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

Identificació de l'expedient

Resolució del procediment sancionador núm. PS 27/2021, referent a la Fundació per a la Universitat Oberta de Catalunya

Antecedents

1. En data 09/03/2020, va tenir entrada a l'Autoritat Catalana de Protecció de Dades un escrit d'una persona pel qual formulava denúncia contra la Fundació per a la Universitat Oberta de Catalunya (en endavant, UOC), amb motiu d'un presumpte incompliment de la normativa sobre protecció de dades personals.

La persona denunciant hi exposava que, en data (...)/2019 va finalitzar la seva relació laboral a la UOC, però tot i així, a la seva adreça de correu electrònic amb el domini de la UOC, que mantenia oberta com a estudiant, seguien arribant-li correus electrònics del departament de recursos humans de l'entitat i de treballadors de la UOC. La persona denunciant afegia a la seva queixa que, també tenia accés "*a la base de dades de nom "Tercers" que conté tota la informació personal, bancària i acadèmica, d'estudiants, col·laboradors docents, i treballadors de la UOC*", fet que va advertir a la delegada de protecció de dades de la UOC a través d'un correu electrònic (...)del qual no va obtenir resposta.

La persona denunciant aportava documentació diversa sobre els fets denunciats, en concret, còpies dels correus electrònics següents:

- correu electrònic, de data (...), amb l'assumpte "(...)", enviat des de la bústia genèrica "Gestió de formació" de la UOC, a l'adreça de correu electrònic de la persona denunciant.

- correu electrònic, de data (...), enviat per l'aquí denunciant a l'adreça de correu electrònic de la delegada de protecció de la UOC, advertint que té accés a la base de dades de "Tercers".

- correu electrònic, de data (...), amb assumpte (...)", enviat des de l'adreça de correu electrònic "(...)", a l'adreça de correu electrònic de la persona denunciant, fent una consulta de feina.

- correu electrònic, de data (...), amb assumpte "(...)", enviats des de l'adreça de correu electrònic "(...)" , a l'adreça de correu electrònic de la persona denunciant, a través de la qual s'informa sobre l'actualització d'una determinada aplicació en un servidor web.

- correu electrònic, de data (...), amb l'assumpte "Comunicació IRPF 2019", enviat des de la bústia genèrica "Àrea de Persones <persones@uoc.edu>" a l'adreça electrònica de la persona denunciant.

2. L'Autoritat va obrir una fase d'informació prèvia (núm. IP 90/2020), 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 15/06/2020 es va requerir l'entitat denunciada perquè informés sobre si s'havien suprimit les dades personals de la persona aquí denunciant com a treballadora de la UOC, o per contra, encara es tractaven les seves dades personals com a treballadora en actiu. També, sobre els motius pels quals la persona denunciant encara rebia correus electrònics d'assumptes vinculats amb les seves anteriors funcions com a treballadora de la UOC, i sobre quines dades personals de la comunitat UOC s'emmagatzemen a la base de dades "Tercers", així com els motius pels quals la persona aquí denunciant podia accedir-hi, i si s'havien adoptat mesures correctores per restringir-ne els accessos indeguts.

4. En data 30/06/2020, la UOC va respondre el requeriment esmentat a través d'escrit en què exposava, entre d'altres, el següent:

- Que "*la FUOC tracta les seves dades per a gestionar la relació laboral ja extingida, però no com a treballadora en actiu.*" I, en relació amb això, concreta que "*referent a la tramesa d'una comunicació relativa al certificat de retencions de l'IRPF que es va enviar a totes les persones que havien percebut rendes durant l'any 2019, per a informar-los dels passos a seguir per a sol·licitar l'esmentada certificació. L'article 108.3 del Reial Decret 439/2007, de 30 de març, pel qual s'aprova el Reglament de l'Impost sobre la Renda de les Persones Físiques, indica que el retenidor, en aquest la FUOC, ha d'expedir en favor del contribuent certificació acreditativa de les retencions practicades i altres dades referents al contribuent que s'han d'incloure en la declaració anual"*

