Dictamen en relació amb la consulta d'una Universitat en relació amb la utilització del producte *Microsoft Office 365* amb tots els col·lectius (alumnes, PAS i PDI)

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit d'una Universitat en què es demana el parer de l'Autoritat sobre la possibilitat d'utilitzar el producte "*Microsoft Office 365"* amb tots els col·lectius (alumnes, PAS i PDI), ateses les implicacions relatives al compliment de la normativa de protecció de dades.

La consulta exposa que, després d'analitzar el Dictamen 27/2014, d'aquesta Autoritat, relatiu a la contractació dels sistemes de correu al núvol de *Google Apps* i de *Microsoft Office 365*, i la *"Resolución de declaración de adecuación de garantías para las transferencias internacionales de datos a los Estados Unidos con motivo de la prestación de Servicios de computación en nube",* de l'Agència Espanyola de Protecció de Dades (AEPD), de 2014, relativa a serveis oferts per Microsoft, entre d'altres, Office 365 i Windows Azure, no disposa de prou informació per determinar si el producte i, per extensió, *"Microsoft Azure",* compleix amb les obligacions establertes ni especialment els mecanismes que cal contemplar per poder realitzar les auditories corresponents.

La consulta puntualitza que després del Dictamen 27/2014, de l'Autoritat, i de la *"Resolución de declaración de adecuación de garantías para las transferencias internacionales de datos a los Estados Unidos con motivo de la prestación de Servicios de computación en nube",* de l'AEPD, (Exp. TI/00023/2014, disponible al web. www.agpd.es), de 9 de maig de 2014, són de 2014 i que posteriorment s'han produït canvis en la prestació del servei i en el marc legal.

Analitzada la petició, vista la normativa vigent aplicable, l'informe del Coordinador d'Auditoria i Seguretat de la Informació de l'Autoritat, i l'informe de l'Assessoria Jurídica de l'Autoritat, es dictamina el següent.

I

(...)

II

La consulta es refereix a la possibilitat d'utilitzar serveis online de Microsoft (Office 365 i Azure), per tractar dades dels col·lectius d'alumnes, PAS (personal administratiu i de serveis) i PDI (personal docent i investigador), sense més concreció.

En principi, atesa la informació aportada, la contractació d'aquests productes per part de la Universitat comprendria el conjunt d'eines o d'aplicacions incloses a Microsoft Office 365 i a Azure, per tractar dades personals en el context de l'activitat de la Universitat, tant dels alumnes, com del seu propi personal, ja sigui PAS o PDI.

D'acord amb la informació disponible a la pàgina web de l'empresa Microsoft, en l'apartat referit a la seva política de privacitat (https://privacy.microsoft.com), els "productes d'empresa" de Microsoft s'ofereixen i es dissenyen principalment per a l'ús d'organitzacions, i inclouen diversos serveis de subscripció en el núvol, com ara Office 365 i Azure, entre d'altres, per als quals una organització ("el client"), contracta els serveis ("serveis en línia") amb Microsoft. Microsoft publica en el seu lloc web informació sobre la

manera com protegeix els sistemes d'informació, sobre les polítiques de privacitat que estableixen i les condicions de servei, i sobre les tecnologies que utilitzen per a la prestació dels serveis que ofereixen (https://www.microsoft.com/es-xl/trustcenter/CloudServices/Office-365).

Segons la informació disponible, *"Microsoft Office 365 cuenta con soluciones online que aumentan la productividad de los equipos de ventas y equipos móviles y favorecen una solución conectada. Nuestros seguros servicios en la nube le ayudan a expandir su negocio y se ajustan a numerosos requisitos normativos del sector y regionales*", i disposa de diferents solucions per a col·lectius com ara empreses, organitzacions governamentals, institucions educatives, o bé a nivell personal. "Microsoft Office 365" està format per diferents aplicacions de tipus ofimàtic i serveis complementaris, als quals l'usuari pot accedir en línia, sens perjudici que puguin existir versions d'escriptori. Entre aquestes aplicacions podem destacar: "Word" -tractament de textos-, "Excel" -full de càlcul-, "Powerpoint" –presentacions-, "Outlook" -correu electrònic- o "Onedrive" –emmagatzemament-).

Pel que fa a "Microsoft Azure", que segons la informació disponible ofereix serveis empresarials online (www.microsoft.com/es-xl/trustcenter/CloudServices/Azure) , es tracta d'un conjunt de serveis en el núvol que s'ofereixen de manera integrada (en una única plataforma), i que, per exemple, permeten disposar de serveis de processament d'aplicacions, de bases de dades, aplicacions per a dispositius mòbils, xarxes d'emmagatzemament, espais web, etc).

Pel que fa als canvis en el servei dels productes de Microsoft sobre els que es consulta, a efectes d'aquest dictamen s'ha tingut especialment en compte la informació que facilita Microsoft sobre els seus productes, en concret, en el document *"Termes dels Serveis Online",* de Microsoft, (versió en català, d'1 de novembre de 2016), i també en el document *"Declaración de privacidad de Microsoft"* (versió de setembre de 2016), entre d'altres.

III

Des de la perspectiva de la protecció de dades, partim de la base que la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD), s'aplica a qualsevol tractament de dades personals quan el tractament s'efectua en territori espanyol, o quan al responsable del tractament no establert en territori espanyol li és aplicable la legislació espanyola (article 2.1.a) i b) de la LOPD). Segons l'article 2.1.c) de l'LOPD, aquesta llei s'aplica en els casos en què el responsable no està establert a la UE però utilitza, per a tractar les dades personals, mitjans situats en territori espanyol.

Cal tenir especialment en compte el Reglament general de protecció de dades (UE) 2016/679 (en endavant, RGPD), que va entrar en vigor el 25 de maig de 2016, i que serà aplicable a partir del 25 de maig de 2018 (art. 99 RGPD).

