- Procedimiento nº.: E/10350/2020

ASUNTO: Recurso de Reposición Nº RR/00784/2021

Examinado el recurso de reposición interpuesto por Don ***A.A.A.*** contra la resolución dictada por la Directora de la Agencia Española de Protección de Datos en el expediente de actuaciones previas de inspección E/10350/2020, y en base a los siguientes:

HECHOS

PRIMERO: Con fecha 24 de noviembre de 2021, se dictó resolución por la Directora de la Agencia Española de Protección de Datos en el expediente de actuaciones previas de inspección E/10350/2020, procediéndose al archivo de actuaciones.

Dicha resolución, que fue notificada al recurrente en fecha 3 de diciembre de 2021, según aviso de recibo que figura en el expediente.

SEGUNDO**:** Don ***A.A.A.*** (en lo sucesivo el recurrente) ha presentado en esta Agencia, en fecha 20 de diciembre de 2021, recurso de reposición, fundamentándolo básicamente en que en el mes de enero de 2021 se dirigió al DPD de la Universidad haciéndole una serie de preguntas sobre si se realizaban transferencias internacionales de datos y que medidas se tomaban para impedir que sus datos fuesen interceptados por el Gobierno de ******PAÍS.1***. La contestación es “Tiene más razón que un santo, la verdad”. Tras recibir la resolución solicita que se actúe de manera proactiva y se investigue.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el presente recurso la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo LPACAP).

II

A pesar de la extensión de la resolución ahora recurrida, es necesario reproducirla para que se compruebe las actuaciones realizadas.

*“PRIMERO: Don **A.A.A.** (en adelante, la parte reclamante), con fechas 29 de septiembre y 12 de octubre de 2020, interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra UNIVERSIDAD *****UNIVERSIDAD.1** con CIF *****CIF.1** (en adelante, la parte reclamada).*

Los motivos en que basa la reclamación son los siguientes:

*- Utilización de los servicios de GOOGLE por parte de la UNIVERSIDAD *****UNIVERSIDAD.1** DE MADRID, los cuales realizan transferencias internacionales de*

datos personales a ******PAÍS.1****, tras la Sentencia del TJUE del 16 de julio de 2020, que invalida la Decisión 2016/1250 sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-*******PAÍS.1.*** *La parte reclamante recuerda que dicha Sentencia es de aplicación inmediata, y prescribe que las organizaciones europeas de cualquier tipo deben abstenerse de utilizar aplicaciones o plataformas cuyo prestador de servicio tenga su sede social en* ******PAÍS.1****, hasta que se garantice el nivel de protección adecuado para las transferencias internacionales de datos personales. En la situación actual, no existen garantías para que las personas no nacionales de ese país, y, en concreto, los usuarios de la Universidad no sean objeto de control por parte de instancias no autorizadas.*

*- Concretamente, es el departamento de Análisis Social de la mencionada Universidad, la que utiliza el servicio de videoconferencia GOOGLE MEETS para la preparación y celebración de Consejos de Departamento a distancia, en base a un acuerdo de 2013 concluido tras licitación pública, que ponía a disposición de la organización el servicio "*******SERVICIO.1****", el cual consta de una serie de herramientas educativas y de gestión en su versión empresarial de forma gratuita, entre las que figura la mencionada aplicación.*

- Con fecha 28 de septiembre de 2020, la parte reclamante solicitó al DPD de la Universidad el cese inmediato del uso de dichas plataformas, y al Departamento de Análisis Social ese mismo cese y la anulación de los acuerdos colegiados de las sesiones celebradas a través de dichas plataformas. En la respuesta del DPD se justifica el tratamiento de datos en las cláusulas estándar utilizadas por la Compañía Google LLC, antes Google Inc., en este tipo de acuerdos a las cuales, según sugiere el Informe, se habría adherido la Universidad, aunque sin especificar el texto concreto de las cláusulas del acuerdo. También se incluyen enlaces a la Decisión de la Comisión de 5 de febrero de 2010, como justificación y garantía de legalidad (que la parte reclamante considera ya superada), y un enlace a los términos del tratamiento de datos en la propia Universidad, indicando la entidad es responsable del tratamiento de los datos personales de sus empleados. En su R.A.T. dicho tratamiento figura con la denominación "gestión de personal", pero asegura que no incluyen transferencias internacionales de datos, y citan como respaldo el Esquema Nacional de Seguridad (ENS).

- La parte reclamante concluye, como empleado y usuario de los servicios digitales de la Universidad, que los mencionados servicios no pueden utilizarse con garantías de privacidad y no son ajustados al RGPD, por las razones descritas.

Documentación relevante aportada por el reclamante:

- Respuesta de la Universidad ******UNIVERSIDAD.1*** *al reclamante con fecha de 2 de octubre de 2020 y donde consta:*

a. Que la Universidad tiene suscrito un acuerdo con Google para la prestación de diversos servicios, entre ellos, en de la herramienta para la realización de videoconferencia Google meet.
b. Que dicho acuerdo supone la adopción de cláusulas tipo que se suponen garantías adecuadas suficientes que permiten una transferencia internacional de datos sin la necesidad de autorización de la autoridad de control y ello pese a no existir una

decisión de adecuación como pudiera ser el Privacy Shield tras el dictado del TJUE de 16 de julio.
c. Se adjunta informe del DPD de la Universidad ******UNIVERSIDAD.1*** *donde consta:*
i. La Universidad ******UNIVERSIDAD.1*** *es responsable del tratamiento de los datos de sus empleados.*
ii. Que la Universidad ******UNIVERSIDAD.1*** *es responsable del tratamiento "Gestión de personal". Que tiene declarado otro tratamiento llamado "actuaciones administrativas no presenciales". Que en el marco de la actividad "actuaciones administrativas no presenciales" tienen suscrito un acuerdo con Google para la realización de videoconferencias Google-meet.*

Aporta Registro de Actividades del Tratamiento donde consta:

- Una actividad, entre otras, con nombre "actuaciones administrativas no presenciales" donde consta:

En el apartado de "Transferencias internacionales" consta "No precisan de autorización. Garantías adecuadas."

En el apartado de "Base jurídica" consta "El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte para la aplicación a petición de este de medidas precontractuales; El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;"

En el apartado de "Categorías de datos" consta "Datos identificativos: Nombre y apellidos, DNI/CIF/Documento identificativo, dirección correo electrónico. Otros datos propios del tratamiento en particular de que se trate. Otros datos: imagen y voz."

- Una actividad, entre otras, con nombre "gestión de recursos humanos" donde consta:

En el apartado de "Transferencias internacionales" consta "No"

En el apartado de "Categorías de datos" consta:

"Datos identificativos: Nombre y apellidos, DNI/CIF/Documento identificativo, dirección, firma, teléfono
Categorías especiales de datos: datos de salud (bajas por enfermedad, accidentes laborales y grado de discapacidad), afiliación sindical, a los exclusivos efectos del pago de cuotas sindicales, representante sindical, justificantes de asistencia de propios y de terceros.
Datos de características personales: Sexo, estado civil, nacionalidad, edad, fecha y lugar de nacimiento y datos familiares. Datos de circunstancias familiares: Fecha de alta y baja, licencias, permisos y autorizaciones.
Datos académicos y profesionales: Titulaciones, formación y experiencia profesional.
Datos de detalle de empleo y carrera administrativa. Incompatibilidades.
Datos de control de presencia: fecha/hora entrada y salida, motivo de ausencia.

Datos económico-financieros: Datos económicos de nómina, créditos, préstamos,." avales, deducciones impositivas baja de haberes correspondiente al puesto de trabajo anterior (en su caso), retenciones judiciales, otras retenciones. Datos bancarios.
Otros datos: datos relativos a la acción social, datos sobre sanciones en materia de función pública.
Imagen y voz. (Videoconferencias)"

iii. Que según capítulo V RGPD solo se pueden realizar transferencias internacionales cuando se haya adoptado una decisión de adecuación a la que se refiere el art- 45.3 RGPD pero también cuando se hayan adoptado garantías adecuadas según prevé el art. 46 RGPD. Que estas garantías adecuadas se pueden aportar mediante, entre otros, cláusulas tipo de protección de datos adoptadas por la Comisión.

*iv. Que los acuerdos que tiene la Universidad con Google en la medida que pueda suponer una transferencia internacional de datos están regulados por las disposiciones contenidas en el enlace ***URL.1 que son las cláusulas aprobadas por la Comisión mediante la decisión 2010/87/UE.*

v. Que dichas cláusulas suponen la existencia de garantías adecuadas suficientes que permiten una transferencia internacional de datos sin la necesidad de autorización de la autoridad de control y ello pese a no existir una decisión de adecuación como pudiera ser el Privacy Shield tras el dictado de la Sentencia del TJUE de 16 de julio pasado.

*- Aporta copia de Cláusulas Contractuales Estándar de GSuite contenidas en el enlace ***URL.1 donde consta, en inglés (se ha traducido), entre otros aspectos:*

«Cláusulas contractuales tipo (transformadores)
a efectos del artículo 26, apartado 2, de la Directiva 95/46/CE para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países que no garanticen una adecuada protección de los datos.
*la entidad jurídica distinta de Google que acepta las cláusulas (el «exportador de datos») y Google LLC (anteriormente conocida como Google Inc.), *****DIRECCIÓN.1** (el «importador de datos»)*
[...]
Han CONVENIDO en las siguientes cláusulas contractuales (en lo sucesivo, «cláusulas») a fin de ofrecer garantías adecuadas con respecto a la protección de la intimidad y los derechos y libertades fundamentales de las personas para la transferencia por el exportador de datos al importador de los datos personales especificados en el apéndice 1.»
[...]
«exportador de datos»: el responsable del tratamiento que transfiere los datos personales;
«importador de datos»: el encargado del tratamiento que acepte recibir del exportador datos personales destinados al tratamiento en su nombre después de la transferencia, de conformidad con sus instrucciones y los términos de las cláusulas, y que no esté sujeto al sistema de un tercer país que garantice una protección adecuada en el sentido del artículo 25, apartado 1, de la Directiva 95/46/CE;
[...]

Cláusula 5
Obligaciones del importador de datos
El importador de los datos acuerda y garantiza lo siguiente:
a) tratar los datos personales únicamente en nombre del exportador de datos y de conformidad con sus instrucciones y las cláusulas; Si no puede facilitar dicho cumplimiento por cualquier motivo, se compromete a informar sin demora al exportador de datos de su incapacidad para cumplir, en cuyo caso el exportador de datos podrá suspender la transferencia de datos o rescindir el contrato;
b) que no tiene motivos para creer que la legislación que le sea aplicable le impida cumplir las instrucciones recibidas del exportador de datos y sus obligaciones contractuales y que, en caso de que se produzca una modificación de dicha legislación que pueda afectar sustancialmente a las garantías y obligaciones proporcionadas por las cláusulas, notificará sin demora el cambio al exportador de datos tan pronto como tenga conocimiento, en cuyo caso el exportador de datos estará facultado para suspender la transferencia de datos o el contrato;
[...]
Cláusula 7
Mediación y jurisdicción
1. El importador de datos acepta que si el interesado invoca los derechos de terceros beneficiarios o reclama una indemnización por daños y perjuicios en virtud de las cláusulas, el importador de datos aceptará la decisión del interesado;
someter el litigio a la mediación, por una persona independiente o, en su caso, por la autoridad de control;
someter el litigio a los órganos jurisdiccionales del Estado miembro en el que esté establecido el exportador de datos.
[...]
Cláusula 9
Normativa aplicable
Las cláusulas se regirán por la legislación del Estado miembro en el que esté establecido el exportador de datos.
Apéndice 1
[...]
Categorías de datos
Los datos personales transferidos entran dentro de las siguientes categorías de datos: Datos personales presentados, almacenados, enviados o recibidos por el exportador de datos o sus usuarios finales a través de los servicios, incluidos identificadores de usuario, correos electrónicos, documentos, presentaciones, imágenes, entradas de calendario, tareas y otros datos presentados, almacenados, enviados o recibidos por los usuarios finales a través de los servicios.
Categorías especiales de datos (si es pertinente)
Los datos personales transferidos se refieren a las siguientes categorías especiales de datos: Datos presentados, almacenados, enviados o recibidos por los usuarios finales a través de los servicios.
[…]"