- Que "*Donades les seves tasques com a treballadora de (...)de la UOC, la interessada era usuària de diverses plataformes per l'intercanvi de informació i gestió interna de la organització.*"

- Que "*la interessada va ser usuària de la plataforma CAU-CABRA (pertanyent a l'àrea de Recursos d'aprenentatge) i per aquest motiu, aquest sistema li remetia avisos automàtics si algun altre usuari de la plataforma l'esmentava. El dia (...)de 2019, la interessada va posar en coneixement al Servei d'Atenció de la UOC que rebia correus de les peticions generades en tal plataforma i en la mateixa data se li va informar que s'havia desactivat el seu usuari de CAU-CABRA*".

- Que "*el dia (...)de 2019, es va remetre un correu electrònic des de Gestió de Formació on se li realitzava el seguiment de la seva formació de llarga durada. La recepció d'aquest correu és deguda al manteniment de la seva bústia de correu institucional de la universitat donada la seva condició d'estudiant."*

- Que "*la interessada va rebre una notificació de la que tenim constància, generada automàticament per l'aplicatiu JIRA. La raó per la qual va rebre tal notificació és que la interessada disposava d'un usuari en tal aplicatiu. Al cessar la seva relació laboral amb la UOC no se li va donar de baixa el seu usuari de l'esmentada plataforma ja que és excepcional que els treballadors de (...)participin en un aplicatiu propi de l'Àrea de Tecnologia i, per tant, no es contemplava tal possibilitat en els existents protocols de Baixa del Personal Propi, aquest incident va ser remediat immediatament i així mateix va ser objecte de correcció juntament amb la modificació del protocol de baixa del personal propi"***.**

- Que "*Les dades personals desades a Tercers són el nom i cognoms, el número d'identificació únic a la base de dades de Tercers, acceptació, en el seu cas, a la recepció de comunicacions comercials, acceptació, en el seu cas, a la tramesa d'enquestes i si aquesta ha manifestat la seva voluntat de no rebre cap tipus de comunicacions per part de la UOC (si està donada d'alta al llistat Robinson UOC), tot això respecte a tots els membres de la Comunitat UOC, això és qualsevol persona física que tingui o hagi tingut una relació jurídica amb la UOC*."

- Que "*La interessada tenia accés a Tercers pels motius que s'exposen a continuació:*
  La interessada formava part de l'equip de (...)de la UOC, concretament duia a terme les tasques relacionades amb (...), els seus accessos a aplicacions i eines corporatives eren d'ampli espectre a fi de poder donar servei a les peticions rebudes des d'altres àrees de la UOC, així com d'estudiants i qualsevol altra persona física les dades de la qual poguessin ser objecte de tractament dins del marc dels serveis oferts per la Universitat."

- Que *"Els diferents accessos del personal de gestió de la UOC venen determinats pel seu rol professional, com a tal, la interessada tenia accessos a:*
  - Directori Actiu (perfil d'usuari de l'entorn Windows, rol d'usuari i permisos d'accés des d'un terminal)
  - Telefonia fixa
  - Google Suite
  - Aplicacions Cloud
  - Aplicacions TREN (aplicacions de gestió interna pròpies de la UOC)"

- Que "*La interessada, particularment, a més d'ostentar la condició de personal de gestió, també fou estudiant, per tant, quan es va extingir la seva relació laboral encara conservava els accessos corresponents al seu perfil d'estudiant, ja que aquest accés*

no es dona automàticament de baixa. Així va ser que, a través del perfil d'estudiant que mantenia al Campus de la UOC, va ser capaç d'accedir a dades personals restringides al personal de gestió, ja que la baixa en les aplicacions TREN no es produïa de forma automàtica, sinó com a conseqüència de la baixa al Directori Actiu, de forma que aquestes aplicacions de gestió encara li eren accessibles a través del seu perfil d'estudiant."

