

**Dictamen en relació amb la consulta formulada per un organisme autònom sobre l'intercanvi d'informació personal en un entorn virtual d'accés restringit**

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit emès per un organisme autònom sobre l'intercanvi d'informació personal en un entorn virtual d'accés restringit i la seva adequació a la normativa de protecció de dades.

Analitzada la petició i la documentació que l'acompanya, i vist l'informe de l'Assessoria Jurídica, es dictamina el següent:

I

(...)

II

L'organisme autònom manifesta, en el seu escrit, que, per tal d'aconseguir una gestió adequada i eficaç, ha de compartir entre els membres d'un òrgan col·legiat (en endavant l'òrgan col·legiat), informació relacionada amb el funcionament de les diferents activitats formatives.

Segons l'organisme consultant, aquesta informació que es comparteix comprèn informació relacionada amb la tasca docent, com ara, els informes d'avaluació dels docents. Aquests informes s'elaboren a partir dels qüestionaris que els alumnes emplen per valorar el seu grau de satisfacció en relació amb una determinada activitat i inclouen, entre d'altra informació, les dades personals relatives al nom i cognom del docent, així com la valoració mitjana que aquest hagi obtingut.

Amb la intenció de millorar-ne la gestió, es vol dotar a l'òrgan col·legiat d'un entorn virtual d'accés restringit (similar a una Intranet) dins la plataforma "e-catalunya" en què, per mitjà d'un repositori específic, es faci accessible tota aquesta informació als seus membres.

En atenció a aquests fets, sol·licita dictamen de l'Autoritat Catalana de Protecció de Dades, per tal de conèixer si el fet de facilitar l'accés als informes d'avaluació, amb les dades de valoració dels docents, per mitjà d'un entorn virtual d'accés restringit, s'adequa a la normativa en matèria de protecció de dades personals.

Aquesta qüestió s'analitza en els apartats següents d'aquest dictamen.

III

Als efectes que interessin en el present dictamen, cal fer referència, d'entrada, als diferents fluxos d'informació que tenen lloc en el supòsit plantejat.

Per a l'exercici de les seves funcions de direcció, coordinació i vigilància del compliment d'un Pla de formació d'una Administració, l'organisme autònom, ha de rebre dels diferents organismes de la mateixa Administració la informació relacionada amb el seus Plans de formació que inclouen l'avaluació dels docents amb les seves dades personals.

Des de la vessant de la protecció de dades personals, la comunicació d'aquesta informació personal, en la mesura que comporta una revelació de dades efectuada a una persona diferent de l'interessat, constitueix una cessió de dades (article 3.i) de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal

(LOPD)) i, com a tal, s'haurà d'efectuar de conformitat amb el règim previst, amb caràcter general, per a les comunicacions o les cessions de dades a l'article 11 de la LOPD.

Aquest precepte preveu, en el seu apartat primer, que *“les dades de caràcter personal objecte de tractament només poden ser comunicades a un tercer per al compliment de finalitats directament relacionades amb les funcions legítimes del cedent i del cessionari amb el consentiment previ de l'interessat”*.

Aquesta regla general troba però determinades excepcions, entre les quals cal destacar, la possibilitat que la comunicació estigui autoritzada en una llei o norma amb rang de llei (apartat 2.a) o que el tractament *“respongui a la lliure i legítima acceptació d'una relació jurídica el desenvolupament, el compliment i el control de la qual impliqui necessàriament la connexió del tractament esmentat amb fitxers de tercers, tenint en compte que la comunicació només és legítima quan es limiti a la finalitat que la justifiqui”* (apartat 2.c).

En el cas examinat, la previsió de l'article 11.2.c) de la LOPD podria donar cobertura suficient a les comunicacions d'informació relativa a l'avaluació dels docents d'una determinada activitat per part dels diferents organismes on s'imparteixi la docència a l'organisme autònom, atesa l'existència d'una relació jurídica entre el docent i l'organisme autònom, el desenvolupament, el compliment i el control de la qual implicaria necessàriament la connexió amb fitxers de tercers, per la qual cosa no requeriria comptar amb el consentiment dels afectats.

D'altra banda, cal fer avinent que la creació d'un entorn virtual dins la plataforma “e-catalunya” perquè l'organisme autònom posi a disposició de l'òrgan col·legiat aquesta informació que inclou el conjunt de les avaluacions dels docents, comportaria, de fet, una nova comunicació de dades personals (article 3.i) LOPD).