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), en fecha 26 de octubre de 2020, se dio traslado de dicha reclamación a la parte reclamada, para que procediese a su análisis e informase a

esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

Con fecha 27 de noviembre de 2020, se presenta escrito de respuesta indicando:

Primero. - En relación con la situación de contexto en que se enmarca la reclamación. La actual situación sobrevenida de crisis sanitaria con motivo de la pandemia por COVID-19 ha supuesto, tanto para la Universidad ******UNIVERSIDAD.1*** *como para toda la sociedad, una situación que ha requerido adaptaciones en la forma de actuar y, en particular, en el desarrollo de las distintas actividades que tienen lugar en la Universidad. Así, tanto las actividades docentes, como de investigación, y las de gestión se desarrollan, con carácter bastante generalizado, a distancia según las circunstancias en cada caso. Una de las formas más generalizadas de realización de actividades a distancia es a través de videoconferencias. A estos efectos, la Universidad tiene un acuerdo con google de Gsuite educación para la prestación de distintos servicios, entre ellos, el de realización de videoconferencias a través de google meet. Toda la información sobre Gsuite educación, se puede encontrar en la siguiente página web de la Universidad:* ******URL.2***

Segundo. - En relación con la información solicitada por esa Agencia. 1.- La decisión adoptada a propósito de la reclamación a que se refiere el requerimiento de la Agencia. Con fecha 28 de septiembre de 2020 el profesor ***A.A.A.*** *presentó escrito dirigido a la Universidad y solicitando "La prohibición inmediata del uso de la plataforma comercial de gestión Google Meet para la convocatoria y celebración de Consejos de Departamento a distancia por parte del Departamento de Análisis Social de la Universidad* ******UNIVERSIDAD.1****, y para otros usos con finalidad educativa", por considerar "Que el uso actual de dicha plataforma comercial incumple la normativa sobre protección de datos y es contrario a la Sentencia del Tribunal de Justicia de la UE del 16 de julio de 2020. Que dicha Sentencia prescribe que las organizaciones de cualquier tipo deben abstenerse de utilizar aplicaciones o plataformas cuyo prestador de servicio tenga su sede social en EE UU, hasta que se garantice el nivel de protección adecuado para la transferencia internacional de datos personales. Que, en la situación actual, no existen garantías para que las personas no nacionales de los Estados Unidos no sean objeto de control por parte de instancias no autorizadas." … / No se ha recibido respuesta a este escrito.*
Se adjunta copia de dicha solicitud como documento nº 1 unido a este escrito. Por la Universidad se solicitó un informe al Delegado de Protección de Datos al respecto de la reclamación presentada, que se adjunta a este escrito como documento nº 2. Por la Universidad se procedió a contestar al indicado profesor sobre la base del citado informe en los términos que constan en el escrito de la directora del Departamento de Análisis Social que se adjunta a este escrito como documento nº 3. Como es de ver, se procedió a contestar al indicado profesor sobre la base de considerar que existe una situación ajustada a derecho en la utilización de la herramienta de google meet tras el dictado de la Sentencia del TJUE que dejó sin efecto el escudo de privacidad de Estados Unidos, toda vez que, en lugar de tener lugar la transferencia internacional de datos al amparo de una decisión de adecuación del nivel de protección adecuado a que se refiere el artículo 45.3 del RGPD, como era el caso del Privacy Shield de Estados Unidos, ésta tiene lugar con garantías adecuadas, como son las cláusulas tipo de protección de datos adoptadas por la Comisión. Como complemento a lo manifestado anteriormente, se adjuntan, además, la comunicación por correo

electrónico remitido por Google en el que consta la aplicación de cláusulas tipo de protección de datos desde el mes de junio de 2020, así como un pantallazo del sistema de gestión de acuerdos con Google de la Universidad del que resulta esta circunstancia. Documentos nº 4 y 5.
(…)
Informe sobre las causas que han motivado la incidencia que ha originado la reclamación. Desde la Universidad se considera que han existido dos causas que han motivado la reclamación: Por un lado, la novedad en la utilización de las herramientas de videoconferencia en la actual situación de pandemia, en la que las autoridades sanitarias han recomendado evitar en la medida de lo posible la celebración de reuniones presenciales, como pueda ser la de un Consejo de un Departamento en la Universidad. Por otro lado, la noticia difundida en los medios de comunicación de la anulación del escudo de privacidad por el TSJE el pasado 16 de julio, y que suponía la necesidad de adoptar por los responsables del tratamiento, en el caso de verse afectado por esta decisión, garantías adecuadas para la transferencia internacional de datos. Ante esta situación, el profesor ***A.A.A.*** *ha presentado el escrito a que se ha hecho referencia, y se le ha informado acerca de cuáles eran las garantías adecuadas adoptadas por la Universidad, con lo que se considera, ha sido adecuadamente atendido su ejercicio de derecho de acceso en los términos a que se ha hecho referencia más arriba.*

Informe sobre las medidas adoptadas para evitar que se produzcan incidencias similares, fechas de implantación y controles efectuados para comprobar su eficacia. A la vista de que se trata de la única solicitud de acceso que ha tenido lugar en la Universidad, tanto entre el colectivo del personal, como entre el colectivo de estudiantes, se ha considerado que no es necesario la adopción de ninguna medida al respecto.

TERCERO: Con fecha 9 de diciembre de 2020, se admitió a trámite la reclamación presentada por la parte reclamante, al amparo de lo establecido en el artículo 65.5 de la LOPDGDD.

CUARTO: Con fecha 17 de enero de 2021, la parte reclamante presenta nuevo escrito en el que, en síntesis, señala lo siguiente:

*- Que a partir del 16 de julio 2020 las transferencias de datos a ***PAÍS.1 han sido declaradas ilegales y contrarias al RGPD a menos que exista un "nivel adecuado" de protección.*
*- Que estas transferencias se realizarían, entre otras, a través de la Plataforma o servicio comercial ***SERVICIO.1cation.*
- Que solicita el cese inmediato de dichas transferencias en caso de no ser acordes con las garantías exigidas por el RGPD.
- Que los acuerdos firmados con Google LLC/Google Inc podrían haberse celebrado en el año 2013 para Google Suite para Educación (gratuito) y tal vez en el año 2020 para la versión de pago Google Suite Enterprise para Educación.

Documentación relevante aportada por el reclamante:

- *Copia de correo electrónico remitido por el DPD de la Universidad* ******UNIVERSIDAD.1 ***EMAIL.1****, con fecha 15 de enero de 2021, enviado "****A.A.A. ***EMAIL.2"*** *donde consta:*

a. La universidad trata datos del reclamante mediante la utilización de los servicios que presta la compañía Google, en particular con la herramienta de videoconferencia Google Meet.
b. Que, por otro lado, la universidad es responsable del tratamiento de datos personales de sus empleados según el Registro de Actividades de Tratamiento con la denominación "Gestión de Personal".
c. A su vez la Universidad tiene declarado el tratamiento "actuaciones administrativas no presenciales".
d. Que la Universidad tiene un acuerdo con Google para la prestación de dichos servicios, entre ellos, el de la herramienta Google Meet.
*e. Que en el marco de dicho acuerdo tienen lugar transferencias internacionales de datos a ***PAÍS.1 en los términos contemplados en el RGPD.*
*f. Que los acuerdos que tiene la Universidad con Google en la medida que pueda suponer una transferencia internacional de datos están regulados por las disposiciones contenidas en el enlace ***URL.1 que son las cláusulas aprobadas por la Comisión mediante la decisión 2010/87/UE.*
g. Que toda la información relacionada con los acuerdos adoptados por la Universidad con Google se puede encontrar en el enlace ******URL.3****.*
h. "Finalmente, en la medida en que las transferencias internacionales se están realizando en el marco de lo dispuesto en el RGPD, no se puede admitir la solicitud formulada por el interesado de que las mismas dejen de hacerse, ya que, frente a la oposición formulada, resultan motivos legítimos imperiosos de la Universidad como responsable del tratamiento, en la medida en que, gran parte de los procesos de gestión se llevan a cabo a través de los servicios y herramientas prestados por Google y, en particular, en la actual situación de pandemia resulta necesario la celebración de reuniones de departamento online, para Io cual la Universidad pone a disposición de su personal la herramienta Google-meet, con las garantías adecuadas según se ha señalado más arriba, sin que puedan prevalecer los intereses y derechos y las libertades del interesado que, como se ha señalado, es un empleado de la Universidad funcionario docente. La Universidad que presta el servicio público de la educación superior debe seguir prestando dicho servicio con continuidad, desarrollando gran parte de su actividad de manera online."

QUINTO: Con 23 de abril de 2021, se recibe nuevo escrito de la parte reclamante en el que señala lo siguiente:

*- Que muchos RATs admiten transferencias internacionales. Que esas transferencias no se realizan solo a ***PAÍS.1 sino a países como ***PAÍS.2. Entre esos tratamientos están "Movilidad internacional", "Contacta (***PAÍS.1)", "Ponentes y conferenciantes". El tratamiento "Órganos de gobierno" se describe como no internacional, pero utilizan medios susceptibles de transferencias a ***PAÍS.1 como Google Hangouts Meets. El tratamiento "Evaluación Académica online" y "Puertas abiertas" invocan el Privacy Shield.*
- Que bien el contrato lo haya firmado la Universidad con GOOGLE LLC o GOOGLE IRELAND, y ya que ésta controlada por GOOGLE LLC que posee el 100%

de sus acciones, es impensable que las transferencias de datos dentro de la Unión Europea queden al margen de las interferencias de la empresa de la cual depende.

- Que GOOGLE LLC tiene la calificación de "electronic data provider" (FISA-702) y por tanto debe colaborar con los programas de vigilancia masiva de las agencias norteamericanas (PRISMA, UPSTREAM, etc) y permitir otras formas de intrusión ampliamente extendidas (EO 12333, warrants, etc)

- Que lo mismo se puede decir de las transferencias a la nube que están sujetas al control estricto de la ley norteamericana (Cloud Act 2018).

- Que como ha señalado el EDPB, la mera ubicación de datos en la Unión Europea no basta ya que lo significativo es la posibilidad factual de acceder a los mismos.

*- Que desde septiembre 2020 se habría cambiado la ubicación de los datos (política de región de datos) para la versión de pago de Google Workplace en centros europeos y no en ***PAÍS.1 como sucedía en la versión anterior GSuite for Education (2013-2020) pero según el DPD los colectivos afectados por la política de región de datos serían el personal empleado con relación vigente con la universidad (personal auxiliar o PAS y personal docente e investigador) que la propia universidad estima en 2500 licencias en el curso académico 2020-2021, al menos del 10% del total de usuarios. En cambio, quedan excluidos los estudiantes que alcanzan un total de 25000 licencias.*

- Que el DPD no menciona las actividades externalizadas como los servicios médicos de la universidad (XXXXXX) que manejan y envían informaciones y datos personales especialmente sensibles que proceden de todos los colectivos. Tampoco se informa de cambios en la configuración para secciones sindicales (XXXXXX). El DPD tampoco menciona las comunicaciones cruzadas (las que tienen lugar entre empleados, estudiantes y los servicios externalizados, que son con mucho mayoritarias en la universidad.