- Que "*En el moment que la interessada va posar de manifest aquest fet en correus de dates (...)de 2019, es va procedir a la immediata baixa de les aplicacions TREN associades a la interessada i a la ràpida modificació dels protocols interns de baixa per posar remei a aquesta possibilitat d'accés maliciós per part de persones en les que la confluència de rols (ex. Estudiants, personal de gestió, personal docent, etc.) podia permetre accessos indeguts*."

- Que "*quan la interessada va posar de manifest aquest fet, es van adoptar les mesures següents*:
  - Baixa manual immediata de totes les aplicacions associades al seu rol professional.
  - Modificació del protocols de baixa del personal propi introduint la necessitat de donar de baixa individualment a totes les eines corresponents al personal de gestió, no essent suficient amb la baixa del directori actiu, donat que si l'usuari manté un altre perfil (i.e. estudiant) podria arribar a accedir a eines no autoritzades."

- Que "*els treballadors de l'entitat que accedeixen a dades personals o sistemes informàtics han realitzat un curs de formació sobre protecció de dades perquè estiguin informats i coneixen les exigències de la normativa en aquesta matèria."*

L'entitat denunciada adjuntava a l'escrit documentació diversa, entre aquesta, el document *"Procediment baixa personal propi*" de setembre de 2019, en el qual es descriuen en detall totes les actuacions a seguir quan es dona de baixa un treballador de la UOC.

5. En data 07/05/2021, la directora de l'Autoritat Catalana de Protecció de Dades va acordar iniciar un procediment sancionador contra la UOC per dues presumptes infraccions: una infracció prevista a l'article 83.5.a) en relació amb l'article 5.1.a); i una altra infracció prevista a l'article 83.4.a) en relació amb els articles 32 i 5.1.f); 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 (en endavant, RGPD). Aquest acord d'iniciació es va notificar a l'entitat imputada en data 11/05/2021.

6. 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.

7. En data 25/05/2021, la UOC va formular al·legacions a l'acord d'iniciació i va aportar documentació diversa.

8. En data 15/10/2021, 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 imposés a la Fundació per a la Universitat Oberta de Catalunya com a responsable, en primer lloc, d'una infracció prevista a l'article 83.5.a) en relació amb l'article 5.1.a); i en segon lloc, d'una infracció prevista a l'article 83.4.a) en relació amb els articles 32 i 5.1.f), tots ells de l'RGPD.

Aquesta proposta de resolució es va notificar en data 15/10/2021 i es concedia un termini de 10 dies per formular al·legacions.

9. En data 26/10/2021, l'entitat imputada va pagar per avançat 2.000.- euros (dos mil euros), corresponents al pagament voluntari avançat de la sanció pecuniària que la persona instructora proposava en la proposta de resolució, una vegada aplicada la reducció corresponent.

10.En data 29/10/2021, la UOC va presentar un escrit en el qual exposava les accions adoptades en relació amb les mesures correctores que es proposaven a la proposta de resolució, i informava sobre el pagament de la sanció pecuniària amb la reducció del 20% per pagament anticipat.

Fets provats

1.La persona denunciant havia finalitzat la relació laboral amb la UOC en data (...)/2019, mantenint el vincle amb l'entitat amb el rol d'estudiant i conservant l'adreça electrònica amb el domini de la UOC. La UOC no va implementar mesures de seguretat suficients per impedir que pogués seguir accedint a la carpeta electrònica "Tercers", de la mateixa manera que quan era treballadora dins l'àrea de (...)de l'entitat, i consultar dades personals de totes les persones de la "Comunitat UOC" (qualsevol persona física que tingui o hagi tingut una relació jurídica amb la UOC.).

De la documentació aportada, es constata que la persona denunciant va tenir accés a la carpeta electrònica "Tercers" almenys fins el (...)/2019.