Pel que fa a l'àmbit d'aplicació territorial del RGPD (Considerant 23 RGPD), segons l'article 3 del RGPD:

> *"1.El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del* ***responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.***
>
> *2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un* ***responsable o encargado no establecido en la Unión,*** *cuando las actividades de tratamiento estén relacionadas con:*

a) ***la oferta de bienes o servicios a dichos interesados en la Unión,*** *independientemente de si a estos se les requiere su pago, o*
b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

(...).”

La Universitat ha de tenir especialment en compte les previsions i obligacions derivades del RGPD en el procés d'elecció i priorització de serveis oferts per tercers que hagin de comportar el tractament de dades personals, especialment, quan es prevegi que aquest tractament ha de tenir continuïtat més enllà d'aquesta data (25.5.2018), com és previsible en el cas que ens ocupa (tractament de dades per part d'una Universitat catalana, tant dels seus alumnes com del seu personal PDI i PAS).

Tal com ha posat de manifest aquesta Autoritat en dictàmens anteriors (CNS 24/2012 sobre la contractació, precisament, dels serveis *Google Apps for Business,* i CNS 57/2013 sobre els riscos derivats de l'ús dels serveis de *cloud storage*, així com en el Dictamen 55/2016, disponibles al web de l'Autoritat, www.apd.cat), la contractació de serveis tipus *cloud computing* o “computació en el núvol” gestionats per un tercer, quan la seva prestació implica tractar dades personals dels fitxers o dels sistemes del responsable del fitxer o tractament, constitueix el que l'LOPD anomena *“un accés de dades per compte de tercers”* (article 12 LOPD).

Com ha analitzat aquesta Autoritat anteriorment, quan un responsable, en aquest cas una Universitat, contracta i utilitza determinats sistemes de comunicació que implementen terceres empreses alienes a l'administració responsable (en aquest cas, serveis de “*cloud storage*” d'una tercera empresa), aquest tercer esdevé l'encarregat del tractament. En aquest esquema, caldria estar a les obligacions que imposa la normativa de protecció de dades (art. 12 LOPD, i arts 20 a 22 RLOPD), i específicament, les previsions del capítol IV del RGPD, referides a les responsabilitats del responsable i de l'encarregat del tractament, atès l'àmbit territorial d'aplicació esmentat (art. 3 RGPD).

Segons el RGPD, quan s'estableix un encàrrec del tractament, el responsable està obligat a triar un encarregat que ofereixi garanties suficients per aplicar mesures tècniques i organitzatives apropiades, de manera que el tractament sigui conforme al RGPD (art. 28.1 RGPD). L'article 28.3 del RGPD exigeix que el contracte o acte jurídic pel qual es regeix el tractament de dades per l'encarregat (en aquest cas, Microsoft), ha d'establir l'objecte, la durada, la naturalesa i la finalitat del tractament, el tipus de dades personals i categories d'interessats, i les obligacions i drets del responsable, en concret, ha d'estipular que l'encarregat:

“a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;

b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;

c) tomará todas las medidas necesarias de conformidad con el artículo 32;

d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;

e) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir

con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;

f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;

h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros."

Atès que Microsoft seria l'encarregat del tractament si la Universitat contracta els serveis online objecte de consulta (Office 365 i Azure), en establir-se el corresponent contracte d'encàrrec la Universitat haurà de preveure els diferents elements que exigeix l'article 28 del RGPD.

Partint d'aquesta base, a continuació analitzarem diferents elements que resulten rellevants des de la perspectiva de la protecció de dades, i que cal tenir en compte als efectes de la consulta formulada, en concret:

- Transferències internacionals de dades (TID)
- Seguretat de les dades
- Notificació de violacions de seguretat
- Subcontractació
- Realització d'auditories

IV

Transferències internacionals de dades (TID)

L'empresa Microsoft té el seu establiment per a la UE a Irlanda, amb la qual cosa el tractament que faci aquesta empresa de dades de ciutadans europeus, es troba sotmès al RGPD; inclús si part del tractament, als efectes que interessen, l'emmagatzematge d'informació dels usuaris, es duu a terme fora de la UE (en servidors que físicament estan ubicats en tercers països, o perquè es duu a terme un tractament a través de la computació en el núvol), també cal aplicar els principis i garanties de la normativa europea de la protecció de dades, ateses les previsions sobre l'àmbit d'aplicació d'aquesta (art. 3 RGPD), com s'ha fet avinent en el Dictamen 55/2016.

Atès que la consulta es refereix a serveis que operen en el núvol, és possible que la contractació d'aquests serveis comporti la realització d'una transferència internacional de dades personals -TID- (article 5.1.s) RLOPD) si la seva transmissió té lloc fora del territori de l'Espai Econòmic Europeu (EEE), ja sigui perquè aquesta transmissió constitueix una cessió o comunicació de dades (article 3.i) LOPD), ja sigui perquè té per objecte la realització d'un tractament per part d'un encarregat del tractament. Quan un responsable, en aquest cas, la Universitat, utilitza sistemes de *"cloud storage",* o quan simplement els

servidors on s'emmagatzemen les dades (missatges de text, les imatges, etc, enviats i rebuts pels usuaris), estiguin ubicats fora de l'àmbit territorial d'aplicació del RGPD, esmentat, ens trobarem davant d'una TID, que estarà sotmesa al règim previst en els articles 33 i 34 LOPD, així com al règim previst en els articles 44 a 50 del RGPD.

Per tant, la Universitat ha de constatar si aquests serveis compleixen amb les exigències previstes per al règim de TID, previstos a l'LOPD i al RGPD, per tal d'assegurar que el tractament de la informació dels afectats s'adequa a les exigències de la normativa europea de protecció de dades.