*- Solicita la suspensión inmediata de las transferencias internacionales de la Universidad ***UNIVERSIDAD.1 a ***PAÍS.1 y otros países que no garantizan la equivalencia de garantías. Solicita la suspensión o finalización del uso de plataformas como Google Workspace for Education y servicios derivados (Google Gmail, Meet,….) que son incompatibles con las garantías Comunitarias. Solicita la supresión de los datos personales de los usuarios exportados entre 2013, y 2021 a países terceros que practican programas de vigilancia masiva, como los ***PAÍS.1 y otros.*

SEXTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

*1. Que existe un acuerdo entre la Universidad ***UNIVERSIDAD.1y Google Ireland Limited para la prestación de servicio GSuite for Education, hoy Google Workspace for Education.*

*2. Que, a este respecto, las solicitudes de información y cómo se procede en función de con quién se ha firmado el contrato y quién solicita la información, puede consultarse en el enlace *****URL.4**. Que son los siguientes términos:*

"Solicitudes de autoridades gubernamentales de fuera de Irlanda Google Ireland ofrece servicios a usuarios de todo el Espacio Económico Europeo y de Suiza, y a veces recibe solicitudes de divulgación de datos procedentes de autoridades gubernamentales de fuera de Irlanda. En ese caso, puede proporcionar datos de usuario si al hacerlo cumple con lo siguiente:
La ley irlandesa, lo que significa que el acceso y la divulgación se permiten en virtud de la ley irlandesa aplicable como, por ejemplo, la ley de justicia penal irlandesa
La ley de la Unión Europea (UE) aplicable en Irlanda, lo que significa cualquier ley de la UE aplicable en Irlanda, incluido el Reglamento General de Protección de Datos (RGPD)
La ley del país solicitante, lo que significa que necesitamos que la autoridad pertinente siga los mismos procedimientos y requisitos legales que se aplicarían si la solicitud se hiciera a un proveedor local de un servicio similar
Las normas internacionales, lo que significa que solo proporcionamos datos en respuesta a solicitudes que cumplen los principios de libertad de expresión y de privacidad de la Global Network Initiative y sus directrices de implementación asociadas
Las políticas de Google, que incluyen todas las políticas de privacidad y todos los términos del servicio aplicables, así como las políticas relacionadas con la protección de la libertad de expresión"

3. "*De lo anterior resulta que, con carácter general, en el marco de los acuerdos con Google Ireland, se aplica la normativa de la Unión Europea y, por tanto, las garantías contenidas en el RGPD a efectos de comunicaciones de datos a autoridades gubernamentales de fuera de Irlanda y, por tanto, de USA."*

4. Que la ubicación de los datos relativos a GSuite Enterprise for Education es territorio europeo. Que esta configuración es establecida para los docentes con relación indefinida durante la vigencia de su relación contractual con la Universidad.

5. Que la Universidad tiene suscrito un acuerdo de procesamiento de datos en el marco de GSuite que incluye a todas las filiales de Google entre ellas Google Ireland Limited y que puede consultarse en ******URL.5.***

6. La Universidad trata los datos del reclamante, profesor y empleado de la Universidad, mediante la utilización de los servicios que presta la compañía Google y en particular la herramienta de videoconferencia Google Meet.

7. Que se ha suscrito acuerdo de prestación de servicios en el marco GSuite for Education con Google Ireland, entidad ubicada en Irlanda y sujeta plenamente al RGPD. Que en principio no tienen lugar transferencias internacionales de datos.

8. Que para los supuestos en que los datos son transferidos por Google Irlanda a otras filiales de Google resultan de aplicación las cláusulas contractuales tipo en ******URL.6.***

9. Además la Universidad facilita los siguientes datos personales de los interesados para darles de alta como usuarios de dichos servicios: Nombre, Apellidos, correo electrónico y Colectivo al que pertenece.

10. Que con el compromiso de cumplimiento del RGPD de Google Ireland en ******URL.7****, el acuerdo de tratamiento de datos en el marco de GSuite* ******URL.8****, así como las cláusulas contractuales tipo asegurándose Google de que GOOGLE LLC cumplirá dichas cláusulas, se han implementado las siguientes medidas técnicas y organizativas adicionales, entre otras:*

a. "Tras la contratación del servicio GSuite Enterprise for Education, se ha establecido la configuración de datos de todos los usuarios con dicha licencia en

territorio europeo. Esta licencia y, por tanto, ubicación es establecida por defecto para los docentes con relación indefinida durante la vigencia de su relación contractual con la Universidad."
b. "Se encuentran habilitadas las alertas del log de transparencia de acceso de modo que los administradores recibirán una notificación en caso de acceso por parte de trabajadores de Google a información de la institución, excepto en los casos detallados en ******URL.9****"*
11. Que la Universidad ha contratado bajo la denominación de GSuite Enterprise for Education según la información ubicada en ******URL.10*** *y* ******URL.11.***

Con fecha 31 de mayo de 2021 se comprueba el contenido de la url ******URL.12*** *donde consta entre otros aspectos:*

*"En el año 2013 la Universidad ***UNIVERSIDAD.1 firmó un acuerdo que pone a disposición de las universidades el servicio ***SERVICIO.1 (actualmente GSuite for Education).*
Fruto de ese acuerdo, la Universidad dispone de acceso de forma gratuita entre otras a las siguientes herramientas:
- Cuentas de Google
- Gmail
- Drive
- Calendar
- Meet
[…]
Desde Septiembre de 2020, además de las licencias GSuite for Education gratuitas, la Universidad dispone de licencias GSuite Enterprise for Education[…]
La política actual de licencias es la siguiente:

Colectivo	*Tipo de Licencia*
Docente con relación vigente	*GSuite Enterprise for Education Teacher (con grabación ilimitada en Meet para sus clases)*
Investigador con relación vigente	*GSuite Enterprise for Education*
PAS con relación vigente	*GSuite Enterprise for Education*
Alumno inscrito en algún grupo de docencia	*GSuite for Education. Próximamente GSuite Enterprise for Education*
Resto de casos (cuentas en carencia, antiguos alumnos, otras relaciones)	*GSuite for Education*

[…]
Ubicación de los datos
Todo el personal docente e investigador y personal de administración y servicios de la Universidad con vinculación vigente como empleado tienen asignada la licencia y aplicada la configuración necesaria para que sus datos de GSuite se ubiquen dentro de la Unión Europea, pudiendo utilizar la mayoría de los servicios de sus cuentas de GSuite para participar en contratos o convocatorias de investigación que requieran ubicación de los datos dentro de la UE.
El detalle de datos y servicios que se ubican en la UE y que por tanto se podrán utilizar en los contratos o proyectos que tengan dicha exigencia está disponible en: ¿A qué datos se aplica una política de región de datos?

El resto de los datos, independientemente de su ubicación, cumplen con la normativa de protección de datos europea (GDPR) tal como explicamos en el epígrafe dedicado a Seguridad y cumplimiento
Seguridad y cumplimiento
Toda la información relativa a seguridad y cumplimiento de normativas legales puede encontrarse en el portal de Confianza y seguridad de Google.
[…]
Acceso a otros servicios
La cuenta de Google proporcionada a todos los usuarios de la UC3M puede permitir el acceso a otros servicios NO incluidos en el acuerdo GSuite for Education, tanto de Google como de terceros.
Al utilizar estos servicios, el usuario acepta a título personal y privado las condiciones de uso de Google y deberá dirigirse directamente al proveedor para cualquier cuestión relativa al servicio.
Teniendo en cuenta la demanda de los usuarios y otras implicaciones organizativas, y tras una evaluación interna, se ha habilitado el acceso por parte de los usuarios a los siguientes servicios no incluidos en GSuite for Edu
Chrome Web Store
Google Analytics
Google Payments (PAS/PDI)
Google Public Data
Google Take Out
Google Voice
Sincronización con Google Chrome
YouTube
[…]"

Con fecha 31 de mayo de 2021, se comprueba el contenido de la url ******URL.13*** *según web.archive.org a fecha 01/08/2020 donde consta entre otros aspectos:*

*"En el año 2013 la Universidad ***UNIVERSIDAD.1firmó el acuerdo que pone a disposición de las universidades el servicio ***SERVICIO.1.*
Fruto de ese acuerdo, la Universidad dispone de acceso a las siguientes herramientas en su versión empresarial de forma totalmente gratuita:
- *Calendario*
- *Contactos*
- *Drive*
- *Gmail*
- *Hangouts*
- *Groups for Business*
- *Sitios web*
- *Cuentas de Google*

[…]
Acceso a otros servicios
La cuenta de Google proporcionada a todos los usuarios de la UC3M puede permitir el acceso a otros servicios no incluidos en el acuerdo GSuite for Education. Al utilizar estos servicios, el usuario acepta a título personal y privado las condiciones de uso y deberá dirigirse directamente a Google para cualquier cuestión relativa al servicio.

*Teniendo en cuenta la demanda de los usuarios y otras implicaciones organizativas, y tras una evaluación interna, se ha habilitado el acceso por parte de los usuarios a los siguientes servicios no incluidos en ***SERVICIO.1*
Chrome Web Store
Google Analytics
Google Payments (PAS/PDI)
Google Public Data
Google Take Out
Google Voice
Tablas dinámicas
Sincronización con Google Chrome
YouTube
[…]"

*Con fecha 7 de junio de 2021 se comprueba el contenido de la url *****URL.14** donde consta entre otros aspectos:*
"
[…]
No se genera ninguna entrada de registro en los siguientes casos:
- Si el personal de Google ha accedido a los datos porque un usuario ha compartido un documento con él.
- SI Google no puede informarte de que ha accedido a los datos por motivos legales.
[…]"

*Con fecha 7 de junio de 2021 se comprueba el contenido de la url *****URL.15** donde consta, en ingles (se ha traducido) entre otros aspectos:*

«El cliente acepta estas condiciones («Customer»), y Google LLC, Google Ireland Limited, Google Asia Pacific Pte. Ltd., o cualquier otra entidad que controle directa o indirectamente, esté controlada por Google LLC (según proceda, «Google»), o esté bajo control común con Google (según proceda, «Google»), hayan celebrado uno o varios acuerdos de Suite G (tal como se definen a continuación) o Acuerdos complementarios sobre productos (tal como se definen a continuación) (cada uno de ellos, modificado periódicamente, un «acuerdo»).
[...]
«Acuerdo de Suite G»: un acuerdo suite G; Un Suite G para la Educación; Un acuerdo maestro de Google Cloud con G. Suite Services Schedule; O cualquier otro acuerdo en virtud del cual Google acepte prestar al cliente cualquiera de los servicios descritos en la sección G Suite Services Summary.
«G Suite Services Summary», la descripción actual de los servicios de la Suite G (incluidas las ediciones correspondientes), tal como figura en https://gsuite.google.com/terms/user_features.html (tal como puede ser actualizado por Google de vez en cuando de conformidad con el acuerdo de la serie G).
[...]
4. Ámbito de aplicación de la Ley de Protección de Datos.
4.1 aplicación del Derecho europeo. Las partes reconocen que la legislación europea de protección de datos se aplicará al tratamiento de datos personales del cliente si, por ejemplo:

A. el tratamiento se lleva a cabo en el contexto de las actividades de un establecimiento de clientes en el territorio del EEE o del Reino Unido; O bien
B. Los datos personales del cliente son datos personales relativos a interesados que se encuentran en el EEE o en el Reino Unido y el tratamiento se refiere a la oferta de bienes o servicios en el EEE o el Reino Unido, o al seguimiento de su comportamiento en el EEE o el Reino Unido.
[...]
5. Tratamiento de datos.
5.1 funciones y cumplimiento de la normativa; Previa.
5.1.1. Responsabilidades del encargado del tratamiento y del responsable del tratamiento. Si la legislación europea de protección de datos se aplica al tratamiento de datos personales del cliente:
A. el objeto y los pormenores del tratamiento se describen en el apéndice 1;
B. Google es el encargado del tratamiento de dichos datos personales del cliente con arreglo a la legislación europea de protección de datos;
C. El cliente es responsable o encargado del tratamiento, según proceda, de dichos datos personales con arreglo a la legislación europea de protección de datos; Y la
[...]
10. Transferencias de datos
10.1 instalaciones de almacenamiento y procesamiento de datos. Google puede almacenar y tratar datos del cliente en cualquier lugar en el que Google o sus subencargados mantengan instalaciones, siempre que:
a. Sección 10.2 (Transferencias de datos) con respecto a las cláusulas tipo de contrato o solución alternativa de transferencia; Y la
B. las condiciones específicas aplicables al servicio (en su caso) con respecto a la ubicación de los datos.
10.2 transferencias de datos. Si el almacenamiento o el tratamiento de datos personales de los clientes implica transferencias de datos personales del cliente desde el EEE, Suiza o el Reino Unido a cualquier tercer país que no garantice un nivel adecuado de protección con arreglo a la legislación europea de protección de datos, y la legislación europea de protección de datos se aplica a dichas transferencias:
A. Si el cliente (como exportador de datos) suscribe las cláusulas contractuales tipo con Google LLC (como importador de datos) en la Console de Admin, entonces:
I. las transferencias estarán sujetas a las cláusulas modelo de contrato; Y la
II. Google garantizará que Google LLC cumpla las obligaciones que le incumben en virtud de las cláusulas contractuales tipo con respecto a dichas transferencias; O
[...]
11. Subencargados
11.1 consentimiento para el encargo del subencargado. El cliente autoriza específicamente el encargo como subencargado de: A) las entidades enumeradas a partir de la fecha efectiva de modificación en la URL especificada en la sección 11.2 (Información sobre los subencargados del tratamiento); Y b) todos los demás socios de Google de vez en cuando. Además, sin perjuicio de lo dispuesto en la sección 11.4 (Oportunidades de objetos sujetos a cambios en el subprocesador), el cliente autoriza en general el compromiso como subprocesador de cualquier otro tercero («Subencargados nuevos terceros»). Si el cliente ha suscrito cláusulas contractuales tipo según lo descrito en la sección 10.2 (Transferencias de datos), las autorizaciones anteriores constituyen el consentimiento previo por escrito del cliente a la subcontratación por parte de Google LLC del tratamiento de datos del cliente.