2. La persona denunciant, malgrat haver finalitzat la seva relació laboral amb la UOC en data (...)/2019, va continuar rebent correus electrònics fins a principis de l'any 2020 relacionats amb les seves anteriors funcions com a treballadora de la UOC, a l'adreça electrònica que conservava com a estudiant.

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

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. De conformitat amb l'article 85.3 de l'LPAC, el pagament voluntari avançat de la sanció pecuniària proposada comporta l'aplicació d'una reducció. L'efectivitat d'aquesta reducció està condicionada al desistiment o la renúncia de qualsevol acció o recurs per la via administrativa contra la sanció i comporta la terminació del procediment.

A aquest respecte, cal assenyalar que l'entitat imputada va formular al·legacions a l'acord d'iniciació i, tal com s'ha indicat als antecedents, s'ha acollit a l'opció per reduir l'import de la sanció consistent en el pagament voluntari avançat de la sanció pecuniària, amb els efectes abans indicats. No obstant, la UOC ha presentat davant la proposta de resolució un escrit en el qual no es formulen pròpiament al·legacions, sinó que s'exposen les actuacions que s'han dut a terme en relació amb les mesures correctores proposades a la proposta de resolució. Dit això, es considera oportú reiterar a continuació el més rellevant de la resposta motivada que la persona instructora va donar a les al·legacions que va presentar l'UOC davant l'acord d'iniciació, i al fonament de dret 7è valorar les mesures correctores adoptades per l'entitat.

2.1 Sobre les mesures de seguretat adoptades per impedir l'accés a la carpeta "Tercers"

En el 1r apartat de l'escrit d'al·legacions presentat davant l'acord d'iniciació, l'entitat imputada exposava que la UOC no tenia implementades les mesures de seguretat per evitar fets com els provats, perquè la seva "*excepcionalitat*" no permetia identificar el risc i no resultava proporcional l'aplicació de mesures específiques per mitigar-lo. En aquest sentit, defensava que les mesures de seguretat establertes eren adequades, i que en el moment en que aquest risc s'identifica, es va procedir a implementar les mesures de seguretat consistents en "*la modificació del procediment de baixes existent i s'elabora el Protocol de Baixa del Personal Propi (el Protocol)*".

Doncs bé, en primer lloc, cal valorar positivament l'actitud proactiva de la UOC que, un cop va tenir coneixement dels fets, va implementar mesures encaminades a corregir els efectes de la infracció imputada, com és la modificació del referenciat "*Protocol de Baixa del Personal Propi*" i la baixa manual immediata de totes les aplicacions associades al rol professional de la persona aquí denunciant. Dit això, també és necessari puntualitzar que l'adopció de mesures per corregir els efectes de la infracció no desvirtuen els fets imputats, ni tampoc modifiquen la seva qualificació jurídica.

Segons l'entitat, l'excepcionalitat dels fets provats parteix del fet que en el moment en que la persona aquí denunciant va finalitzar la seva relació laboral amb la UOC, es va procedir a donar de baixa el "perfil de gestió" del seu usuari, però, arran d'un "error humà", no es va completar la baixa, i es va deixar actiu dins del "perfil de gestió" el sistema TREN. El sistema TREN gestiona l'accés a les aplicacions web desenvolupades internament, i permet l'accés, entre d'altres, a la carpeta electrònica "Tercers". Això, juntament amb el fet que l'aquí denunciant també era estudiant de la UOC, i per tant, mantenia actiu el seu usuari amb el "perfil d'estudiant", va permetre-li accedir al Campus Virtual de la UOC, i, des d'aquí, a través del sistema TREN - que mantenia actiu malgrat haver finalitzat la seva relació laboral-, a la carpeta electrònica "Tercers".