Segons explicita el document de Microsoft *"Termes dels Serveis Online"* (1 de novembre de 2016, apartat de "Ubicació i processament de les dades"):

> *"Llevat del que es descrigui als OST, les Dades del Client que Microsoft tracti en nom del Client es poden* ***transmetre, emmagatzemar i tractar als Estats Units o a qualsevol altre país*** *on Microsoft o les seves filials o els seus subcontractistes tinguin instal·lacions. El Client designa a Microsoft perquè faci aquesta transferència de les Dades del Client a qualsevol d'aquests països i perquè emmagatzemi i tracti les Dades del Client amb la finalitat de prestar els Serveis Online. Microsoft es regirà pels requisits de la llei de protecció de dades de la Comunitat Econòmica Europea i Suïssa pel que fa a la recopilació, l'ús, la transmissió, la conservació i altres processaments de dades personals provinents de la Comunitat Econòmica Europea i Suïssa.* ***A més dels compromisos de Microsoft en virtut de les clàusules contractuals estàndard i altres contractes model, Microsoft té la certificació de l'Escut de privacitat de la UE-EUA."***

El RGPD preveu que la Comissió de la UE pot decidir que un tercer país, un territori o un o varis sectors específics d'un país, garanteix un nivell de protecció adequat (art. 45). A manca d'aquesta Decisió de la Comissió, només es podrien transmetre dades personals a un tercer país, si l'empresa o servei en qüestió ofereix garanties adequades i a condició que els afectats disposin de drets exigibles i d'accions legals efectives (art. 46 RGPD). Cal tenir en compte que els mecanismes que estableix el RGPD per tal de considerar que s'ofereixen garanties adequades, són diversos –normes corporatives vinculants (BCR), clàusules tipus, mecanismes de certificació, etc- (art. 46.2 RGPD) i, per tant, la Universitat ha de tenir en compte quins d'aquests instruments o mecanismes ofereixen els serveis Office 365 i Azure.

En qualsevol cas, cal tenir en compte que la Resolució de l'AEPD, de 9 de maig de 2014, va considerar adequades les garanties establertes en els models de contractes aportats per Microsoft Corporation per a la TID amb destinació a Microsoft, establerta als Estats Units, amb motiu de la presentació dels serveis Office 365, i Windows Azure, entre d'altres, actuant Microsoft com a encarregat del tractament. Així mateix, l'AEPD va considerar autoritzades les TID fetes sota l'empara de les clàusules contractuals esmentades, sempre que es doni compliment a les condicions establertes en la pròpia Resolució.

Com s'ha apuntat, els servidors que utilitzen els serveis objecte de consulta podrien estar, a banda dels Estats Units, en altres ubicacions geogràfiques. En aquest sentit, com es feia avinent en el Dictamen 27/2014, Microsoft s'hauria compromès a signar amb els clients les clàusules contractuals tipus establertes per la Comissió Europea en la seva Decisió 2010/87/UE de 5 de febrer de 2010, relativa a les clàusules contractuals tipus per a la transferència de dades a encarregats del tractament establerts en tercers països, qüestió a la que es va referir aquesta Autoritat en el Dictamen 27/2014, citat.

Així, segons la Resolució de l'AEPD, de 9 de maig de 2014, es feia constar que*, "con la finalidad de aportar las garantías suficientes para las transferencias de datos a MICROSOFT CORPORATION y a sus subcontratistas, ofrece a sus clientes la posibilidad de firmar las* ***cláusulas contractuales tipo,*** *adoptadas por la Comisión Europea en su Decisión 2010/87/UE, y un acuerdo suplementario a dichas cláusulas para adecuar a las características de los servicios de computación en nube la realización de las auditorías de las actividades de tratamiento y la subcontratación de operaciones de tratamiento con subencargados ulteriores del tratamiento."*

L'AEPD va considerar adequada aquesta vinculació, als efectes de les TID relacionades amb els serveis de Microsoft: ("(...) *ofrecen al cliente la posibilidad de firmar con Microsoft Corporation, como importador de datos, las* ***cláusulas contractuales tipo*** *adoptadas por la Comisión Europea en su Decisión 2010/87/UE, que en su apéndice 1 establece los detalles de la transferencia de manera específica, por una parte, para los servicios* ***Office 365*** *y Microsoft Dynamics CRM Online y, por otra, para los servicios de* ***Windows Azure****, y un acuerdo suplementario con la finalidad de adecuar a las características de los servicios de computación en nube la realización de las auditorías de las actividades de tratamiento cubiertas por las cláusulas y la subcontratación con subencargados ulteriores del tratamiento.* (...)".

Com apunta la consulta, aquesta Resolució de l'AEPD és de l'any 2014, per tant, anterior a l'entrada en vigor del RGPD, que estableix específicament la possibilitat d'aplicar clàusules contractuals tipus en relació amb els encàrrecs de tractament per part de tercers.

Així, l'article 28 RGPD disposa el següent:

> *"(...)*
>
> *6. Sin perjuicio de que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato u otro acto jurídico a que se refieren los apartados 3 y 4 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales tipo a que se refieren los apartados 7 y 8 del presente artículo, inclusive cuando formen parte de una certificación concedida al responsable o encargado de conformidad con los artículos 42 y 43.*
>
> *7.La* ***Comisión podrá fijar cláusulas contractuales tipo*** *para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.*
>
> *8. Una* ***autoridad de control podrá adoptar cláusulas contractuales tipo*** *para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el mecanismo de coherencia a que se refiere el artículo 63.*
>
> *(...)"*

Sens perjudici de la possibilitat que s'estableixin, en aplicació del RGPD, noves clàusules contractuals tipus en relació amb els contractes d'encàrrec del tractament, en el moment d'emetre aquest dictamen cal tenir en compte que, segons la informació de Microsoft ("*Termes dels Serveis Online*", d'1 de novembre de 2016, apartat relatiu als "Termes de processament de dades" (DPT, *data processing terms*)):

"Els Termes de Tractament de Dades també inclouen les "Clàusules Contractuals Tipus", ***d'acord amb la Decisió de la Comissió Europea de 5 de febrer de 2010*** *sobre clàusules contractuals tipus per a la transferència de dades personals a encarregats del tractament establerts en tercers països en virtut de la Directiva de Protecció de Dades de la Unió Europea.* (...)*."*

L'Apèndix 3 del document d'1 de novembre, citat, reprodueix les clàusules contractuals tipus incloses en l'Annex de la Decisió de la Comissió de 5 de febrer de 2010, que ja van ser en el seu moment tingudes en compte en la Resolució de l'AEPD, citada.