11.2 información sobre los subprocesadores. La información sobre los subprocesadores, incluidas sus funciones y ubicaciones, está disponible en https://gsuite.google.com/intl/en/terms/subprocessors.html (tal como puede ser actualizado por Google de vez en cuando de conformidad con la presente Enmienda sobre el tratamiento de datos).
11.3 requisitos para el encargo del subprocesador. Al contratar a cualquier subencargado del tratamiento, Google:
A. asegurarse, mediante un contrato escrito, de que:
I. el subencargado solo accede y utiliza los datos del cliente en la medida necesaria para cumplir las obligaciones subcontratadas, y lo hace de conformidad con el Acuerdo (incluida la presente modificación del tratamiento de datos) y el modelo de contrato o solución alternativa de transferencia, según proceda en virtud de la sección 10.2 (Transferencias de datos); Y la
II. Si el RGPD se aplica al tratamiento de datos personales de los clientes, las obligaciones en materia de protección de datos descritas en el artículo 28, apartado 3, del RGPD, tal como se describen en la presente modificación del tratamiento de datos, se imponen al subencargado del tratamiento; Y la
B. seguirá siendo plenamente responsable de todas las obligaciones subcontratadas al subencargado del tratamiento, así como de todos los actos y omisiones de este.
[...]
Apéndice 1: Asunto y detalles del tratamiento de datos
Asunto
Prestación de servicios y TSS por parte de Google al cliente.
Duración del tratamiento
El término aplicable más el período comprendido entre la expiración de dicho plazo y la supresión de todos los datos del cliente por parte de Google de conformidad con la Enmienda sobre el tratamiento de datos.
Naturaleza y finalidad del tratamiento
Google tratará los datos personales de los clientes con el fin de prestar los servicios y la TSS al cliente de conformidad con la Enmienda sobre el tratamiento de datos.
Categorías de datos
Datos relativos a personas facilitados a Google a través de los servicios, por (o bajo la dirección de) clientes o usuarios finales.
Interesados
Los interesados incluyen a las personas sobre las que se facilitan datos a Google a través de los servicios del cliente o usuario final (o bajo la dirección de estos).
Apéndice 2: Medidas de seguridad
A partir de la fecha efectiva de la modificación, Google aplicará y mantendrá las medidas de seguridad descritas en el presente apéndice 2.
1. Centro de Datos y Seguridad de las Redes
a) Centros de datos.
Infraestructuras. Google mantiene centros de datos geográficamente distribuidos. Google almacena todos los datos de producción en centros de datos físicamente seguros.
Redundancia. Los sistemas de infraestructura se han diseñado para eliminar puntos únicos de fallo y minimizar el impacto de los riesgos medioambientales previstos. Los circuitos dobles, los interruptores, las redes u otros dispositivos necesarios contribuyen a esta redundancia. Los servicios están diseñados para permitir a Google realizar determinados tipos de mantenimiento preventivo y correctivo sin interrupción. Todos los equipos e instalaciones ambientales cuentan con procedimientos

documentados de mantenimiento preventivo que detallan el proceso y la frecuencia de las prestaciones de acuerdo con las especificaciones internas o del fabricante. El mantenimiento preventivo y correctivo del equipo del centro de datos está programado a través de un proceso de cambio estándar con arreglo a procedimientos documentados.

Potencia. Los sistemas de energía eléctrica del centro de datos están diseñados para ser redundantes y manejables sin que ello afecte a un funcionamiento continuo, 24 horas al día y 7 días a la semana. En la mayoría de los casos, se proporciona una fuente de energía primaria y una alternativa, cada una de las cuales tiene la misma capacidad, para componentes críticos de infraestructura en el centro de datos. La energía de reserva se suministra mediante diversos mecanismos, como las baterías de fuentes de alimentación ininterrumpidas (SAI), que proporcionan una protección fiable y constante durante los navegadores de servicio, apagones, sobretensión, bajo tensión y condiciones de frecuencia fuera de tolerancia. Si se interrumpe la energía de servicio público, la potencia de reserva está diseñada para suministrar energía transitoria al centro de datos, a plena capacidad, durante un máximo de 10 minutos hasta que los sistemas de generadores diésel se hagan cargo. Los generadores diésel son capaces de encenderse automáticamente en segundos para suministrar suficiente energía eléctrica de emergencia para hacer funcionar el centro de datos a plena capacidad, normalmente durante un período de días.

Sistemas operativos del servidor. Los servidores de Google utilizan una implementación basada en Linux adaptada al entorno de aplicación. Los datos se almacenan utilizando algoritmos privados para aumentar la seguridad y la redundancia de los datos. Google utiliza un proceso de revisión de códigos para aumentar la seguridad del código utilizado para prestar los servicios y mejorar los productos de seguridad en entornos de producción.

Continuidad de las empresas. Google ha diseñado y planificado y probado periódicamente sus programas de planificación de la continuidad de las actividades y de recuperación en caso de catástrofe.

b) Redes y transporte.

Transmisión de datos. Los centros de datos suelen conectarse a través de enlaces privados de alta velocidad para proporcionar una transferencia segura y rápida de datos entre centros de datos. El objetivo es evitar que los datos sean leídos, copiados, alterados o retirados sin autorización durante la transferencia o el transporte electrónicos o cuando se graben en soportes de almacenamiento de datos. Google transfiere datos a través de protocolos estándar de Internet.

Superficie de ataque exterior. Google emplea múltiples capas de dispositivos de red y detección de intrusiones para proteger su superficie de ataque externo. Google considera posibles vectores de ataque e incorpora tecnologías adecuadas integradas con fines en los sistemas exteriores.

Detección de intrusiones. La detección de intrusiones tiene por objeto proporcionar información sobre las actividades de ataque en curso y proporcionar información adecuada para responder a los incidentes. La detección de intrusiones de Google implica:

1. controlar rigurosamente el tamaño y la composición de la superficie de ataque de Google mediante medidas preventivas;

2. utilización de controles de detección inteligentes en los puntos de entrada de datos; Y la

3. utilizar tecnologías que solucionen automáticamente determinadas situaciones peligrosas.

Respuesta a incidentes. Google supervisa una serie de canales de comunicación para incidentes de seguridad, y el personal de seguridad de Google reaccionará rápidamente ante incidentes conocidos.
Tecnologías de cifrado. Google pone a disposición el cifrado HTTPS (también denominado conexión SSL o TLS). Los servidores de Google apoyan el intercambio de claves criptográficas de la curva elíptica efímera Diffie-Hellman firmado con RSA y ECDSA. Estos métodos perfectos de secreto hacia delante (EPA) ayudan a proteger el tráfico y minimizar el impacto de una llave en peligro o de un avance criptográfico.
2. Acceso y controles in situ.
a) Controles in situ.
Operación de seguridad del centro de datos in situ. Los centros de datos de Google mantienen una operación de seguridad in situ responsable de todas las funciones de seguridad del centro de datos físicos 24 horas al día, 7 días a la semana. El personal de la operación de seguridad in situ vigilará las cámaras de circuito cerrado de televisión (TVCC) y todos los sistemas de alarma. El personal de las operaciones de seguridad in situ realiza periódicamente patrullas internas y externas del centro de datos.
Procedimientos de acceso al centro de datos. Google mantiene procedimientos formales de acceso para permitir el acceso físico a los centros de datos. Los centros de datos están alojados en instalaciones que requieren acceso a clave de tarjeta electrónica, con alarmas vinculadas a la operación de seguridad in situ. Todos los participantes en el centro de datos deberán identificarse y demostrar la identidad de las operaciones de seguridad in situ. Solo se permite la entrada en los centros de datos a los empleados, contratistas y visitantes autorizados. Solo los empleados y contratistas autorizados pueden solicitar acceso a estas instalaciones a la clave de la tarjeta electrónica. Las solicitudes de acceso a claves de tarjetas electrónicas al centro de datos deben realizarse por correo electrónico y requieren la aprobación del gestor del solicitante y del director del centro de datos. Todos los demás participantes que necesiten acceso temporal al centro de datos deberán: Obtener previamente la aprobación de los gestores del centro de datos para el centro de datos específico y los ámbitos internos que deseen visitar; Iniciar sesión en las operaciones de seguridad in situ; Y iii) hacer referencia a un registro aprobado de acceso al centro de datos que identifique a la persona aprobada.
Dispositivos de seguridad del centro de datos in situ. Los centros de datos de Google emplean una clave de tarjeta electrónica y un sistema de control del acceso biométrico vinculado a una alarma del sistema. El sistema de control de acceso vigila y registra la clave de tarjeta electrónica de cada persona y cuando accede a puertas perimetrales, envío y recepción, y a otras zonas críticas. La actividad no autorizada y los intentos de acceso fallidos son registrados por el sistema de control de acceso e investigados, según proceda. El acceso autorizado a lo largo de las operaciones comerciales y los centros de datos está restringido en función de las zonas y de las responsabilidades laborales de cada persona. Las puertas contraincendios de los centros de datos están alarmadas. Las cámaras de CCTV funcionan tanto dentro como fuera de los centros de datos. La colocación de las cámaras se ha diseñado para cubrir áreas estratégicas, entre ellas el perímetro, las puertas del edificio del centro de datos y el envío/recepción. El personal de operaciones de seguridad in situ gestiona los equipos de vigilancia, grabación y control de CCTV. Los cables seguros en todos los centros de datos conectan los equipos de CCTV. Las cámaras graban in situ a través de videocámaras digitales 24 horas al día, 7 días a la semana. Los registros de vigilancia se conservan durante un máximo de 30 días en función de la actividad.

b) Control de accesos.
Personal de seguridad de infraestructuras. Google tiene y mantiene una política de seguridad para su personal y requiere formación en materia de seguridad como parte del paquete de formación de su personal. El personal de seguridad de la infraestructura de Google es responsable del seguimiento continuo de la infraestructura de seguridad de Google, la revisión de los servicios y la respuesta a los incidentes de seguridad.
Control de accesos y Gestión Privilege. Los administradores y usuarios finales del cliente deben autenticarse a través de un sistema de autenticación central o mediante un único signo en el sistema para utilizar los servicios.
Procedimientos y políticas de acceso a los datos internos — Política de acceso. Los procesos y políticas de acceso interno a los datos de Google están diseñados para impedir que personas o sistemas no autorizados accedan a los sistemas utilizados para tratar datos personales. Google diseña sus sistemas para: I) solo permiten a las personas autorizadas acceder a los datos a los que están autorizadas; Y ii) garantizar que los datos personales no puedan ser leídos, copiados, alterados o retirados sin autorización durante el tratamiento, la utilización y después del registro. Los sistemas están diseñados para detectar cualquier acceso inadecuado. Google emplea un sistema centralizado de gestión del acceso para controlar el acceso del personal a los servidores de producción y solo proporciona acceso a un número limitado de personal autorizado. Los sistemas de autenticación y autorización de Google utilizan certificados SSH y claves de seguridad, y están diseñados para proporcionar a Google mecanismos de acceso seguros y flexibles. Estos mecanismos están diseñados para conceder únicamente derechos de acceso aprobados a los anfitriones, los registros, los datos y la información sobre la configuración. Google exige el uso de identificadores únicos de usuario, contraseñas fuertes, autenticación de dos factores y listas de acceso cuidadosamente supervisadas para minimizar el potencial de uso no autorizado de cuentas. La concesión o modificación de derechos de acceso se basa en: Las responsabilidades del personal autorizado en el puesto de trabajo; Los requisitos en materia de obligaciones laborales necesarios para llevar a cabo las tareas autorizadas; Y la necesidad de conocer la base. La concesión o modificación de derechos de acceso también debe ser conforme con las políticas internas de acceso a los datos y la formación de Google. Las aprobaciones se gestionan mediante herramientas de flujo de trabajo que mantienen registros de auditoría de todos los cambios. El acceso a los sistemas está registrado para crear una pista de auditoría para la rendición de cuentas. Cuando se utilizan contraseñas para la autenticación (por ejemplo, conectarse a los puestos de trabajo), se aplican políticas de contraseñas que se ajustan, como mínimo, a las prácticas estándar del sector. Estas normas incluyen restricciones a la reutilización de contraseñas y un grado suficiente de contraseña. Para acceder a información extremadamente sensible (por ejemplo, datos de tarjetas de crédito), Google utiliza tokens de hardware.
3. Datos
a) Almacenamiento de datos, aislamiento y registro.
Google almacena datos en un entorno multiarrendatario en servidores propiedad de Google. Sin perjuicio de las instrucciones en contrario del cliente (por ejemplo, en forma de selección de localización de datos), Google reproduce los datos del cliente entre múltiples centros de datos geográficamente dispersos. Google también aísla lógicamente los datos de los clientes y, lógicamente, separa los datos de cada usuario final de los datos de otros usuarios finales, y los datos de un usuario final autenticado

