es considera oportú reiterar a continuació el més rellevant de la resposta motivada de la persona instructora a aquestes al·legacions.

   "**2.1. Sobre la infracció de l'article 31 de l'RGPD, relativa a la manca de col·laboració amb l'autoritat de control.**

   Inicialment, a l'acord d'iniciació, aquesta Autoritat va imputar al departament la infracció de l'article 83.4.*a* en connexió amb l'article 31 de l'RGPD, per la manca de col·laboració amb aquesta Autoritat. Aquesta imputació es basava en el fet que l'institut no va respondre al requeriment d'informació d'aquesta Autoritat de 29/02/2024, ni tampoc al posterior requeriment amb advertiment de 05/04/2024, notificats durant la fase d'informació prèvia IP 122/2023.

   L'institut s'ha pronunciat respecte d'aquesta qüestió i ha manifestat que no van poder respondre dins del termini atorgat perquè fins el dia 16/05/2024 no van tenir coneixement del present procediment sancionador ni de l'existència de la fase d'informació prèvia. I que, des del moment en què van tenir coneixement – durant la fase d'al·legacions a l'acord d'iniciació - van procedir a respondre el requeriment immediatament i sense exhaurir el termini concedit. També afirma que el departament li va reconèixer que la falta de notificació dels requeriments es va produir per un error seu.

   En base a l'exposat, escau tenir en compte que, des del moment en què l'institut implicat va saber que havia estat requerit per aquesta Autoritat per contestar a unes qüestions que eren rellevants per investigar el fet denunciat, va col·laborar de manera immediata. En conseqüència, no escau mantenir la imputació referida a la manca de col·laboració amb l'autoritat de control, sense perjudici que, tal com s'exposarà tot seguit, sí que es mantingui la imputació pel fet assenyalat a l'apartat de fets provats.

2.2. Sobre el fet provat consistent en la modificació de la clau d'accés del compte del denunciant i l'accés a totes les aplicacions de "Google Workspace G Suites" del denunciant.

(...)

Exposat l'anterior, escau entrar a analitzar les al·legacions efectuades per l'institut. En el seu escrit, l'institut reconeix que una persona aliena al denunciant (el coordinador informàtic de l'institut) **va accedir al compte de "Google Workspace G Suites" del denunciant** i que "va atorgar accés a tot el professorat del centre." També confirma que no existeix cap document per informar a les persones treballadores sobre les instruccions en relació amb l'ús d'aquests comptes i que, únicament, s'informa de manera oral que "tots els documents que es treballen en els moodles de les assignatures han d'estar ubicats al drive corporatiu del centre, que el material dels mòduls professionals són de propietat del centre i han d'estar a disposició de tots els docents que en puguin necessitar fer ús." També reconeix que no es va adoptar cap mesura compensatòria per a realitzar l'accés, ni se li va oferir estar present durant la intervenció. De fet, la directora de l'Institut manifesta que va tenir coneixement dels fets a través del denunciant.

L'institut al·lega que va intentar contactar amb el denunciant en **reiterades ocasions sense èxit i que, per aquest motiu, va decidir accedir-hi al seu compte.** Però, el denunciant ha acreditat que se li va demanar la documentació controvertida en data 07/12/2022 i que, al dia següent, el dia 08/12/2022, va donar resposta. Això es desprèn en el correu electrònic de 08/12/2022 en què el professor substitut manifestava "ja no fa falta que facis res amb el correu del (...) [el denunciant], ja que m'ha donat accés a totes les pràctiques." Aquesta prova desvirtua els arguments de l'institut tota vegada que ha quedat constatat que el professor que necessitava els materials didàctics va obtenir-los el dia 08/12/2022. A més, no consta provada per part de l'institut la insistència al·legada.

Sobre la legitimitat de l'accés, cal destacar que aquest es va produir sense que l'entitat responsable disposes d'unes normes que regulin aquesta qüestió – rellevants des del punt de vista de la protecció de dades personals – i sense adoptar cap mesura compensatòria ni amb preavís a l'afectat. Això suposa una infracció molt greu de la normativa de protecció de dades. Tal i com es va avançar en l'acord d'iniciació, l'institut només pot accedir als dispositius i mitjans digitals dels seus treballadors/es quan aquest accés **estigui justificat, no hi hagi cap altre mecanisme** que permeti assolir l'objectiu perseguit, i es dugui a terme d'acord amb les **normes d'ús dels dispositius i mitjans digitals** prèviament aprovades i **conegudes per les persones treballadores.** En el cas que s'analitza no es va donar cap dels pressupostos assenyalats i, en conseqüència, contravenint el Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat (ENS) en l'àmbit de l'Administració electrònica.