En definitiva, les condicions vigents en el moment d'elaborar aquest dictamen, previstes per Microsoft per als seus serveis online (incloent Office 365 i Azure), segueixen explicitant la vinculació amb les clàusules contractuals tipus previstes a la Decisió de la Comissió, de 5 de febrer de 2010, citada.

Cal fer avinent que, segons disposa l'article 46.5 del RGPD, en relació amb les TID mitjançant garanties adequades:

> *"Las **autorizaciones otorgadas por un Estado miembro** o una autoridad de control de conformidad con el artículo 26, apartado 2, de la Directiva 95/46/CE seguirán siendo válidas hasta que hayan sido modificadas, sustituidas o derogadas, en caso necesario, por dicha autoridad de control. Las decisiones adoptadas por la Comisión en virtud del artículo 26, apartado 4, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas, en caso necesario, por una decisión de la Comisión adoptada de conformidad con el apartado 2 del presente artículo."*

Per tot això, atès el que ja va resoldre l'AEPD en la seva Resolució de 9 de maig de 2014 (que, per aplicació de l'art. 46.5 RGPD continuaria essent vàlida), i tenint en compte que en el moment d'emetre aquest dictamen Microsoft segueix explicitant la seva vinculació a les clàusules contractuals tipus de la Decisió de la Comissió de 5 de febrer de 2010, es pot considerar que el contracte d'encàrrec del tractament de la Universitat amb Microsoft, per utilitzar els serveis objecte de consulta, que es subscrigui en aquests termes, seguiria en principi ajustant-se a les exigències de la normativa de protecció de dades.

Per altra banda fem avinent que, a partir del 12 de juliol de 2016, la UE ha posat en marxa "l'Escut de la privacitat UE- EEUU" ("Privacy shield"), en substitució de l'anterior acord "U.S.-E.U. Safe Harbor", (anul·lat per la STJUE de 6 d'octubre de 2015), al que s'adherien entitats d'Estats Units per certificar el compliment de principis i obligacions de protecció de dades, amb la finalitat d'habilitar TID (veure, al respecte, les consideracions fetes pel Grup de Treball de l'article 29 (GT 29) en el Dictamen 1/2016, sobre el projecte d'Escut de Privacitat entre la UE i EE.UU).

La informació sobre la *"Guía del Escudo de la Privacidad UE-EE.-UU"* es troba disponible al web oficial de la UE: http:// europa.eu.

Als efectes que interessen, Microsoft consta com a empresa adherida a l'Escut de Privacitat, segons la informació del web del Departament de Comerç d'Estats Units (https://www.privacyshield.gov/welcome), amb certificació de data 8 de desembre de 2016, que té una vigència anual, prorrogable.

En conseqüència, el compromís de Microsoft de respectar les previsions de l'Escut de privacitat en relació amb la protecció de dades (obligacions en matèria de dret d'informació a l'afectat, exercici de drets, comunicació de dades, etc), podria donar validesa a la transferència internacional de dades als servidors d'aquesta empresa, quan la informació s'emmagatzemi en servidors ubicats, específicament, als Estats Units.

V

Seguretat de les dades

Com ja es va fer avinent en el Dictamen 24/2013 (FJ VIII), les previsions que puguin explicitar les empreses respecte la confidencialitat amb la que tracten les dades dels

usuaris, no eximeixen de les obligacions que, en funció de la informació tractada, siguin exigibles (article 9 LOPD i Títol VIII RLOPD). Com ha quedat dit, per aplicació de l'article 12.2 LOPD, el contracte d'encàrrec del tractament ha de contenir de manera expressa, entre d'altres, les mesures de seguretat que l'encarregat està obligat a implementar.

L'article 28.3.c) del RGPD preveu que el contracte d'encàrrec del tractament ha d'estipular que l'encarregat *"tomará todas las medidas necesarias de conformidad con el artículo 32".* Segons l'article 32 del RGPD:

> *"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; (...)".*

A més, el RGPD explicita que l'encarregat ha d'ajudar el responsable a aplicar les mesures de seguretat que pertoqui, tenint en compte la naturalesa del tractament i la informació a disposició de l'encarregat (art. 28.3.f) i art. 32 RGPD).

El RGPD configura un sistema de seguretat que no es basa en els nivells de seguretat bàsic, mitjà i alt, previstos al RLOPD i que segueixen temporalment vigents, sinó en determinar, arran d'una prèvia valoració dels riscos, quines mesures de seguretat són necessàries en cada cas, tenint en compte el tipus d'informació tractada (Considerant 83 RGPD).

Segons l'article 24.1 RGPD:

> *"Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario."*

A més, com hem dit, segons l'article 28.3.c) RGPD l'encarregat ha de prendre totes les mesures de seguretat que siguin necessàries.

És a dir, més que l'establiment de mesures concretes predeterminades en atenció al tractament i la informació tractada, el RGPD estableix un **esquema integral de seguretat,** en el qual cal determinar quines mesures cal aplicar, a partir de les característiques del tractament, i d'una anàlisi de riscos en els termes del RGPD (Considerants 83 i 84).

Als efectes que interessen, un element fonamental que la Universitat haurà de tenir en compte, és el model de seguretat que implementa, en aquest cas, Microsoft, com a encarregat del tractament, i si realitza una valoració de riscos.