La plataforma “e-catalunya” (accessible des de l'adreça <http://ecatalunya.gencat.cat>) és una iniciativa de la Generalitat de Catalunya creada per millorar l'eficiència en la prestació de serveis públics a la ciutadania mitjançant l'ús d'eines de col·laboració de la xarxa Internet. Es configura com un punt de trobada virtual per a comunitats formades per personal de l'administració pública catalana i altres professionals que tenen necessitat de comunicar-se i treballar en xarxa.

En aquest sentit, la plataforma “e-catalunya” ofereix a cada comunitat la possibilitat d'interactuar en un portal propi, que pot ser públic o privat (només per a membres prèviament registrats), així com un conjunt d'eines de participació, amb l'objectiu de facilitar el treball en equip i la presa de decisions de manera consensuada, d'agilitzar i de millorar la comunicació entre els membres del grup, de facilitar l'accés als continguts generats per aquests i de gestionar la informació de forma més eficient.

En el cas examinat, els participants de l'entorn virtual creat dins la plataforma “e-catalunya” serien els membres de l'òrgan col·legiat.

Posant en marxa aquest entorn virtual sembla que cadascun d'aquests membres tindria accés a tota la informació que inclouria tant les avaluacions dels docents del seu propi organisme, com les corresponents a altres organismes.

Aquest accés a la informació personal dels docents d'altres organismes constitueix una cessió de dades personals (article 3.i) LOPD) que, com s'ha vist, requereix comptar amb el consentiment dels afectats o, en el seu defecte, amb l'existència d'alguna de les excepcions previstes a l'article 11.2 de la LOPD.

Cal fer avinent que, per al compliment de les funcions que l'òrgan col·legiat té assignades, tot i que pugui ésser necessari accedir a les avaluacions de totes les activitats, no sembla desprendre's que els seus membres hagin d'accedir

necessàriament al conjunt dels informes d'avaluació dels docents, atès que, en principi, no es desprèn que els correspongui dur a terme aquesta tasca d'avaluació del personal docent. Això, sens perjudici que el responsable de cada organisme pugui accedir a les avaluacions d'aquells docents que hagin impartit una determinada activitat en el seu organisme.

Per tant, per poder facilitar als membres de l'òrgan col·legiat aquesta informació en concret (no hi hauria problemes amb la resta d'informació que no inclogui dades personals), caldria comptar amb el consentiment previ dels afectats (article 11.1 LOPD).

Alternativament, l'organisme autònom podria facilitar l'accés a aquesta informació de manera dissociada o anonimitzada, és a dir, de tal manera que els docents no resultin identificables (article 5.1.e) del Reglament de desplegament de la LOPD (RLOPD), aprovat pel Reial decret 1720/2007, de 21 de desembre).

Ara bé, perquè la dissociació pugui ser considerada suficient als efectes de la LOPD, cal que de l'aplicació del procés de dissociació (article 3.j) LOPD) resulti realment impossible associar una determinada dada amb un individu determinat. En aquest sentit, es considera que l'afectat no serà determinable o identificable quan la seva identificació exigeixi terminis o activitats desproporcionades (article 5.1.o) RLOPD).

Escau assenyalar que, d'acord amb l'article 11.6 de la LOPD, *“si la comunicació s'efectua amb el procediment previ de dissociació, no és aplicable el que estableixen els apartats anteriors”*, és a dir, no cal comptar amb el consentiment previ de l'afectat.

#### IV

Examinats els fluxos d'informació que tenen lloc en el supòsit plantejat, es considera necessari fer una consideració específica pel que fa, en concret, a l'ús d'un entorn virtual dins la plataforma “e-catalunya” com a mitjà per intercanviar informació personal.

Com s'ha apuntat en l'apartat anterior d'aquest dictamen, la creació d'aquest entorn virtual privat o d'accés restringit, per tal de millorar la gestió del coneixement en l'àmbit formatiu, permetrà recollir i intercanviar informació de diversa índole entre els seus participants que, en el cas examinat, inclou les dades personals dels docents que s'hagin incorporat en els informes d'avaluació (nom, cognom i valoració mitjana obtinguda).