A aquest respecte, cal indicar que, quant l'entitat invoca un "error humà" per referir-se al fet que no es va tramitar la baixa del sistema TREN, adduint que el responsable d'iniciar el dit procediment no va executar l'acció perquè també havia finalitzat el seu contracte laboral, en puritat, no ens trobaríem davant d'un "error humà". En aquest cas, ens trobem davant d'un defecte en el disseny del circuit de tramitació i seguiment del procés de baixa d'un usuari, que no va permetre detectar i alertar aquesta situació circumstancial, derivada de la coincidència en el temps de la baixa laboral de diferents persones, en concret, la de la persona aquí denunciant i la del seu superior jeràrquic que era el responsable de iniciar el procediment de baixa de l'usuari del sistema TREN. De l'exposat, s'evidencia que el disseny del circuit intern que tenia la UOC per donar de baixa a un usuari del sistema TREN no era el més segur per assegurar la baixa del sistema, doncs, per una banda, no va permetre detectar que no s'havia iniciat el procés de baixa del sistema TREN de l'ex-empleada, i per l'altra, no va alertar d'aquesta situació a cap altre responsable de la gestió de permisos de la UOC.

Sigui com sigui, el fet és que la concurrència de totes aquestes circumstàncies va permetre a la persona denunciant accedir a la carpeta electrònica "Tercers" malgrat ja no ser empleada de la UOC, posant en evidència que el sistema de mesures de seguretat de la UOC no era suficient per garantir la seguretat de les dades personals del què és responsable. Sobre això, fer avinent que l'RGPD configura un sistema de seguretat que es basa en determinar, arran d'una prèvia valoració de riscos, quines mesures de seguretat són necessàries en cada cas (considerant 83 i article 32).Aquesta anàlisis de riscos ha de portar necessàriament a concloure que, amb caràcter previ al desplegament dels permisos als sistemes d'informació gestionats per la UOC, és necessari determinar i aplicar les mesures de seguretat tècniques i organitzatives apropiades al risc que comporta el tractament, per salvaguardar el dret a la protecció de dades dels possibles afectats.

A aquest respecte, la disposició addicional primera de l'LOPDGDD estableix el següent: "*L'Esquema Nacional de Seguretat ha d'incloure les mesures que s'hagin d'implantar en cas de tractament de dades personals per evitar-ne la pèrdua, l'alteració o l'accés no autoritzat, amb l'adaptació dels criteris de determinació del risc en el tractament de les dades al que estableix l'article 32 del Reglament (UE) 2016/679*".

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

Doncs bé, respecte la conducta descrita a l'apartat de fets provats, s'infereix que l'entitat imputada va vulnerar la mesura de seguretat prevista a l'article 16 de l'Esquema Nacional de Seguretat, precepte que regula l'autorització i el control dels accessos en els següents termes: "*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*."

De conformitat amb el que s'ha exposat, les al·legacions formulades per la UOC han de ser desestimades, doncs, és obvi que les mesures de seguretat que tenien implementades no eren suficients ni adequades per impedir que la persona aquí denunciant pogués accedir amb el seu usuari a la controvertida carpeta electrònica "Tercers" malgrat haver finalitzat la seva relació laboral amb la UOC i només tenir actiu el seu "perfil d'estudiant".

2.2. Sobre els correus electrònics

Seguidament, l'entitat imputada fa una sèrie de consideracions per defensar la legitimitat de l'enviament dels correus electrònics d'àmbit laboral a l'adreça de correu electrònic que la persona aquí denunciant mantenia activa en la seva qualitat d'estudiant de la UOC, i que era la mateixa que tenia quan era treballadora.

En relació amb això, quant a les al·legacions realitzades per cadascun dels correus electrònics que va rebre la persona aquí denunciant, es considera que la UOC només va actuar de forma legítima quan va enviar el correu electrònic de data (...), amb l'assumpte "Comunicació IRPF", ja que estava donant compliment a una obligació legal en matèria fiscal que li pertocava com a retenidora de rendes del treball generades per l'aquí denunciant durant el període en que va ser empleada de l'entitat (art. 108.3 del Reial Decret 439/2007, de 30 de març).