Segons explicita el document de Serveis Online de Microsoft, d'1 de novembre de 2016 (apartat de *"Termes de privacitat i Seguretat*"), *"Microsoft es compromet a ajudar a protegir la seguretat de la informació del Client. Microsoft ha implementat, mantindrà i seguirà les mesures tècniques i organitzatives adequades amb l'objectiu de protegir les Dades de Client en cas de pèrdua accidental, no autoritzada o l'accés no autoritzat o il·lícit, la revelació, l'alteració, la pèrdua o la destrucció. (...).*

D'entrada, que Microsoft expliciti que es compromet a ajudar a protegir la informació tractada, i que aplicarà les mesures tècniques i organitzatives adequades, pot entendre's com una previsió que dóna compliment, en principi, als requeriments de l'article 9 LOPD, que exigeix l'aplicació de mesures tant per part del responsable (la Universitat) com, en aquest cas, pel propi encarregat (Microsoft).

Dit això, el mateix apartat del document d'1 de novembre de 2016, citat, es concreten les mesures de seguretat establertes per Microsoft per als serveis online (als que es refereix la consulta), que s'engloben en els següents apartats (pàgines 11 i 12), els quals resumim a continuació:

- *Organització de seguretat de la informació.* Microsoft preveu l'obligació de confidencialitat per al personal de Microsoft amb accés a les dades del client. El document consultat explicita que *"Microsoft va fer una avaluació de riscos abans de tractar les Dades de Client o de llançar el servei de Serveis Online. Microsoft reté els vostres documents de seguretat d'acord amb els vostres requisits de retenció després que hagin deixat de tenir vigència.".* Per tant, segons la informació disponible, Microsoft hauria fet una avaluació de riscos abans de tractar les "dades del "client" (denominació que el document defineix com *"totes les dades, inclosos tots els fitxers de text, so, vídeo, imatge que el Client, o qui el representi, proporcioni a Microsoft mitjançant el seu ús del Servei Online"*).

- *Gestió d'actius*. Microsoft manté un inventari de tots els suports físics on s'emmagatzemen les dades de client amb accés restringit, i classifica les dades de client per facilitar-ne la identificació i perquè l'accés que s'hi fa estigui adequadament restringit. També es preveu que el personal de Microsoft ha d'obtenir l'autorització de Microsoft abans d'emmagatzemar dades de client en dispositius portàtils, accedir-hi de manera remota o tractar-los fora de les instal·lacions de Microsoft.

- *Seguretat de recursos humans*. Microsoft preveu informar el seu personal dels procediments de seguretat pertinents i de les seves respectives funcions, i de possibles conseqüències de l'incompliment dels procediments de seguretat previstos.

- *Seguretat física i ambiental*. Entre d'altres qüestions, es preveu limitar l'accés a les instal·lacions on estan ubicats els sistemes d'informació que tracten les dades de client a persones autoritzades identificades; Microsoft utilitza diversos sistemes estàndard del sector per a la protecció contra la pèrdua de dades ocasionada per un error del sistema d'alimentació o per una interferència de les línies, així com processos estàndard del sector per suprimir les dades del client quan ja no són necessàries.

- *Administració de comunicacions i operacions*. Microsoft manté documents de seguretat on es descriuen les seves mesures de seguretat i els procediments i les responsabilitats pertinents del seu personal que té accés a les dades de client. També procediments de recuperació de dades (De manera constant, però en cap cas amb una freqüència inferior a un cop per setmana (tret que durant aquest període no s'hagi actualitzat cap de les Dades de Client), Microsoft manté diverses còpies de les dades de client des d'on es poden recuperar aquestes dades, còpies de seguretat, procediments de recuperació de dades que s'avaluen periòdicament, i controls de programari maliciós. Microsoft xifra (o permet que el client xifri) les dades que es transmeten per xarxes públiques, i disposa d'un *"Registre d'Esdeveniments",* amb el qual Microsoft registra (o permet que el client registri) l'accés i l'ús de sistemes d'informació que contenen dades de client, que registren l'identificador d'accés, l'hora, l'autorització concedida o denegada, i l'activitat pertinent.

- *Controls d'accés*. Microsoft manté i actualitza un registre del personal autoritzat per accedir als sistemes de Microsoft que contenen les dades del client, accés a les dades, controla les credencials d'autenticació del personal, estableix un accés a dades limitat per

al personal d'assistència tècnica "privilegi mínim", exigeix al seu personal mesures d'integritat i de confidencialitat, i estableix mecanismes d'autenticació en base a procediments estàndard del sector. Incloent pràctiques dissenyades per protegir la confidencialitat i la integritat de les contrasenyes.

- *Gestió d'infraccions de seguretat de la informació.* Microsoft té previst un procés de resposta en cas d'infracció, i manté un registre d'incompliments de la seguretat amb una descripció, el període, les conseqüències de l'incompliment, el nom de l'informador i de la persona a qui s'ha informat de l'incompliment, així com el procediment per recuperar dades. Per a cada incident de seguretat que sigui una Infracció de Seguretat, Microsoft proporcionarà una notificació (com es descriu a la secció "Notificació d'Infracció de Seguretat" anterior) sense retards innecessaris i, en qualsevol cas, en un termini de 30 dies naturals. Microsoft fa un seguiment (o permet que el client faci un seguiment) de les revelacions de dades del client, que inclou les dades que s'han revelat, a qui i en quin moment.

- *Gestió de continuïtat de negocis*. Microsoft manté plans d'emergència i contingència per a les instal·lacions on estan ubicats els sistemes d'informació de Microsoft que tracten les Dades de Client. L'emmagatzematge redundant de Microsoft i els seus procediments per recuperar dades estan dissenyats per intentar reconstruir les Dades de Client en el seu estat original o replicat per última vegada des d'abans del moment en què es van perdre o destruir.