Atès aquest tractament de dades de caràcter personal (article 3.c) LOPD) és necessari garantir que terceres persones alienes a aquest entorn virtual privat (per exemple, altres comunitats que també participin en la plataforma “e-catalunya”) no puguin accedir fàcilment a aquesta informació.

En aquest sentit, convé tenir en compte que la LOPD imposa l'obligació al responsable del tractament i, si s'escau, a l'encarregat del tractament d'adoptar les mesures de caràcter tècnic i organitzatiu necessàries per tal de garantir la seguretat de les dades personals que seran tractades, així com per evitar la seva alteració, pèrdua, tractament o accés no autoritzat (article 9).

Aquestes mesures de seguretat venen regulades en el Títol VIII del Reglament de desplegament de la LOPD, aprovat pel Reial decret 1720/2007, de 21 de desembre (RLOPD).

D'acord amb aquest Reglament, *“les mesures de seguretat exigibles als accessos a dades de caràcter personal a través de xarxes de comunicacions, siguin públiques o no, han de garantir un nivell de seguretat equivalent al corresponent als accessos en mode local, conforme als criteris que estableix l'article 80”* (article 85 RLOPD).

L'esmentat article 80 del RLOPD classifica les mesures de seguretat exigibles als fitxers i tractaments de dades en tres nivells diferents –bàsic, mitjà i alt- en funció de la tipologia de dades personals que en cada cas es prevegin tractar.

En el cas examinat, i d'acord amb la tipologia de dades personals que sembla ser que serien tractades (dades identificatives i professionals) les mesures de seguretat a implementar correspondran a les de nivell bàsic (article 81.1 RLOPD), atès que *a priori* no es preveu tractar dades personals que requereixin l'adopció d'un nivell superior de mesures de seguretat.

En concret, tenint en compte que el tractament d'aquestes dades s'efectuarà de manera automatitzada, correspondrà aplicar les mesures descrites en els articles 89 a 94 del RLOPD:

- a) L'elaboració d'un document de seguretat on es fixin les obligacions i funcions dels usuaris o perfils d'usuaris que accedeixin a les dades, una descripció del sistema informàtic i una definició de les funcions de control o autoritzacions delegades pel responsable del fitxer o tractament (article 89).
- b) L'establiment d'un registre d'incidències (article 90).
- c) L'establiment d'un control d'accés (article 91).
- d) La correcta gestió de suports i documents (article 92).
- e) L'adopció de mesures que garanteixin la correcta identificació i autenticació dels usuaris (article 93).
- f) L'establiment de processos de còpies de seguretat i recuperació de les dades (article 94).

Per tant, abans de facilitar, per mitjà d'un entorn virtual privat, l'accés als informes d'avaluació de les activitats de formació amb les dades de valoració dels docents, caldrà adoptar necessàriament les mesures de seguretat abans esmentades.

Atesos els termes en què s'efectua la consulta, cal fer referència, en concret, a la necessitat d'adoptar les mesures de seguretat relatives a l'establiment d'un control d'accés (article 91) i a l'adopció de mecanismes que permetin la correcta identificació i autenticació dels usuaris (article 93 RLOPD):

*"Article 91. Control d'accés*

- 1. Els usuaris han de tenir accés només als recursos que necessitin per a l'exercici de les seves funcions.*
- 2. El responsable del fitxer s'ha d'encarregar que hi hagi una relació actualitzada d'usuaris i perfils d'usuaris, i els accessos autoritzats per a cadascun d'ells.*
- 3. El responsable del fitxer ha d'establir mecanismes per evitar que un usuari pugui accedir a recursos amb drets diferents dels autoritzats.*
- 4. Exclusivament el personal autoritzat per fer-ho en el document de seguretat pot concedir, alterar o anul·lar l'accés autoritzat sobre els recursos, de conformitat amb els criteris que estableix el responsable del fitxer.*
- 5. En cas que existeixi personal aliè al responsable del fitxer que tingui accés als recursos, ha d'estar sotmès a les mateixes condicions i obligacions de seguretat que el personal propi."*

*"Article 93. Identificació i autenticació*

- 1. El responsable del fitxer o tractament ha d'adoptar les mesures que garanteixin la correcta identificació i autenticació dels usuaris.*
- 2. El responsable del fitxer o tractament ha d'establir un mecanisme que permeti la identificació de forma inequívoca i personalitzada de qualsevol usuari que intenti accedir al sistema d'informació i la verificació conforme està autoritzat.*