no se mostrarán a otro usuario final (a menos que el antiguo usuario final o un administrador permita compartir los datos).
Se dará al cliente el control de políticas específicas de intercambio de datos. Estas políticas, de acuerdo con la funcionalidad de los servicios, permitirán al cliente determinar los ajustes de reparto de productos aplicables a los usuarios finales para fines específicos. El cliente puede optar por utilizar la función de registro que Google pone a disposición a través de los servicios.
b) Desmantelado Disks and Disk Erase Policy.
Los discos que contienen datos pueden experimentar problemas de rendimiento, errores o fallos de hardware que conducen a su desmantelamiento («disco despedido»). Todos los discos desmantelados están sujetos a una serie de procesos de destrucción de datos («Disk Erase Policy») antes de abandonar los locales de Google para su reutilización o destrucción. Los disquetes desmantelados se eliminan en un proceso en varias fases y son verificados por al menos dos validadores independientes. Los resultados de la supresión se registran mediante el número de serie del disco despedido para su seguimiento. Por último, la disco despedida suprimida se publica para su inventario para su reutilización y redistribución. Si, debido a un fallo del hardware, el disco despedido no puede borrarse, se almacenará de forma segura hasta que pueda destruirse. Cada instalación es objeto de auditorías periódicas para supervisar el cumplimiento de la política de detección de la enfermedad.
4. Personal de seguridad
El personal de Google debe comportarse de conformidad con las directrices de la empresa en materia de confidencialidad, ética empresarial, uso adecuado y normas profesionales. Google lleva a cabo controles de antecedentes razonablemente adecuados en la medida en que sea legalmente admisible y de conformidad con la legislación laboral local y la normativa legal aplicables.
El personal debe ejecutar un acuerdo de confidencialidad y acusar recibo y cumplimiento de las políticas de confidencialidad y privacidad de Google. El personal recibe formación en materia de protección. El personal que manipula los datos del cliente debe completar los requisitos adicionales adecuados a su función (por ejemplo, certificaciones). El personal de Google no tratará los datos de los clientes sin autorización.
5. Seguridad del subprocesador.
Antes de embarcar subencargados, Google lleva a cabo una auditoría de las prácticas de seguridad y privacidad de los subencargados para garantizar que los subencargados ofrezcan un nivel de seguridad y privacidad adecuado a su acceso a los datos y al alcance de los servicios contratados. Una vez que Google haya evaluado los riesgos presentados por el subencargado del tratamiento y, a continuación, con sujeción a los requisitos descritos en la sección 11.3 (Requisitos para el encargo del subencargado) de la presente Enmienda sobre el tratamiento de datos, el subencargado deberá celebrar las condiciones contractuales adecuadas en materia de seguridad, confidencialidad y privacidad.»

Con fecha 7 de junio de 2021 se comprueba el contenido de la url ******URL.16*** *donde consta que la política de región de datos se aplica a datos principales de servicios como Gmail, Drive, Meet, entre otros, siendo estos para Drive "Todo el contenido subido a Drive:el cuerpo de los archivos, el texto, las imágenes y los dibujos insertados y los comentarios asociados de los usuarios" y para Gmail "Asunto, cuerpo, archivos adjuntos, remitentes y destinatarios de mensajes". Para Meet los datos*

principales consta "grabaciones de audio almacenados en Drive (los mensajes de Meet se añaden a Drive si la llamada se graba)". Consta que la política de región de datos también se aplica a índices y a copias de seguridad. Consta que no están incluidos en la política de región de datos "los datos de clientes ni los tipos de datos que no se mencionan explícitamente en este artículo, como los registros o el contenido almacenado en caché".

Con fecha 7 de junio de 2021 se comprueba el contenido de la url ******URL.17*** *donde consta el expediente de contratación XXXXXXXX de la Universidad ***UNIVERSIDAD.1 relativo al "Suministro de licencias GSuite Enterprise for Education y consultoría asociada" con fecha de adjudicación 06/08/2020 y fecha de formalización 28/08/2020. Y donde consta un enlace para descarga del Pliego de Prescripciones Técnicas donde consta que el objeto es el suministro de 2500 licencias Enterprise for Education para trabajadores y de 25000 licencias Enterprise for Education para alumnos.*

*Con fecha 7 de junio de 2021 se comprueba el contenido de diversas actividades del tratamiento de la Universidad ***UNIVERSIDAD.1 donde consta entre otros tratamientos:*

Para uno de los tratamientos:
a. En "denominación del tratamiento" consta "Gestión de Recursos Humanos"
*b. En "responsable" consta "Universidad ***UNIVERSIDAD.1 de Madrid"*
c. En "Fines del tratamiento" consta "La gestión integral de los expedientes administrativos y económicos del personal de la Univerdad".
d. En "Transferencias internacionales" consta "no"
e. En "Categorías de datos" consta entre otros; datos identificativos, datos de contacto, y categorías especiales de datos como datos de salud (bajas por enfermedad, accidentes laborales, grado de discapacidad), datos económicos-financieros, datos de circunstancias familiares, sexo, estado civil, afiliación sindical, datos académicos y profesionales.
f. En "Medidas de seguridad" en el apartado "mp.ei.5 Trabajo con ficheros alojados en el dispositivo" consta "La utilización de dispositivos de almacenamiento locales (discos de equipos de sobremesa, portátiles, discos USB) para almacenamiento de de datos personales no se recomienda, ya que impiden o dificultan la creación de copias de respaldo. Por ello se recomienda la utilización del servicio de Google para la edición de documentos (Google Docs, Sheets, etc)". Asimismo consta "El Servicio de almacenamiento de datos de Google (Google Drive) se encuentra adherido al "Escudo de privacidad/Privacy Shield" que aporta las garantías necesarias para el almacenamiento de datos personales cumpliendo con el Reglamento General de Protección de Datos (RGPD)".

Para otro tratamiento:
a. En "denominación del tratamiento" consta "actuaciones administrativas no presenciales"
*b. En "responsable" consta "Universidad ***UNIVERSIDAD.1 de Madrid"*
c. En el apartado de "Transferencias internacionales" consta "No precisan de autorización. Garantías adecuadas."
d. En el apartado de "Base jurídica" consta "El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes

públicos conferidos al responsable del tratamiento; El tratamiento es necesario para la ejecución deun contrato en el que el interesado es parte opara la aplicación a petición de este de medidas precontractuales; El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;"

e. En el apartado de "Categorías de datos" consta "Datos identificativos: Nombre y apellidos, DNI/CIF/Documento identificativo, dirección correo electrónico. Otros datos propios del tratamiento en particular de que se trate. Otros datos: imagen y voz."

Para otro tratamiento:

a. En "denominación del tratamiento" consta "Movilidad internacional Erasmus"

*b. En "responsable" consta "Universidad ***UNIVERSIDAD.1de Madrid"*

*c. En el apartado de "Transferencias internacionales" consta "Sí. ***PAÍS.2. Marco de Programa Erasmus."*

d. En el apartado de "Base jurídica" consta "El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales; El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;"

e. En el apartado de "Categorías de datos" consta "Nombre y apellidos, DNI, correo electrónico., teléfono y dirección postal. Sexo, nacionalidad, edad, lugar de nacimiento. Necesidades especiales, grado de discapacidad. Datos académicos, área de estudios, Departmento/Servicio de la universidad al que pertenece el beneficiario, Universidad u Organziación &Institución en la que se va a llevar a cabo l amovilidad, becas de movilidad que hayan sido otorgadas previamente el solicitante.". Asimismo, constan datos académicos y bancarios.

Para otro tratamiento:

a. En "denominación del tratamiento" consta "Contacta"

*b. En "responsable" consta "Universidad ***UNIVERSIDAD.1 de Madrid"*

c. En el apartado de "Transferencias internacionales" consta "XXX. Salesforce"

d. En el apartado de "Base jurídica" consta "El interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales; El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;"

e. En el apartado de "Categorías de datos" constan datos identificativos y de contacto, datos académicos, profesionales, grado de discapacidad, sexo, nacionalidad, entre otros.

Para otro tratamiento:

a. En "denominación del tratamiento" consta "Puertas abiertas"

*b. En "responsable" consta "Universidad ***UNIVERSIDAD.1 de Madrid"*

c. En el apartado de "Transferencias internacionales" consta "No precisan de autorización. Privacy Shield."

d. En el apartado de "Base jurídica" consta "El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; El tratamiento es necesario para la

ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales; El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; El interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.(autorización de envío de información)"
e. En el apartado de "Categorías de datos" constan datos identificativos y de contacto, datos académicos, profesionales, imagen y voz.
f. Destinatarios de los datos. Encargados del tratamiento: Blackboard Collaborate.
Para otro tratamiento:
a. En "denominación del tratamiento" consta "Evaluación Académica online"
*b. En "responsable" consta "Universidad ***UNIVERSIDAD.1 de Madrid"*
c. En el apartado de "Transferencias internacionales" consta "No precisan de autorización. Privacy Shield."
d. En el apartado de "Base jurídica" consta "El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales; El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento : Ley orgánica de universidades artículo 2.2f)"
e. En el apartado de "Categorías de datos" constan datos identificativos y de contacto, datos académicos, profesionales, imagen y voz.
f. Destinatarios de los datos. Encargados del tratamiento: Blackboard Collaborate y Google Hangouts Meet, entre otros.

*Con fecha 23 de julio de 2021 se comprueba que la url *****URL 18** redirige a la url *****URL.19** y donde consta entre otros los servicios Gmail, Google Drive, Google Hangouts, Google Meet.*

*Con fecha 23 de julio de 2021 se comprueba que la url *****URL.20** redirige a la url *****URL.21** y donde consta el mismo contenido que el referido anteriormente para la url ***URL.1*

*Con fecha 12 de agosto de 2021, la UNIVERSIDAD ***UNIVERSIDAD.1 remite a esta Agencia la siguiente información y manifestaciones:*

*1. Que utilizan ***SERVICIO.1 cation desde el 22 de febrero de 2013 hasta la actualidad. Que esta vinculación y prestación de servicios gratuita se ha prorrogado tácitamente hasta la actualidad. Que actualmente están en preparación y negociación de la suscripción del nuevo convenio que sustituya el firmado el 22 de febrero de 2013.*
*2. Que ***SERVICIO.1 cation, G.Suite for Edu, GSuite for Education y Google Worspace for Education, Google Worspace for Education Fundamentals son distintos nombres comerciales del mismo producto.*

Aporta copia de contrato firmado en fecha 6 de marzo de 2013 donde consta:

"Acuerdo de Google Apps para Educación

*El presente Acuerdo de Google Apps para Educación (el "Acuerdo") se celebra entre Google Ireland Limited, con sede en Gordon House, Barrow Street, Dublin 4, Irlanda ("Google") y Universidad ***UNIVERSIDAD.1 con domicilio en Calle ***DIRECCIÓN.2 ("Cliente"). El presente Acuerdo rige el acceso y uso de los Servicios por parte del Cliente y entrará en vigor en la Fecha de Entrada en Vigor.*

[…]

Protección de Datos. En las Cláusulas 1.7 a 1.11, los términos "datos personales", "tratamiento', "responsable del fichero" y "encargado del tratamiento" tendrán el significado que se les atribuye en la Directiva. A los fines del presente Contrato y con respecto a los datos personales de los Usuarios, las partes acuerdan que el Cliente será el responsable del fichero y Google el encargado del tratamiento. El Cliente reconoce que ha decidido que los datos personales de los Usuarios sean tratados por Google como parte de los Servicios y en el ámbito de las prestaciones que conforman los mismos, que se describen en las Políticas de Privacidad de Google. En consecuencia, el Cliente instruye en este acto a Google para prestar los Servicios y tratar los datos de carácter personal de los Usuarios de conformidad con las Políticas de Privacidad de Google, comprometiéndose Google a prestar los Servicios y a tratar dichos datos con arreglo a las mismas. Tales Políticas de Privacidad de Google se incorporan por referencia al presente Contrato.