Cal tenir en compte que la Universitat tracta un conjunt d'informació personal, tant del seu propi personal (PAS i PDI) com de l'alumnat, de tipologia diversa (dades economicofinanceres, acadèmiques i de formació, etc), sense descartar la possibilitat que hagi de tractar dades considerades com mereixedores d'especial protecció (article 7 LOPD i art. 9 RGPD).

Tenint en compte això, i sens perjudici que, atesa l'entrada en vigor del RGPD, cal establir un sistema integral de seguretat i no només referir-se a les mesures establertes pel RGPD en funció del nivell exigit (bàsic, mitjà o alt), fem notar que, de la informació consultada, es preveu que Microsoft estableixi entre d'altres mesures relacionades amb la identificació i l'autenticació, amb el control i el registre d'accessos, la realització d'auditories, el xifratge de les dades, o la realització de còpies de seguretat, algunes de les quals són pròpies del nivell alt de mesures de seguretat (arts. 101 a 104 RLOPD), tenint en compte les mesures que, atenent a les circumstàncies del tractament, preveu l'article 32.1 RGPD).

En definitiva, atesa la informació disponible, es pot considerar que el conjunt de les previsions que Microsoft té establertes en el moment d'emetre aquest dictamen (amb data 1 de novembre de 2016), recull en bona mesura el que serien les mesures de seguretat previstes al Títol VIII del RLOPD.

En qualsevol cas, atès que correspon al responsable (la Universitat) la tasca de garantir als afectats (els alumnes de la Universitat, i el seu personal, PAS i PDI) que les seves dades personals seran en tot moment tractades de conformitat amb la legislació vigent en matèria de protecció de dades (article 20.2 RLOPD i art. 28.3 RGPD), la Universitat ha de fer una anàlisi prèvia de l'impacte de la contractació dels serveis *de Microsoft Office 365* i *Azure*, en la privacitat de les dades, tenint en compte la concreta informació personal que previsiblement es tractarà, i l'efectiva implantació de les mesures esmentades.

Cal tenir en compte que en la documentació consultada (apartat d'organització de seguretat de la informació) Microsoft explicita que ***es duu a terme una avaluació de riscos,*** *abans de tractar les dades de client o de llançar el servei de Serveis Online.*

Per tant, el model de gestió de la seguretat de la informació dels serveis objecte de consulta (i les mesures de seguretat, tècniques i organitzatives, que caldrà aplicar) estaria basat en la prèvia avaluació del risc, com exigeix el RGPD, de manera que, de cara a la plena aplicació del RGPD, els serveis estudiats de Microsoft (Office 365 i Azure), es podrien considerar, en principi, adequats, pel que respecta a l'aplicació de mesures de seguretat.

En relació amb el model de seguretat de les dades, cal tenir especialment en compte els **mecanismes de certificació.**

En línia amb el que s'ha apuntat sobre el fet que una empresa s'hagi adherit a l'Escut de Privacitat, es pot tenir en compte si una empresa utilitza mecanismes de certificació, a l'hora de considerar si un determinat servei (en aquest cas, Office 365 i Azure), s'ajusten a les exigències de la normativa europea de protecció de dades.

Segons disposa l'article 28.5 del RGPD: *"La adhesión del encargado del tratamiento a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a que se refieren los apartados 1 y 4 del presente artículo."*

Així, el RGPD preveu la utilització de mecanismes de certificació (veure, al respecte, l'article 25.3 RGPD). Segons disposa l'article 42 del RGPD:

> *"1.Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la* ***creación de mecanismos de certificación*** *en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas.*
>
> *(...)".*

Sens perjudici de la concreció que pugui tenir aquesta previsió del RGPD, el responsable hauria de tenir en compte els mecanismes de certificació de que disposa Microsoft actualment. En el marc de l'encàrrec del tractament que establiria la Universitat amb Microsoft, que aquesta empresa compleixi amb certs estàndards de seguretat, pot ser un indicador a tenir en compte.

Com indica Microsoft en el seu document *"Termes dels Serveis Online",* citat (apartat *"Directiva de Seguretat de la Informació de Serveis Online*, pàg. 13): *"Cada Servei Online segueix una política de seguretat de dades escrites ("Política de Seguretat de la Informació") que compleix amb els marcs i estàndards de control que es mostren a la taula següent."* Segons la taula indicada, els Serveis d'Office 365 i d'Azure compleixen amb els marcs i estàndards de control de la ISO 27001 (norma certificable pel que fa a gestió de seguretat de la informació, que està activa, segons la informació disponible al web de l'entitat que certifica els serveis de Microsoft (BSI- *British Standards Institution*), de la ISO 27018 (norma que, alineada amb la ISO 27001, descriu el codi de pràctiques per a la protecció de dades personals tractades per encarregats del tractament mitjançant serveis al núvol, que per la informació consultada, també es troba activa), i de la ISO 27002 (codi de pràctiques pels controls de seguretat de la informació, equivalent a la ISO 27018, però per a qualsevol tipus de sistemes d'informació, no només referits a serveis al núvol.)

Addicionalment, fem notar que tant "Office 365" com "Azure", estan certificats conforme a l'Esquema Nacional de Seguretat (regulat pel Reial decret 3/2010, de 8 de gener), per a sistemes de categoria alta, segons la informació disponible a

https://www.microsoft.com/en-us/TrustCenter/Compliance/SpainENS. En el web de l'empresa, s'explica que tant Microsoft Azure com Microsoft Office 365, han passat una rigorosa auditoria que ha realitzat una tercera empresa, l'informe de la qual considera que les mesures de seguretat dels dos serveis, així com els serveis d'informació i el tractament de les dades, dóna compliment als requisits de nivell alt, en aplicació de la normativa, sense que s'hagi considerat necessari, en aquesta auditoria, aplicar mesures correctores.