Segons l'institut, en base a la normativa de la funció pública i l'LOPDGDD, pot accedir als continguts derivats de l'ús dels mitjans digitals facilitats als treballadors "per al control del compliment de les obligacions laborals i per garantir la integritat dels dispositius." Considera que l'accés es va produir per assegurar **"el bon funcionament dels sistemes d'informació i comunicació i dispositius**

digitals, fer un seguiment de la seva adequada utilització, així com detectar i respondre als possibles incidents de seguretat." Aquesta manifestació no pot prosperar perquè el cert és que l'accés es va produir – tal i com ha afirmat l'institut – per obtenir uns materials didàctics, motiu aquest que res té a veure amb la finalitat al·legada.

En aquest punt, cal recordar que la única informació que l'institut facilita a les persones treballadores en relació amb l'ús d'eines informàtiques és que els materials didàctics són de propietat de l'escola i han d'estar ubicats al "drive corporatiu" accessibles a tots els docents. Respecte d'això, escau dir que, tot i que la titularitat dels materials sigui de l'institut, aquesta circumstància no legitima la intromissió als comptes d'usuaris dels treballadors sense el seu consentiment. Per a dur a terme l'accés als comptes d'usuaris amb la deguda observança de la normativa de protecció de dades– i tot i que la finalitat d'aquests comptes sigui laboral – aquesta Autoritat ha recomanat en reiterades ocasions la prèvia aprovació d'uns mecanismes d'accés i posada en coneixement de les persones treballadores, així es recull en diversos pronunciaments citats en l'acord d'iniciació d'aquest procediment. En definitiva, les funcionalitat laborals del compte no impedeixen que dins d'aquest hi pugui haver dades personals dels usuaris que fan indispensable l'adopció de mesures per evitar accessos a informació de l'esfera privada de l'usuari i la iniciativa de preveure l'adopció d'aquestes mesures i de demostrar la seva existència respon a la obligació del responsable del tractament de complir el principi de responsabilitat proactiva, previst a l'article 5.2 de l'RGPD.

En base a tot l'exposat, escau afirmar que l'institut va incomplir les seves obligacions com a responsable del tractament, en concret, els articles 25 i 32 de l'RGPD, al no haver adoptat totes les mesures adients per a garantir el respecte del dret fonamental a la protecció de dades."

3. En relació amb els fets descrits a l'apartat de fets provats, relatiu a la protecció de dades des del disseny i per defecte, cal acudir a l'article 25 de l'RGPD, que preveu el següent (la negreta és de l'APDCAT):

"Protección de datos desde el diseño y por defecto. 1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el **responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos**, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados. 2. El responsable del tratamiento **aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento**. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por

> defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas".

Per altra banda, 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, tenint en compte a l'hora d'avaluar l'adequació del nivell de seguretat, especialment la comunicació o l'accés no autoritzats a aquestes dades, entre d'altres.

El fet recollit a l'apartat de fets provats constitueix la infracció de l'article 83.4.*a* de l'RGPD, que tipifica com a tal 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 les recollides als articles 25 i 32 de l'RGPD.

D'acord amb el que disposa la disposició addicional primera de l'LOPDGDD, cal esmentar el que estableix l'article 16 del Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat (ENS) en l'àmbit de l'Administració electrònica:

> "Article 16. Autorització i control dels accessos.
>
> L'accés al sistema d'informació ha de ser controlat i limitat als usuaris, processos, dispositius i altres sistemes d'informació, degudament autoritzats, restringint l'accés a les funcions permeses."

L'apartat 3, "Marc organitzatiu [org]", punt 2 "Normativa de seguretat [org. 2], de l'annex II, "Mesures de seguretat", de l'ENS, determina el següent:

> "3.2 Normativa de seguretat [org. 2].

dimensions	Totes		
categoria	bàsica	mitjana	alta
	aplica	=	=

> S'ha de disposar d'una sèrie de documents que descriguin:
>
> a. L'ús correcte d'equips, serveis i instal·lacions.
>
> b. El que es considera ús indegut.
>
> c. La responsabilitat del personal respecte del compliment o violació d'aquestes normes: drets, deures i mesures disciplinàries d'acord amb la legislació vigent."

Per la seva banda, l'apartat 4.2.5, "Mecanismes d'autenticació [op. acc. 5]", determina el següent:

> "

dimensions	I C A T		
nivell	baix	mitjà	alt
	aplica	+	++

Els mecanismes d'autenticació davant del sistema s'han d'adequar al nivell del sistema atenent les consideracions que segueixen.