[…]

Sub-contratación. Google podrá proporcionar los datos personales de los Usuarios a sus Sociedades del Grupo (incluyendo Google Inc.) u otras personas físicas o jurídicas de confianza, con el fin de que dichos terceros traten los datos personales como sub-encargados. Google exigirá que dichos terceros acepten tratar los datos personales en cumplimiento con lo dispuesto en el presente Contrato, las Políticas de Privacidad de Google y cualesquiera otras medidas de confidencialidad y seguridad. Al utilizar los Servicios, el Cliente autoriza a Google a subcontratar sus obligaciones en virtud del presente Contrato conforme a lo descrito en el presente párrafo.

[…]

Transferencias. Como consecuencia de la prestación de los Servicios, Google podrá transferir, almacenar y tratar los datos personales de los Usuarios en Estados Unidos (incluyendo por Google Inc.) o cualquier otro país en el existan instalaciones mantenidas por Google o sus Sociedades del Grupo. Google Inc. se ha adherido a los Principios de Puerto Seguro (IJ.S. Safe Harbor Privacy Principles) y se encuentra registrada bajo el Programa de Puerto Seguro del Departamento de Comercio de Estados Unidos (IJ.S. Department of Commerce's Safe Harbor Program). Cuando Google transfiera datos personales de los Usuarios fuera de la Unión Europea y los Estados Unidos, deberá asegurar el cumplimiento por parte de Google Inc. del principio de "Transferencias Ulteriores" (Onward Transfers) de Puerto Seguro. Si en cualquier momento, durante el Plazo de Duración Google Inc. pierde su certificación de Puerto Seguro, el Cliente tendrá derecho a resolver el Contrato de conformidad con Io establecido en la Cláusula IO del presente Contrato. Al utilizar los Servicios, el Cliente autoriza la transferencia, el tratamiento y el almacenamiento de los datos personales de los Usuarios, que se describe en el presente párrafo.

[…]"

3. Que GSuite Enterprise for Education y Google Workspace for Education Plus son distintos nombres comerciales de la licencia de pago que añade funcionalidades adicionales.

4. Que usan GSuite Enterpsise for Education desde el 06/08/2020 hasta la actualidad.

5. Que las herramientas se ofrecen a los usuarios "Personal" (que incluye a personal PAS/PDI y a externos) y a "Alumnos" (que incluye alumnos matriculados y antiguos alumnos). Que dentro de la suite de Google Workspace son, entre otras, las herramientas ofrecidas, Gmail, Drive, Meet.

*6. Que los acuerdos firmados entre la Universidad ***UNIVERSIDAD.1y Google son:*

a. "Adenda sobre Tratamiento de Datos de Google Workspace o contrato de un producto complementario" ubicado en la url ******URL.22.***

b. "Cláusulas contractuales tipo de la UE de Google Workspace" ubicado en la url ****URL.1*

7. Que según las Cláusulas Contractuales tipo de la UE de Google Workspace:

*a. El exportador de datos es la Universidad ***UNIVERSIDAD.1de Madrid*

b. El importador de datos es Google LLC (anteriormente Google Inc.)

Aporta captura de pantalla donde consta la aceptación de la "Adenda sobre Tratamiento de Datos de Google Workspace o contrato de un producto complementario" por ******EMAIL.1*** *en fecha 24 de febrero de 2021 y la aceptación de "Cláusulas contractuales tipo de la UE de Google Workspace" por* ******EMAIL.3*** *en fecha 5 de junio de 2019.*

8. Que la política de región de datos es aplicable a la licencia Google Workspace for Education Plus.

Aporta los "Términos Específicos de los Servicios de Google Workspace" disponible en ******URL.23.***

Aporta captura de pantalla donde consta que está activada la región de dato "Europa".

9. "Todos los datos no explícitamente incluidos en el apartado 1.3 del documento de "Términos Específicos de los Servicios de Google Workspace" indicada en el apartado a) que precede, incluyendo la IP, no están cubiertos por la política de región de datos."

10. Que a las cuentas de empresas externas XXXXXXX no se les aplica la política de región de datos. Que las cuentas XXXXXXX sí se les aplica la política de región de datos.

*11. Que en relación a los accesos remotos desde los ***PAÍS.1 a datos de sus usuarios, solo constan 4 accesos en los últimos 6 meses, según los informes de registro de auditoría de transparencia de acceso. Que esos 4 accesos han sido motivados por una petición de soporte realizada desde la Universidad, bien a instancias de una alumna o bien a instancia de la propia Universidad. Que es cierto que es posible que no aparezca ningún registro si Google no puede informarles legalmente de que se ha abierto una solicitud o proceso de ese tipo.*

Aporta copia de los informes de registro de auditoría.

12. Que a fecha de 3 de agosto de 2021 se encuentran activas un total de 167648 cuentas, entre cuentas personales y no personales, y de todo tipo de personal incluyendo PAS/PDI, externos y antiguos alumnos. Que de estas, las cuentas de tipo XXXXXX son XXX.

13. Que las transferencias internacionales de datos ocurren para los supuestos no comprendidos en el ámbito de la política de regiones de datos.

*14. Que se producen transferencias de datos a ***PAÍS.1 desde el 6 de marzo de 2013, fecha de inicio de la prestación de los servicios.*

*15. Que los tipos de datos transferidos a ***PAÍS.1 son:*

*a. Datos transferidos a iniciativa directa de la Universidad ***UNIVERSIDAD.1 para la prestación de los servicios de la plataforma Google Workspace a sus usuarios; nombre, apellidos, dirección de correo electrónico, el NIA del alumno como parte de la*

propia dirección de correo electrónico e indicación de si el usuario es personal, alumno o antiguo alumno. De forma indirecta se proporcionan datos de si el usuario pertenece a distintos grupos al incluirlo en listas de distribución y colaboración. Estos grupos son "Grupos de Trabajo", "Consejos". "Comisiones", alumnos por campus, centro, titulación, curso y asignatura. Que los datos de nombre, apellidos, correo electrónico y colectivo de pertenencia no están sujetos a la política de región de datos.

b. Datos transferidos por el uso de la plataforma por parte de sus usuarios son los datos de cuyo tratamiento es responsable la Universidad exceptuando los incluidos en el apartado 1.3 de los "Términos Específicos de los Servicios de Google Workspace" y para aquellos usuarios con licencia Google Worspace for Education Plus.

*16. Que los usuarios afectados por las transferencias de datos a ***PAÍS.1 son menos de 166379 usuarios personales con cuenta activa a fecha 3 de agosto de 2021. Que el número de personas físicas afectadas es inferior ya que una misma persona física puede disponer de varias cuentas.*

17. Que para las transferencias de datos se basan en Privacy Shield (hasta julio 2020) y en Cláusulas Contractuales Tipo a las que se refiere el art. 46.2.c RGPD, suscritas el 5 de junio de 2019, junto con medidas adicionales. Asimismo, también se basan en que la transferencia es necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento (art. 49.1.b RGPD) (contrato de matrícula para el caso de los estudiantes o vinculación de empleado con la Universidad para el caso de profesorado y de administración y servicios) en el marco de la prestación del servicio público de la educación superior.

18. Que existe el compromiso de Google para suscribir las nuevas cláusulas contractuales tipo conforme al nuevo modelo aprobado recientemente por el Comité Europeo de Protección de Datos.

19. Que desde Google se ha puesto de manifiesto el compromiso con sus clientes de la UE para la adopción de medidas en orden al cumplimiento del RGPD:

a. Almacenamiento de datos en UE.

b. Medidas específicas de cifrado.

c. Nuevas cláusulas contractuales tipo.

d. Medidas de transparencia para ayudar a la evaluación basada en riesgos de modo que las consultas de los organismos gubernamentales sobre datos de clientes de Enterprise cloud es muy baja, con lo que la probabilidad de que estos datos se vean afectados es muy baja.

e. Adhesión de Google al código de conducta del RGPD.

f. Certificaciones en estándares ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701.

*Que todo ello puede consultarse en *****URL.23.***

20. Que hasta ahora no han identificado disposiciones en la legislación del tercer país que hagan imposible que Google cumpla con las cláusulas contractuales tipo o mantenga un nivel de protección de datos esencialmente equivalente al del Espacio Económico Europeo.

*a. Que el motivo de esta conclusión se recoge en el documento *****URL.24**:*

i. salvaguardas técnicas, entre otras, cifrado de los datos en tránsito y en reposo.

ii. salvaguardas legales como las SCC, procesamiento de datos conforme a las instrucciones del cliente, compromisos de medidas de seguridad con controles de seguridad adicionales, certificaciones de terceros y auditorías de cumplimiento,

iii. Salvaguardas de la organización ante solicitudes gubernamentales de datos.

"se indicará que los datos deben solicitarse al interesado, pero si no obstante el Gobierno requiere los datos, se estudiará la solicitud por personal especializado de

Google para verificar si es legal y proporcionada siguiendo las siguientes pautas: 1) Verificación del respeto por la privacidad y seguridad de los datos que se almacenan con Google. Cuando se recibe una solicitud gubernamental de datos de clientes, el equipo de Google la revisa para asegurarse de que satisfaga los requisitos legales aplicables y las políticas de Google. En términos generales, para que se facilite cualquier dato, la solicitud debe hacerse por escrito, firmada por un funcionario autorizado de la agencia solicitante y emitida bajo una ley apropiada. Si se considera que una solicitud es demasiado amplia, se intentará limitar por Google. 2) Notificación al cliente: Notificaremos al cliente antes de que se divulgue su información, a menos que dicha notificación sea prohibida por la ley o la solicitud implica una emergencia, como una amenaza inminente a la vida. Se notificará con retraso al cliente si se levanta una prohibición legal de notificación previa, como cuando ha expirado un período de prohibición de divulgación por ley o por orden judicial. Esta notificación normalmente va al punto de contacto del cliente de Google Cloud. 3) Consideración de las objeciones del cliente: Google, en la medida en que lo permita la ley y los términos de la solicitud gubernamental, cumplirá con las solicitudes razonables del cliente con respecto a sus esfuerzos para oponerse a una solicitud, como la presentación del cliente una objeción a la divulgación ante el tribunal correspondiente y proporcionar una copia de la objeción a Google. Si Google notifica al cliente de una solicitud legal del gobierno de EE. UU. Y el cliente posteriormente presenta una objeción a la divulgación ante el tribunal y proporciona una copia de la objeción a Google, Google no facilitará los datos en respuesta a la solicitud si la objeción se resuelve a favor del cliente. Otras jurisdicciones pueden tener procedimientos diferentes y se manejan caso por caso.

Además, se incorporan en dicho documento técnico medidas específicas relativas a (EO 12333) y el Título 50 del Código de los Estados Unidos (U.S.C.) S 1881a (FISA 702), los cuales fueron objeto de consideración por el TJUE en su Sentencia de JULIO DE 2020. En particular, se adoptan medidas respecto de los dos programas referidos como Upstream y Downstream.

Respecto a "Section 702 upstream" que autoriza a las autoridades estadounidenses a recopilar datos de viaje a través de la infraestructura "troncal" de Internet controlada por proveedores de servicios de comunicaciones electrónicas en Estados Unidos (por ejemplo, proveedores de telecomunicaciones de EE. UU.). Para la extensión de los datos de los clientes de Google Cloud atraviesa redes sujetas a Upstream 702 recopilación, estos datos están cifrados en tránsito, cómo se ha descrito más arriba.

Respecto a "Section 702 Downstream" que autoriza a las autoridades estadounidenses a obtener datos específicos directamente desde el servicio de comunicación electrónica proveedores, en la medida en que Google LLC pueda recibir solicitudes específicas relacionadas con Google Cloud datos del cliente en Downstream 702, se revisará cuidadosamente cada solicitud de acuerdo con las pautas descritas anteriormente para asegurarse de que la solicitud satisface todos los requisitos legales aplicables y las políticas de Google."