Ara bé, pels altres correus electrònics, es considera que no hi hauria habilitació per emprar l'adreça electrònica que la persona aquí denunciant mantenia activa pel seu rol d'estudiant. Doncs, un cop desapareguda la relació laboral, i per tant, la base jurídica que legitimaria el tractament de les seves dades com empleada (art.6.1.b RGPD), ja no es podia emprar la dita adreça electrònica per enviar-li informació que només hauria d'arribar-li en el cas que fos treballadora.

Aquest és el cas del correu electrònic de data (...), amb l'assumpte "(...)", que l'aquí denunciant va rebre perquè no se l'havia donat de baixa de la llista de distribució dels enviaments periòdics dels esdeveniment formatius oferts als treballadors. Al respecte, l'entitat exposa que la baixa d'aquesta llista de distribució no es produeix de manera automàtica, sinó de manera manual i en el termini aproximat d'un mes des de que l'usuari deixa de tenir perfil de gestió, i surt del directori actiu. Doncs bé, tenint en compte que la base jurídica que legitimaria la recepció del referenciat correu electrònic seria la vigència del contracte laboral, i aquest va finalitzar el dia (...)/2019, es considera que l'enviament del dit correu electrònic, de data (...), no es trobava emparat per cap base jurídica de les

previstes a l'article 6.1 de l'RGPD. És a dir, la baixa de la llista de distribució hauria de coincidir amb la data de finalització de la relació laboral, o, en qualsevol cas, dur-la a terme en un termini prudencial, inferior al termini d'un mes que preveu la UOC (i que en el present cas, inclús va superar).

Així mateix, pel que fa als dos correus electrònics que van enviar dos treballadors de la UOC, en data (...) i (...), amb els assumptes correlatius (...)" i "(...)", tampoc poden prosperar les al·legacions de la UOC invocant la seva manca de responsabilitat. Que els correus electrònics fossin enviats per dos empleats no implica que la UOC no sigui la responsable d'aquest tractament de dades, doncs els dos remitents formaven part de l'entitat i els assumptes sobre els quals tractaven eren de caire laboral, i denota l'acció que no havien estat informats per l'entitat de la baixa laboral de la persona denunciant, ni que havien rebut cap instrucció de mantenir actualitzat el directori de correus electrònics de la resta d'empleats. Per tant, la UOC era la responsable d'evitar que alguns dels empleats continuessin enviant correus electrònics d'àmbit laboral a l'ex-treballadora, quan dit tractament ja no era lícit per manca de base jurídica suficient.

De conformitat amb el que s'ha exposat, s'estima que aquesta al·legació no pot reeixir.

3. En relació amb els fets descrits al punt 1r de l'apartat de fets provats, cal acudir a l'article 5.1.f) de l'RGPD, que preveu que les dades personals seran *"tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas".*

Per la seva banda, l'article 32 de l'RGPD, referent a la seguretat de les dades, disposa el següent:

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

Durant la tramitació d'aquest procediment s'ha acreditat degudament el fet descrit al punt 1r de l'apartat de fets provats, que és constitutiu de la infracció prevista a l'article 83.4.a) de l'RGPD, que tipifica com a tal la vulneració de *"las obligaciones del responsable y del encargado"*, entre les quals es troba la recollida a l'article 32 de l'RGPD a dalt transcrit, referent a la seguretat del tractament.

La conducta que aquí s'aborda s'ha recollit com a infracció greu a l'article 73.f) de l'LOPDGDD, en la forma següent:

> *"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 del Reglament (UE) 2016/679"*

4. Pel que fa al fet descrit al punt 2 de l'apartat de fets provats, cal acudir a l'article 5.1.a) de l'RGPD, que preveu que les dades personals han de ser tractades "*de manera lícita, leal y transparente en relación con el interesado ("licitud, lealtad y transparencia").*

En aquest sentit, l'RGPD disposa que tot tractament de dades personals ha de ser lícit (article 5.1.a) i, en relació amb això, estableix un sistema de legitimació del tractament de dades que es fonamenta en la necessitat de que concorri alguna de les bases jurídiques establertes al seu article 6.1.