3. *Quan el mecanisme d'autenticació es basi en l'existència de contrasenyes, hi ha d'haver un procediment d'assignació, distribució i emmagatzematge que en garanteixi la confidencialitat i integritat.*

4. *El document de seguretat ha d'establir la periodicitat, que en cap cas ha de ser superior a un any, amb què s'han de canviar les contrasenyes que, mentre estiguin vigents, s'han d'emmagatzemar de forma intel·ligible.”*

En el cas examinat, i de conformitat amb la informació disponible al portal de la plataforma “e-catalunya”, l'accés a l'esmentada plataforma requereix un registre previ com a persona usuària i, per tal de poder participar en un entorn virtual de caràcter privat, cal, a més a més, disposar d'un perfil personal i d'unes claus d'autenticació constituïdes per un usuari (adreça de correu electrònic) i una contrasenya.

Aquest sistema d'identificació i d'autenticació basats en un usuari i una contrasenya per accedir al contingut de l'espai virtual privat que es creï es considera conforme amb allò disposat al RLOPD, si bé cal que:

- El procediment de gestió de les contrasenyes garanteixi la confidencialitat i la integritat de les mateixes.
- La contrasenya sigui robusta. La major o menor exigència en aquest aspecte dependrà de la naturalesa de la informació protegida, però en qualsevol cas pot portar a establir uns requeriments mínims.
- Les contrasenyes es canviïn de forma periòdica, i en qualsevol cas sempre abans d'un any.
- El responsable estableixi perfils d'usuaris per tal que cada usuari pugui accedir només a aquella informació per a la qual estigui autoritzat.

És a dir, cal garantir que només tindran accés als informes d'avaluació de les activitats de formació amb les dades de valoració dels docents, les persones que requereixin tal accés per a l'exercici de les seves funcions. Així mateix, per aplicació del principi de qualitat de les dades (article 4 LOPD), en la seva vessant de finalitat, cal garantir que aquestes persones només podran consultar la informació personal que en cada cas resulti necessària, pertinent i adequada.

D'altra banda, en la mesura en que el funcionament d'aquests entorns virtuals privats no és aliè als riscos que per a la informació comporta l'ús de la xarxa, cal adoptar aquelles mesures que evitin la propagació de virus en el sistema d'informació, així com emprar barreres de seguretat (“tallafocs” o firewalls).

Convé destacar la importància de l'adopció de totes aquestes mesures, atès que l'objectiu perseguit amb la seva implementació és garantir no només la confidencialitat, sinó també la integritat i la disponibilitat de la informació amb la finalitat de garantir el dret fonamental a la protecció de dades personals.

Així mateix, cal tenir en compte que tant el responsable com els qui intervinguin en qualsevol fase del tractament de les dades estan obligats al “*secret professional pel que fa a les dades i al deure de guardar-les, obligacions que subsisteixen fins i tot després de finalitzar les seves relacions amb el titular del fitxer o, si s'escau, amb el seu responsable*” (article 10 LOPD).

D'acord amb les consideracions fetes en aquest dictamen en relació amb la consulta plantejada, es fan les següents,

## **Conclusions**

La comunicació dels informes d'avaluació de les activitats de formació, que inclouen les dades de valoració dels docents, a l'organisme autònom per a l'exercici de les seves funcions constitueix una cessió de dades personals que troba habilitació en allò disposat a l'article 11.2.c) de la LOPD.

L'accés a aquesta informació personal per part dels membres de l'òrgan col·legiat requereix comptar amb el consentiment previ dels docents (article 11.1 LOPD), atès que el seu coneixement no sembla ser necessari per a l'exercici de les seves funcions. Aquest consentiment no serà necessari si la informació es dissocia prèviament.

La creació d'un entorn virtual privat dins la plataforma "e-catalunya" que permeti accedir i compartir informació de caràcter personal, requereix l'adopció de les mesures de caràcter tècnic i organitzatiu necessàries per garantir la seguretat de les dades personals tractades, així com per evitar la seva alteració, pèrdua, tractament o accés no autoritzat (article 9 LOPD). En particular, caldrà adoptar les mesures de seguretat de nivell bàsic establertes al RLOPD.

Barcelona, 13 de setembre de 2012