Sens perjudici que això es pot considerar com un indici d'un nivell adequat de protecció de la informació, com ha fet avinent aquesta Autoritat en els Dictàmens 57/2013 o 55/2016, disposar d'una o altra certificació o estàndard internacional en matèria de seguretat no garanteix per sí sol el compliment de les mesures de seguretat exigibles, especialment, en casos en què s'utilitza la computació en el núvol. Sens perjudici de la pertinença que Microsoft disposi d'aquestes certificacions i que la Universitat ho pugui tenir en compte, aquesta, com a responsable, ha de vetllar pel compliment de totes les exigències derivades del RGPD.

VI

Notificació de violacions de seguretat

Com ha quedat dit, l'article 28.3.f) del RGPD disposa que el contracte d'encàrrec del tractament ha de preveure que l'encarregat ajudarà al responsable (la Universitat, en el cas que ens ocupa), al compliment de les obligacions establertes, entre d'altres, en l'article 33 RGPD, segons el qual:

> *"1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida (…).*
>
> *2. El **encargado del tratamiento** notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.*
>
> *(…)."*

Com ha quedat dit, en l'apartat de *"Gestió d'infraccions de seguretat de la informació",* del document d'1 de novembre de 2016, s'explicita que, per a cada incident de seguretat que sigui una Infracció de Seguretat, Microsoft proporcionarà una notificació sense retards innecessaris i, en qualsevol cas, en un termini de 30 dies naturals.

Aquesta notificació es concreta en el mateix document, a la secció *"Notificació d'Infracció de Seguretat",* en la qual es preveu que *"Si Microsoft tingués coneixement de qualsevol accés il·lícit a les Dades de Client emmagatzemades a l'equip o les instal·lacions de Microsoft, o l'accés no autoritzat a aquests equips o instal·lacions derivés en la pèrdua, revelació o alteració de les Dades de Client (considerat cadascun d'ells com una "Infracció de Seguretat"), Microsoft, de manera immediata, us demanarà que (1) notifiqueu la Infracció de Seguretat al Client; (2) investigueu la Infracció de Seguretat i proporcioneu al Client informació detallada sobre la Infracció de Seguretat; i (3) preneu mesures raonables per mitigar els efectes i minimitzar els danys derivats de la Infracció de Seguretat. Les Notificacions d'Infraccions de Seguretat es lliuraran a un o més dels administradors del Client per qualsevol mitjà que Microsoft seleccioni, inclòs el correu electrònic. (...)."*

És a dir, segons la informació disponible, actualitzada i vigent en el moment d'emetre aquest dictamen, Microsoft es compromet amb el client (als efectes que ens ocupen, la Universitat, si contracta els serveis online objecte de consulta), a que li comunicarà les

infraccions de seguretat *"de manera immediata",* previsió que podria considerar-se ajustada a la previsió de l'article 33.2 RGPD, segons la qual l'encarregat està obligat a comunicar sense dilacions indegudes aquestes situacions.

VII

Subcontractació

Pel que fa a la subcontractació de part del tractament de dades que un responsable encarrega a un tercer, la normativa preveu que aquesta ha d'estar autoritzada pel responsable (art. 21 RLOPD).

En igual sentit, es pronuncia l'article 28.2 RGPD:

> *"El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios."*

Segons el document dels *"Termes dels Serveis Online"* (1 de novembre de 2016), citat, *"Microsoft pot contractar subcontractistes per proporcionar determinats serveis limitats o suplementaris en nom seu. Qualsevol subcontractista a qui Microsoft transmeti Dades del Client, fins i tot els utilitzats amb finalitats d'emmagatzematge,* ***haurà de celebrar contractes per escrit*** *amb Microsoft que exigeixin una* ***protecció almenys equivalent*** *a la que ofereixen els DPT. El Client ha acceptat anteriorment que Microsoft transmeti les Dades del Client als subcontractistes com es descriu als DPT. Llevat en allò que s'estipula als DPT, o com el Client pugui autoritzar d'altra manera, Microsoft no transmetrà a cap tercer (ni tan sols amb finalitats d'emmagatzematge) les dades personals que el Client proporcioni a Microsoft a través de l'ús dels Serveis Online. Microsoft proporciona un lloc web que indica una llista de subcontractistes que estan autoritzats a accedir a les Dades del Client dels Serveis Online i als serveis limitats o suplementaris que proporcionen. Com a mínim 6 mesos abans d'autoritzar qualsevol nou subcontractista perquè accedeixi a Dades del Client, Microsoft actualitzarà el lloc web corresponent i proporcionarà al Client un mecanisme per obtenir la notificació d'aquesta actualització.* ***Si el Client no aprova un nou subcontractista,*** *el Client pot resoldre el Servei Online afectat sense sanció proporcionant, abans que acabi el període de notificació, una notificació escrita de resolució que inclogui una explicació dels motius de la no-aprovació (...)."*

Es deriva d'aquesta informació que el client, en el cas que interessa, la Universitat, haurà d'estar informat i autoritzar una possible subcontractació en relació amb el tractament de les dades de les que és responsable, en uns termes que en principi s'ajustarien a les previsions de la normativa de protecció de dades.

En qualsevol cas, d'acord amb el Dictamen 5/2012, del Grup de Treball de l'Article 29, sobre computació en el núvol, en cas que existeixi un o varis subcontractistes caldria especificar el nom de cadascú en el contracte. Així mateix, els proveïdors dels serveis examinats hauran de signar un contracte específic amb cada subcontractista en què es fixin totes les obligacions que el client (el responsable) ha imposat al proveïdor i que aquests també hauran de complir (apartats 3.3.2 i 3.4.2.7 del Dictamen).

Com ha quedat dit, en el document de *"Termes de Serveis Online",* d'1 de novembre de 2016 (Annex 3) es preveu el compliment de les Clàusules Contractuals Estàndard de la Decisió de la Comissió de 5 de febrer de 2010. La clàusula 11 de la Decisió esmentada especifica les condicions del *"subtractament de dades"* que, per tant, resulten d'aplicació al cas que ens ocupa.