De conformitat amb el que s'ha exposat, el fet recollit al punt 2 de l'apartat de fets provats constitueix la infracció prevista l'article 83.5.a) de l'RGPD, que tipifica com a tal la vulneració de "*los principios básicos para el tratamiento (…)".*

Al seu torn, aquesta conducta s'ha recollit com a infracció molt greu a l'article 72.1.a) de la LOPDGDD, en la forma següent:"*El tratamiento de datos personales vulnerando los*

principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679", en relació amb el principi de licitud establert a l'article 5.1.a) del mateix RGPD.

5. Al tractar-se la UOC, d'una entitat de dret privat, resulta d'aplicació el règim sancionador general previst a l'article 83 de l'RGPD.

Per una banda, en relació amb la conducta descrita al punt 1er dels fets imputats, l'article 83.4 de l'RGPD, preveu una sanció de multa 10.000.000 d'euros com a màxim, 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.

D'altra banda, en relació amb la conducta descrita al punt 2on dels fets imputats, l'article 83.5 de l'RGPD, preveu una sanció de multa 20.000.000 d'euros com a màxim, o tractant-se d'una empresa, d'una quantia equivalent al 4% 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, especialment, la contemplada a la dicció b).

5.1 Quant al fet provat 1er (la falta d'adopció de les mesures seguretat apropiades)

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 infracció imputada va arribar a afectar a la seguretat de les dades de totes les persones de la "Comunitat UOC", i deixa en evidència que les mesures tècniques i organitzatives de l'entitat no eren les apropiades per garantir un nivell de seguretat adequat al risc del tractament de dades que estava duent a terme.

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 estableixen els articles 83.2 RGPD i 76.2 LOPDGDD, i també de conformitat amb el principi de proporcionalitat consagrat a l'article 29 de la Llei 40/2015, tal com indicava la persona instructora en la proposa de resolució, escau imposar la sanció de 1.500 euros (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 causes següents:

- Els perjudicis causats a les persones afectades, atès que no es té constància de que s'hagin causat perjudicis greus en les persones afectades (art. 83.2.a RGPD). A aquest respecte, també cal tenir en compte, que l'abast de la informació a la que l'ex-

treballadora va tenir accés era la mateixa que li era accessible per raó del seu càrrec immediatament abans de la seva baixa laboral.
- La manca d'intencionalitat (art. 83.2.b RGPD) .
- El grau de cooperació amb l'Autoritat amb la finalitat de posar remei a la infracció i mitigar els possibles efectes adversos de la infracció - que es reflecteix amb la immediata baixa de les aplicacions TREN de la persona denunciant i la modificació del "*Protocol de Baixa del Personal Propi (el Protocol)*" (art.83.2.f RGPD).
- La categoria de les dades personals afectades per la infracció –no es té constància que afectés a categories especials de dades– (art. 83.2.g RGPD).
- La manca de beneficis com a conseqüència de la comissió de la infracció (art. 83.2.k RGPD i 76.2.c LOPDGDD).

Per contra, com a criteris agreujants, cal tenir en compte els següents elements:

- Les infraccions comeses amb anterioritat per la UOC – procediments sancionadors números PS 40/2014, PS 29/2017 i PS 30/2020 - (art. 83.2.e RGPD).
- La vinculació de l'activitat de l'infractor amb la pràctica de tractaments de dades personals (art. 83.2.k RGPD i 76.2.b LOPDGDD).

5.2 Quant al fet provat 2on (enviament de correus electrònics vinculats en l'àmbit laboral)

En el present cas, tal com exposava la persona instructora en la proposta de resolució, també escau descartar la possibilitat substituir la sanció de multa administrativa per la sanció d'amonestació prevista a l'article 58.2.b) RGPD, atesa la gravetat de la infracció imputada, i que la UOC, per la seva especialització, es considera que ha de gestionar adequadament els perfils de les persones treballadores un cop acabada la seva relació laboral.