Y añaden a su manifestación en este punto:

b. Certificaciones de terceros como ISO/IEC 27001, 27017, 27018, 27701 o informes de auditoría.

c. Certificado de Cloud Code of Conduct (CoC).

d. Que Google tiene la obligación bajo las cláusulas contractuales tipo de notificarles si no pueden procesar los daros del cliente de acuerdo con sus instrucciones y las cláusulas contractuales tipo o bien si hay un cambio en la legislación que les sea aplicable que probablemente tenga un efecto adverso

sustancial en las garantías y obligaciones previstas por las cláusulas contractuales tipo.

e. Que no han recibido tal notificación de Google.

f. Que hasta ahora han determinado, en función del Informe de Transparencia de Google que la probabilidad de que sus datos se vean afectados en la práctica por FISA 702 es muy bajo.

21. La Universidad considera que está realizando las transferencias internacionales conforme al RGPD y conforme a unas garantías adecuadas.

Con fecha 24/09/2021 se comprueba que:

*1. En la url *****URL.25** consta, en inglés (se ha traducido) lo siguiente:*

"[…]

1. Regiones de datos. Los siguientes términos se aplican únicamente a los servicios de espacio de trabajo de Google y a los datos del cliente descritos en la definición de «datos localizados» de la sección 1.3 (Definiciones) de las presentes condiciones específicas del servicio:

1.1 almacenamiento primario de datos. Si el cliente utiliza una edición dentro del ámbito de aplicación de los servicios, el cliente puede utilizar la Console de Addmin para seleccionar una región de datos para almacenar datos localizados en reposo y Google, de conformidad con la legislación aplicable, almacenará dichos datos localizados en consecuencia («Google Workspace Data Regions Policy»).

1.2 limitación. Para los datos de los clientes que no estén cubiertos por la política de las regiones de datos espaciales de Google, Google puede almacenar cualquier dato del cliente que no esté cubierto por la política de las regiones de datos espaciales de Google en cualquier lugar en el que Google o sus subencargados mantengan instalaciones, sin perjuicio de lo dispuesto en la sección 10.2 (Transferencias de datos) de la Enmienda sobre el tratamiento de datos (si procede).

1.3 definiciones.

«Datos localizados»: solo los siguientes datos primarios dentro de los datos del cliente para el servicio correspondiente:

a) Gmail: La línea de asunto y el cuerpo del correo electrónico, los documentos adjuntos y los remitentes y destinatarios de los mensajes.

b) Calendario de Google: Título y descripción del evento, fecha, hora, invitados, frecuencia y lugares.

c) Google Docs, Google Sheets y Google Slides: Texto de la caja del archivo, imágenes incorporadas y comentarios asociados generados por el usuario final.

D) Google Drive: Contenido original del archivo cargado en Drive.

e) Hangout Chat: Mensajes y documentos adjuntos.

f) Google Vault: Exportaciones de vault.

«Región de datos»: A) los Estados Unidos o b) Europa.

«Edición incluida en el ámbito de aplicación», las siguientes ediciones:

a) G Suite Business

b) Google Workspace Enterprise Plus

c) Google Workspace for Education Standard (Google Workspace for Education Standard)

D) Google Workspace for Education Plus

[...]»

*2. En la url *****URL.26** consta:*

«[...]

Nuestros clientes de Google Workspace (anteriormente G Suite) pueden optar por almacenar sus datos cubiertos en Europa. Además, estamos procediendo a encriptar

un paso más en el espacio de trabajo dando a los clientes el control directo de las claves de cifrado y del servicio de identidad que elijan para acceder a ellas. Con el cifrado desde el lado del cliente, los datos de los clientes son indecibles para Google, mientras que los usuarios pueden seguir aprovechando la colaboración nativa basada en la web de Google, acceder a contenidos en dispositivos móviles y compartir archivos codificados externamente. Esta capacidad está disponible actualmente en la Beta Pública para Google Drive, Docs, fichas y Slides con planes para ampliarla a otros servicios espaciales. Los clientes también pueden beneficiarse de soluciones de terceros que ofrezcan un cifrado de extremo a extremo para Gmail. Con estas soluciones, los clientes pueden conservar llaves en su geolocalización preferida y gestionar el acceso a los contenidos cubiertos.
[...]
Nuevas cláusulas contractuales tipo
La Comisión Europea ha publicado nuevas cláusulas contractuales tipo para ayudar a proteger los datos personales europeos. Google Cloud tiene previsto aplicar las nuevas CCT para ayudar a proteger los datos de nuestros clientes y cumplir los requisitos de la legislación europea en materia de privacidad. Al igual que las CCT anteriores, estas cláusulas pueden utilizarse para facilitar las transferencias legales de datos.
Transparencia para ayudar a su evaluación basada en el riesgo
Las recomendaciones del CEPD introducen un enfoque basado en el riesgo en virtud del cual los exportadores de datos deben evaluar el nivel de riesgo para los derechos fundamentales que supondría en la práctica una determinada transferencia.
Nuestro Informe de Transparencia revela el número de solicitudes de información a los clientes en la nube de empresas realizadas por las fuerzas y cuerpos de seguridad y los organismos públicos. Las cifras históricas muestran que el número de solicitudes relacionadas con la nube empresarial es extremadamente bajo en comparación con nuestra base de clientes Enterprise Cloud. Por ejemplo, nuestro informe muestra que no se produjeron datos de clientes de Google Cloud Platform Enterprise en respuesta a las solicitudes del Gobierno para el último período de referencia. Por lo tanto, la probabilidad de que los datos de información de los clientes en nube se vean afectados por este tipo de solicitudes es baja.
[...]
Responsabilidad
Siempre estamos estudiando maneras de aumentar nuestra rendición de cuentas y nuestro apoyo al cumplimiento para nuestros clientes. Recientemente hemos anunciado nuestra adhesión al Código de Conducta del RGPD de la UE.

3. En la url ******URL.27*** *consta que "Google Cloud (Google Cloud Platform y Google Workspace) ha acreditado su cumplimiento con los requisitos definidos en el ENS para los sistemas de información de categoría alta"*
4. En la url ******URL.28*** *consta "Google Cloud te ofrece recursos de seguridad, auditorías y certificaciones de terceros, documentación y compromisos contractuales líderes del sector para ayudarte en el proceso de cumplimiento. Con el Administrador de informes de cumplimiento puedes acceder en todo momento y de forma sencilla a estos recursos esenciales sobre cumplimiento, sin coste adicional. Entre los recursos clave se incluyen nuestros últimos certificados ISO/IEC, los informes sobre los estándares de cumplimiento y los autodiagnósticos" y constan asimismo los certificados siguientes para el producto Google Workspace:*

a. ISO/IEC 27017:2015. "provides guidelines for information security controls applicable to the provision and use of cloud services."
b. ISO/IEC 27018:2019. "focuses on privacy and security controls for public-cloud service providers that process personally identifiable information (PII)."
c. ISO/IEC 27001:2013 "Information security management system (ISMS), specifies a set of best practices and details the security controls that can help manage information risks."
*5. En la url *****URL.29** consta:*
"Cloud External Key Manager
[…]
Descripción general
Con Cloud EKM, puedes usar las claves que administras dentro de un socio de administración de claves externo compatible para proteger los datos en Google Cloud. Puedes proteger los datos en reposo en servicios de integración de CMEK admitidos o llamando directamente a la API de Cloud Key Management Service.
[…]
En todos los casos, la clave reside en el sistema externo y nunca se envía a Google.
[…]"
*6. En la url *****URL.30** consta, en inglés (se ha traducido):*

"«Avanzar en el control y la visibilidad en la nube
[...]
Gestor de claves externo: Almacenar y gestionar claves de cifrado fuera de Google Cloud
[...]
Google Cloud codifica por defecto los datos de los clientes y ofrece a los clientes múltiples opciones para controlar y gestionar sus claves de cifrado. Hoy nos complace anunciar el próximo nivel de control con nuestro nuevo gestor de claves externo. Pronto a beta, el gestor de claves externo trabaja con Cloud KMS y te permite encriptar datos en BigQuery and Compute Engine con claves de cifrado almacenadas y gestionadas en un sistema de gestión de claves de terceros desplegado fuera de la infraestructura de Google. El gestor de claves externo le permite mantener la separación entre sus datos en reposo y sus claves de encriptación, aprovechando al mismo tiempo el poder de la nube para computar y analizar.
[…]"
*7. En la url *****URL.31** consta en inglés (se ha traducido):*

«Google Workspace ofrece nuevos niveles de colaboración de confianza para un mundo laboral híbrido.
[...]
Refuerzo de la privacidad y la seguridad de los datos con el cifrado desde el lado del cliente
Al poner en marcha el cifrado de Google Workspace Client-side, estamos ayudando a los clientes a reforzar la confidencialidad de sus datos, abordando al mismo tiempo una amplia gama de soberanía de datos y requisitos de cumplimiento. Google Workspace ya utiliza las últimas normas criptográficas para encriptar todos los datos en reposo y en tránsito entre nuestras instalaciones. Estamos dando un paso más dando a los clientes el control directo de las claves de cifrado y del servicio de identidad que elijan para acceder a ellas. Con el cifrado desde el lado del cliente, los datos de los clientes son indecibles para Google, mientras que los usuarios pueden

seguir aprovechando la colaboración nativa basada en la web de Google, acceder a contenidos en dispositivos móviles y compartir archivos codificados externamente. Si se combina con nuestras otras capacidades de cifrado, los clientes pueden añadir nuevos niveles de protección de datos a sus datos de Google Workspace.
El cifrado del cliente es especialmente beneficioso para las organizaciones que almacenan datos sensibles o regulados, como la propiedad intelectual, los historiales médicos o los datos financieros. Puede ayudar a cumplir los requisitos de soberanía de datos y los requisitos de cumplimiento de ITAR, CJIS, TISAX, IRS 1075 y EAR.
[...]
En las próximas semanas se pondrá en marcha una beta para el cifrado del lado del cliente para los clientes de Google Workspace Enterprise Plus y Google Workspace Education Plus. El cifrado del cliente estará inicialmente disponible para Google Drive, Docs, Sheets y Slides, con apoyo para múltiples tipos de archivos, incluidos archivos de oficina, ficheros PDF, etc. Los clientes interesados pueden adherirse ahora a la beta.
Estamos comprometidos con una hoja de ruta que permita el cifrado del lado del cliente en todo el espacio de trabajo de Google, incluidos Gmail, Meet y Calendar. El apoyo a Google Meet está entrando en otoño. ¡Consérvese para más detalles!

Google Cloud acoge con satisfacción las nuevas cláusulas contractuales tipo de la UE para las transferencias transfronterizas de datos y tiene previsto incluir las nuevas CCT en nuestros contratos dentro del plazo definido por la Comisión Europea para cumplir los requisitos de la legislación europea en materia de privacidad.
[...]
En el asunto Schrems II, el TJUE dictaminó que cualquier persona que transfiera (es decir, que exporte) datos personales fuera de la UE a un tercer país (es decir, el país de importación) en virtud de CCT debe evaluar si dicho tercer país ofrece una protección sustancialmente equivalente a la garantizada por el Derecho de la UE para determinar si las CCT pueden garantizar un nivel adecuado de protección en la práctica. En otras palabras, a fin de transferir datos personales basados en CCT, el exportador y el importador de datos deben evaluar si la legislación del tercer país de que se trate ofrece el nivel adecuado de protección que ofrecen las CCT.
Aunque no está claro si, en circunstancias específicas, las CCT garantizarán por sí solas la protección requerida por el Derecho de la UE, el TJUE indicó que las «medidas complementarias», cuando se utilizan con CCT, podrían establecer un nivel de protección adecuado.
Las recomendaciones del CEPD sobre medidas complementarias se ajustan a nuestras prácticas tradicionales y estamos encantados de reafirmar nuestro compromiso de seguir invirtiendo en ámbitos críticos y ayudar a los clientes de Google Cloud a proteger sus datos y a navegar por su viaje de cumplimiento cuando utilicen nuestros servicios y a la luz de las recomendaciones del CEPD.
[...]
Salvaguardias técnicas
Cifrado de los datos en tránsito y en reposo
El cifrado es un elemento importante de la estrategia de seguridad de Google Workspace for Education/Google Workspace, que ayuda a proteger tus correos electrónicos, chats, videoreuniones, archivos y otros datos. En primer lugar, ciframos algunos datos, tal como se describe en nuestra lista blanca de cifrado espacial de Google mientras se almacenan «en reposo» — almacenados en un disco (incluidos los impulsores de estado sólido) o soportes de seguridad. Incluso si un agresor o

alguien con acceso físico obtiene el equipo de almacenamiento que contiene tus datos, no podrá leerlos porque no dispone de las claves de cifrado necesarias. En segundo lugar, ciframos todos los datos de los clientes mientras están «en tránsito», pasando por Internet y por la red de Google entre centros de datos. Si un agresor intercepta estas transmisiones, solo podrán capturar datos cifrados. Examinaremos detalladamente cómo ciframos a continuación los datos almacenados en reposo y los datos en tránsito.