Només garantint el compliment d'aquestes condicions es podria admetre, des de la vessant de la protecció de dades, la participació d'empreses subcontractades en la prestació del serveis Microsoft Office 365 i Azure, a contractar per la Universitat.

VIII

Realització d'auditories

La consulta fa referència, específicament, als mecanismes que cal contemplar per realitzar les auditories corresponents, en relació amb els productes en qüestió (Office 365 i Azure)

Com ha fet avinent aquesta Autoritat, pertoca al responsable del tractament (en el cas que ens ocupa, la Universitat), vetllar perquè l'empresa responsable dels serveis en qüestió, com a encarregat del tractament, garanteixi la implementació de les mesures de seguretat que cal aplicar, previstes al RLOPD (article 20.2 RLOPD), i les que correspongui aplicar, en base al model integral de seguretat a què es refereix el RGPD, en els termes apuntats.

Pel que fa a la realització d'auditories, ens remetem a la previsió de l'article 96 RLOPD.

L'article 28.3.h) del RGPD disposa, en relació amb el contracte d'encàrrec del tractament, aquest ha d'estipular, en particular, que l'encarregat:

> *"h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable."*

En la informació disponible al web de Microsoft ("*Microsoft Trust Center*", citat), s'explicita que l'empresa compta amb exhaustius mecanismes d'auditoria. En el Document de *"Termes dels Serveis Online",* d'1 de novembre de 2016 (apartat "Auditories de Microsoft de Serveis Online", pàg. 13), Microsoft preveu que anualment es realitzin, per tercers independents i qualificats, auditories dels seus sistemes d'informació, afectant a cadascun dels serveis, i que com a resultat de cada auditoria es generarà un informe, que *"revelarà amb claredat qualsevol conclusió de material per part de l'auditor. Microsoft solucionarà immediatament el problemes que es plantegin en qualsevol Informe d'Auditoria de Microsoft per aconseguir la conformitat de l'auditor."*

El document també preveu que el client, si ho sol·licita per escrit, pot obtenir còpia de l'informe d'auditoria, *"perquè el Client pugui verificar el compliment per part de Microsoft de les obligacions en matèria de seguretat en virtut del DPT* (Data Processing Terms) *(...)".*

Fem avinent que Microsoft disposa de l'anomenat *"Service Trust Portal"* (STP), que posa a disposició dels seus clients i els permet accedir a informació sobre certificacions, seguretat i auditories dels seus serveis. Segons la informació consultada:

"The Service Trust Portal (STP) serves customers of Microsoft Azure, Microsoft Dynamics CRM Online, and Microsoft Office 365 (including Yammer) with both active and trial subscriptions. It offers access to a deep set of security, privacy, and compliance resources, such as ***independent audit reports of Microsoft cloud services****, risk assessments, security best practices, and other such materials".*

És a dir, la Universitat, com a responsable que ha de vetllar per la realització d'auditories per part de l'encarregat (art. 28.3.h) RGPD), disposa d'aquest mecanisme d'auditoria, dut a terme per un tercer independent, que preveu Microsoft.

També fem notar que, en la Resolució de declaració d'adequació de garanties de l'AEPD, de 9 de maig de 2014, ja es va tenir en compte que els serveis de Microsoft, entre els quals, Office 365 i Azure, *"incorporan la posibilidad de que el cliente acepte que sea el importador quien audite, al menos anualmente, la seguridad de los ordenadores y el entorno de computación que utilice el tratamiento de los datos del cliente, llevándose a cabo la auditoría por terceros profesionales en materia de seguridad y concediéndose al cliente, si así lo solicita, el acceso a la información mediante un resumen confidencial del informe de auditoría llevada a cabo. Asimismo, se indica que si el cliente desea cambiar esta instrucción acerca del ejercicio de su facultad de auditoría tiene derecho a hacerlo según lo mencionado en las cláusulas contractuales tipo, solicitándolo por escrito."*

L'AEPD va considerar *"que estas condiciones proporcionan garantías suficientes para la transmisión de datos a los Estados Unidos en el marco de la prestación de servicios de computación en nube a los que se refiere el presente expediente".*

Per tot això, en principi, es pot considerar que el mecanisme d'auditoria que ofereix Microsoft en el moment d'emetre aquest dictamen (segons les condicions d'1 de novembre de 2016), continua essent adequat a les exigències de la normativa de protecció de dades.

En qualsevol cas, tenint en compte la previsió de l'article 28.3.h) RGPD si la Universitat considerés que aquest sistema no resulta prou adequat o suficient, també es pot adreçar a Microsoft per articular un altre mecanisme d'auditoria. Vista la documentació que aporta Microsoft (pàg. 13 *"Termes dels serveis Online*"), aquesta empresa ofereix al client (en el cas que interessa, la Universitat), la possibilitat de fer una auditoria directament, seleccionant el seu propi auditor.

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

Conclusions

Tenint en compte la Decisió de la Comissió de 5 de febrer de 2010, la Resolució de l'AEPD de 9 de maig de 2014, així com l'adhesió de Microsoft a l'Escut de Privacitat, es pot considerar que el contracte d'encàrrec del tractament que podria subscriure la Universitat amb Microsoft en relació amb els serveis "Microsoft 365" i "Microsoft Azure", seguiria en principi ajustant-se a les exigències de la normativa de protecció de dades (LOPD, RLOPD i RGPD).

Pel que fa a les mesures de seguretat tècniques i organitzatives per garantir la seguretat de les dades, es pot considerar que les previsions de Microsoft en relació amb els serveis "Microsoft 365" i "Microsoft Azure" poden ser, a priori, adequades al que preveu la normativa de protecció de dades tenint en compte que la implantació de les mesures previstes és objecte de certificació i auditoria per part d'un tercer independent.

Barcelona, 29 de novembre de 2016