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 estableixen els articles 83.2 RGPD i 76.2 LOPDGDD, i també de conformitat amb el principi de proporcionalitat consagrat a l'article 29 de la Llei 40/2015, tal com indicava la persona instructora en la proposa de resolució, escau imposar la sanció de 1.000 euros (mil 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 causes següents:

- La naturalesa, gravetat i duració de la infracció, tenint en compte la naturalesa i l'abast del tractament i el número d'afectats i el nivell de danys i perjudicis causats (art.83.2.a RGPD).
- La manca d'intencionalitat (art.83.2.b RGPD)

- La categoria de les dades de caràcter personal afectades per la infracció, tenint en compte que l'adreça de correu electrònic corporativa on va rebre els correus i que mantenia activa com estudiant, era la mateixa que la que tenia quan era treballadora de l'entitat (art.83.2.g RGPD)
- La manca de beneficis obtinguts com a conseqüència de la infracció (art. 83.2.K RGPD i art. 76.2.c LOPDGDD)
- Les mesures adoptades per la UOC per donar de baixa a la persona denunciant de la llista de distribució dels enviaments periòdics dels esdeveniment formatius oferts als treballadors, un cop en va tenir coneixement (art. 83.2.k RGPD)

Per contra, com a criteris agreujants, cal tenir en compte els següents elements:

- Les infraccions comeses amb anterioritat per la UOC – procediments sancionadors números PS 40/2014, PS 29/2017 i PS 30/2020 - (art. 83.2.e RGPD).
- La vinculació de l'activitat de l'infractor amb la pràctica de tractaments de dades personals (art. 83.2.k RGPD i 76.2.b LOPDGDD).

6. D'altra banda, de conformitat amb l'article 85.3 de l'LPAC i tal com s'avançava a l'acord d'iniciació, 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, en data 26/10/2021, l'entitat imputada ha abonat de manera avançada 2.000 euros (dos mil euros), corresponents a la quantia de la sanció resultant que s'indicava a la proposta de resolució, un cop aplicada la reducció acumulada del 20%.

7. Davant la constatació de les infraccions previstes a l'art. 83 de l'RGPD en relació amb fitxers o tractaments de titularitat privada, 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 relació amb això, escau indicar que la UOC ha exposat i ha acreditat el compliment de les mesures correctores que es van proposar a la proposta de resolució, i únicament queda pendent d'acreditar en el termini més aviat possible, i en tot cas en el termini màxim de 10 dies a comptar des de l'endemà de la notificació d'aquesta resolució, l'adopció del "*Protocol de creació, manteniment i eliminació de llistes de distribució*".

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

Per tot això, resolc:

1. Imposar a la Fundació per a la Universitat Oberta de Catalunya, en primer lloc, la sanció consistent en una multa de 1500.- euros (mil cinc-cents euros), com a responsable d'una infracció prevista a l'article 83.4.a) en relació amb els articles 32 i 5.1.f); en segon lloc, la sanció consistent en una multa de 1.000.- euros (mil euros), com a responsable d'una infracció prevista a l'article 83.5.a) en relació amb l'article 5.1.a), tots ells de l'RGPD. L'import total de les dues sancions ascendeix a la quantitat de 2.500.-euros (dos mil cinc-cents euros).

2. Declarar que la Fundació per a la Universitat Oberta de Catalunya ha fet efectiu el pagament avançat de 2.000.- euros (dos mil euros), que correspon a l'import total de les dues sancions imposades, un cop aplicat el percentatge de deducció del 20% corresponent a la reducció del pagament voluntari avançat prevista a l'article 85 de la LPAC.

3. Requerir la Fundació per a la Universitat Oberta de Catalunya perquè adopti la mesura correctora assenyalada al fonament de dret 7è i acrediti davant d'aquesta Autoritat el seu compliment.

4. Notificar aquesta resolució a la Fundació per a la Universitat Oberta de Catalunya.

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, 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,