Les guies CCN-STIC han de desenvolupar els mecanismes concrets adequats a cada nivell.

Nivell BAIX

a) S'admet l'ús de qualsevol mecanisme d'autenticació: claus concertades, o dispositius físics (en expressió anglesa <<tokens>>) o components lògics com ara certificats de programari o altres d'equivalents o mecanismes biomètrics.
b) En el cas de fer servir contrasenyes s'han d'aplicar regles bàsiques de qualitat.
c) S'ha d'atendre la seguretat dels autenticadors de forma que:

1r Els autenticadors s'han d'activar una vegada estiguin sota el control efectiu de l'usuari.
2n Els autenticadors han d'estar sota el control exclusiu de l'usuari.
3r L'usuari ha de reconèixer que els ha rebut i que coneix i accepta les obligacions que implica la seva tinença, en particular el deure de custòdia diligent, protecció de la confidencialitat i informació immediata en cas de pèrdua.
4t Els autenticadors s'han de canviar amb una periodicitat marcada per la política de l'organització, atenent la categoria del sistema al qual s'accedeix.
5è Els autenticadors s'han de retirar i ser deshabilitats quan l'entitat (persona, equip o procés) que autentiquen acaba la seva relació amb el sistema.

Nivell MITJÀ

a) No es recomana l'ús de claus concertades.
b) Es recomana l'ús d'un altre tipus de mecanismes del tipus dispositius físics («tokens») o components lògics com ara certificats de programari o altres d'equivalents o biomètrics.
c) En el cas de fer servir contrasenyes s'han d'aplicar polítiques rigoroses de qualitat de la contrasenya i renovació freqüent.

Nivell ALT

a) Els autenticadors se suspenen després d'un període definit de no ser utilitzats.
b) No s'admet l'ús de claus concertades.
c) S'exigeix l'ús de dispositius físics («tokens») personalitzats o biometria.
d) En el cas d'utilització de dispositius físics («tokens») s'han d'utilitzar algoritmes acreditats pel Centre Criptològic Nacional.
e) S'han d'utilitzar, preferentment, productes certificats [op.pl.5].

Taula resum de mecanismes d'autenticació admissibles:

		Nivell		
		BAIX	MITJÀ	ALT
alguna cosa que se sap	claus concertades	sí	Amb cautela	no
alguna cosa que es té	«tokens»	si	sí	criptogràfics
alguna cosa que s'és	biometria	sí	sí	+ doble factor

"

La conducta que aquí s'aborda s'ha recollit com a infracció greu a l'article 73.*d* i *f* de l'LOPDGDD. La lletra *d* preveu: "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 la lletra *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."

I l'apartat 3r de l'article 77 de l'LOPDGDD estableix que:

> "Sense perjudici del que estableix l'apartat anterior, l'autoritat de protecció de dades ha de proposar també la iniciació d'actuacions disciplinàries quan hi hagi indicis suficients per fer-ho. En aquest cas, el procediment i les sancions que s'han d'aplicar són els que estableix la legislació sobre règim disciplinari o sancionador que sigui aplicable.
>
> Així mateix, quan les infraccions siguin imputables a autoritats i directius, i s'acrediti l'existència d'informes tècnics o recomanacions per al tractament que no s'hagin atès degudament, en la resolució en què s'imposi la sanció s'ha d'incloure una amonestació amb la denominació del càrrec responsable i se n'ha d'ordenar la publicació al «Butlletí Oficial de l'Estat» o autonòmic que correspongui."

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. A més, pot proposar, si escau, la iniciació d'actuacions disciplinàries d'acord amb el que estableix la legislació vigent sobre el règim disciplinari del personal al servei de les administracions públiques. Aquesta resolució s'ha de notificar a la persona responsable del fitxer o del tractament, a l'encarregada del tractament, si escau, a l'òrgan del qual depenguin i a les persones afectades, si n'hi ha."

En aquest cas, no escau requerir cap mesura per cessar o corregir els efectes de la infracció, atès que es tracta d'un fer consumat i puntual.

Resolució

Per tot això, resolc:

1. Declarar que (...) del Departament d'Educació i Formació Professional ha comès una infracció prevista a l'article 83.4.*a* en relació amb l'article 25 i 32, ambdós de l'RGPD.

2. Notificar aquesta resolució a (...) del Departament d'Educació i Formació Professional.

3. Comunicar la resolució al Síndic de Greuges, de conformitat amb el que preveu l'article 77.5 de l'LOPDGDD.

4. Ordenar que aquesta resolució es publiqui 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