[...]

1. Cifrado en una parte del cliente

Estamos procediendo a encriptar un paso más en el espacio de trabajo dando a los clientes el control directo de las claves de cifrado y del servicio de identidad que elijan para acceder a ellas. Con el cifrado del cliente, los datos de los clientes son indecibles para Google, mientras que los usuarios pueden seguir aprovechando la colaboración nativa basada en la nube de Google, acceder a contenidos en dispositivos móviles y compartir archivos codificados externamente.

Esta capacidad está disponible actualmente en la Beta Pública para Google Drive, Docs, fichas y Slides con planes para ampliarla a otros servicios espaciales. Los clientes también pueden beneficiarse de soluciones de terceros que ofrezcan un cifrado de extremo a extremo por parte del cliente para Gmail.

[...]

Garantías jurídicas.

Las condiciones de protección de datos de Google Cloud ofrecen una sólida protección jurídica:

Nuevas CCT.

La Comisión Europea ha publicado nuevas cláusulas contractuales tipo para ayudar a proteger los datos personales europeos. Google Cloud tiene previsto aplicar las nuevas CCT dentro del plazo definido por la Comisión de la UE para ayudar a proteger los datos de nuestros clientes y cumplir los requisitos de la legislación europea en materia de privacidad. Al igual que las CCT anteriores, estas cláusulas pueden utilizarse para facilitar las transferencias legales de datos.

El CCSC se aplica automáticamente.

El CCSC se aplica ahora automáticamente, mientras no exista una solución alternativa de transferencia, a todos los clientes de Google Workspace for Education/Google Workspace que estén sujetos a los requisitos de transferencia de datos de la UE.

Tratamiento de acuerdo con las instrucciones.

Google se compromete a tratar los datos de los clientes siguiendo las instrucciones del cliente y de conformidad con nuestras obligaciones en virtud de la legislación aplicable.

Compromisos en materia de seguridad.

Google se compromete a aplicar y mantener medidas técnicas y organizativas que proporcionen un determinado nivel de seguridad aprobado por el cliente. Google garantiza que estas medidas incluyan medidas para encriptar datos personales; Contribuir a garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de Google; Ayudar a restablecer el acceso oportuno a los datos personales tras un incidente; Y para la comprobación periódica de la eficacia. Google también se compromete a notificar a los clientes cualquier incidente de datos sin demora indebida.

Controles de seguridad adicionales.

Google supera los requisitos del RGPD al comprometerse a ofrecer controles de seguridad adicionales que los clientes pueden utilizar a medida que determinen. Estos

controles incluyen una consola de admin, capacidades de cifrado, capacidades de registro y seguimiento, gestión de identidad y acceso, escaneado de seguridad y cortafuegos. Para más detalles, véase la sección «Garantías técnicas» de esta lista blanca.
Certificaciones e informes de auditoría.
Google también supera los requisitos del RGPD al comprometerse a mantener varias certificaciones rigurosas de terceros, así como informes de auditoría de terceros onerosos. Para más detalles, véase a continuación la sección «Certificaciones de terceros y ofertas de cumplimiento».
Salvaguardias organizativas
Solicitudes de datos del Gobierno
Las recomendaciones del CEPD introducen un enfoque basado en el riesgo en virtud del cual los exportadores de datos deben evaluar el nivel de riesgo para los derechos fundamentales que supondría en la práctica una determinada transferencia. Nuestro Informe de Transparencia revela el número de solicitudes de información a los clientes en la nube de empresas realizadas por las fuerzas y cuerpos de seguridad y los organismos públicos. Las cifras históricas muestran que el número de solicitudes relacionadas con la nube empresarial es extremadamente bajo en comparación con nuestra base de clientes Enterprise Cloud, lo que demuestra que la probabilidad de que estos tipos de solicitudes afecten a la información de los clientes en nube es baja. Por ejemplo, nuestro informe muestra que no se produjeron datos de clientes de Google Cloud Platform Enterprise en respuesta a las solicitudes del Gobierno para el último período de referencia. También trabajamos intensamente para ayudar a nuestros clientes a llevar a cabo una evaluación significativa ofreciendo una comprensión clara y detallada de nuestro proceso para responder a las solicitudes gubernamentales de datos de clientes en nube en raras ocasiones. Este proceso puede resumirse como sigue: Si un gobierno busca datos de clientes en el curso de una investigación, Google normalmente informará al Gobierno de que debe solicitar los datos directamente al cliente en cuestión. Si, no obstante, el Gobierno obliga a Google a responder a una solicitud de datos de clientes, un equipo específico de abogados de Google y personal especialmente formado Will revisará cuidadosamente la solicitud para verificar que es legal y proporcionada, siguiendo estas directrices:
Respeto de la privacidad y la seguridad de los datos que almacena en Google
Cuando recibimos una solicitud gubernamental de datos de clientes, nuestro equipo la revisa para asegurarse de que cumple los requisitos legales aplicables y las políticas de Google. En términos generales, para que podamos aportar cualquier dato, la solicitud debe hacerse por escrito, firmada por un funcionario autorizado del organismo solicitante y emitida con arreglo a la legislación pertinente. Si creemos que una solicitud es demasiado amplia, intentaremos reducirla.
Notificación al cliente
Notificaremos al cliente antes de que se revele cualquiera de sus informaciones, a menos que dicha notificación esté prohibida por la ley o que la solicitud implique una emergencia, como una amenaza inminente para la vida. Notificaremos tardíamente a los clientes si se levanta la prohibición legal de notificación previa, por ejemplo cuando haya expirado un plazo legal o judicial de prohibición de revelar información. Esta notificación suele dirigirse al punto de contacto del cliente Google Cloud.
Consideración de las objeciones de los clientes
Google, en la medida en que lo permita la ley y los términos de la solicitud del Gobierno, atenderá las solicitudes razonables de un cliente en relación con sus esfuerzos por oponerse a una solicitud, como el cliente que formula una objeción a la

divulgación ante el órgano jurisdiccional pertinente y facilitará una copia de la oposición a Google. Si Google notifica al cliente una solicitud legal del Gobierno de los Estados Unidos y posteriormente el cliente presenta una objeción a la divulgación ante el tribunal y facilita una copia de la oposición a Google, Google no facilitará los datos en respuesta a la solicitud si la oposición se resuelve en favor del cliente. Otras jurisdicciones pueden tener procedimientos diferentes y se tratan caso por caso.

También reconocemos que la Decisión Schrems II ha generado incertidumbre sobre el impacto de la legislación estadounidense en las transferencias de datos y sobre el papel de Google LLC, una empresa estadounidense, como importador de datos en el marco de las CCT que entró con los clientes de Google Cloud. Muchos clientes tienen dudas sobre la clasificación de Google Cloud y nuestros servicios con arreglo a la legislación estadounidense, así como cuestiones específicas en torno a (EO 12333) y título 50 del United States Code (U.S.C.) § 1881.a (FISA 702), ambas examinadas por el TJUE. Para abordar estas cuestiones, a continuación presentamos información específica sobre esas leyes y su aplicación a los productos de Google Cloud.

Las actividades específicas de inteligencia realizadas en virtud del EO 12333 están sujetas a procedimientos de ejecución más específicos (que pueden clasificarse) que incluyen salvaguardias y protecciones adecuadas a ese tipo de actividad de inteligencia. El EO 12333 regula principalmente las actividades de inteligencia que tienen lugar fuera de los Estados Unidos. Se entiende que el EO 12333 permite a los EE.UU. llevar a cabo una vigilancia electrónica fuera de los EE.UU. de conformidad con los requisitos legales estadounidenses; No autoriza la vigilancia electrónica en los Estados Unidos ni impone requisitos a los proveedores de servicios dentro o fuera de los Estados Unidos.

El artículo 702 es una disposición de la Ley de Enmiendas de la FISA de 2008 (FAA) que permite al Gobierno de los EE.UU. llevar a cabo una vigilancia específica de las personas extranjeras ubicadas fuera de los Estados Unidos, con la asistencia obligatoria de «proveedores de servicios de comunicaciones electrónicas» (según lo definido en el título 50, artículo 1881, letra b), del CEU (4). Dos programas autorizados en virtud de la sección 702 de la FAA se denominan «upstream» y «Downstream». La sección 702, «Upstream», autoriza a las autoridades estadounidenses a recoger datos que circulen por una infraestructura «troncal» de Internet controlada por proveedores de servicios de comunicaciones electrónicas en los EE. UU. (por ejemplo, proveedores de telecomunicaciones estadounidenses). En la medida en que los datos de los clientes de Google Cloud trazan redes sujetas a la recopilación Upstream 702, dichos datos están cifrados en tránsito, como se ha descrito anteriormente.

La sección 702 Downstream autoriza a las autoridades estadounidenses a obtener datos específicos directamente de los proveedores de servicios de comunicaciones electrónicas. En la medida en que Google LLC puede recibir solicitudes específicas relacionadas con los datos de clientes de Google Cloud en el marco de Downstream 702, examinamos cuidadosamente cada solicitud de conformidad con las directrices descritas anteriormente para asegurarse de que la solicitud cumple todos los requisitos legales aplicables y las políticas de Google.

Para saber más sobre cómo tramitamos las solicitudes de datos del Gobierno, consulte nuestra lista blanca (solicitudes gubernamentales de datos de clientes: Control del acceso a sus datos en Google Cloud), nuestra página política (policies.google.com/terms/ disclosures request), y nuestro Informe de transparencia actualizado periódicamente(https://transparencyreport. google.com/user-data/us-national-security?hl=en), que fue el primer informe de este tipo que publicó un proveedor de servicios en nube.

*9. En la url *****URL.32** consta un documento con título "How Google Workspace uses encryption to protect your data" donde consta en inglés (se ha traducido) que:*
"[…]
Cifrado de los datos almacenados en reposo.
[...]
Este cifrado se produce sin que el cliente tenga que tomar ninguna medida.
[...]
Cifrado de los datos en tránsito.
[...]
[..] ciframos el tráfico entre su navegador y nuestros centros de datos [...]
[...]
Gestionamos una red privada altamente segura y resiliente que rodea el mundo y conecta nuestros centros de datos entre sí, garantizando la seguridad de sus datos [...].
[...]
Encriptado del cliente de Google Workspace.
[...]
No hay acceso al contenido de texto claro: El contenido de archivo se encripta en el navegador antes de enviarlo a los servidores de Google para su almacenamiento. Google no puede acceder unilateralmente a los contenidos. Por ejemplo, si Google necesita acceder a un archivo descifrado por motivos de apoyo, requiere una autorización explícita del cliente por expediente.
Soberanía de los clientes sobre las claves de cifrado: Para utilizar el CSE, los clientes necesitan crear de forma independiente su servicio de acceso clave de cifrado utilizando uno de los socios que han construido sus servicios con arreglo a las especificaciones del CSE.
[...]
Es importante señalar que el CSE se centra en el contenido de archivo para esta capa adicional de cifrado. La mayoría de los metadatos, incluidos los nombres de los archivos, las etiquetas y la lista de control de acceso, siguen estando a disposición de Google para gestionar el servicio.
[...]
Google Workspace CSE está diseñada para trabajar para navegadores y aplicaciones móviles mediante el cifrado y descifrado contenidos en los dispositivos del usuario final.
[...]»

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

II

El artículo 45 del RGPD establece lo siguiente:

"1. Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica.

2. Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos: a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos; b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

3. La Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2 del presente artículo. El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. El acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control a que se refiere el apartado 2, letra b), del presente artículo. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

4. La Comisión supervisará de manera continuada los acontecimientos en países terceros y organizaciones internacionales que puedan afectar a la efectiva aplicación de las decisiones adoptadas con arreglo al apartado 3 del presente artículo y de las decisiones adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE.

5. Cuando la información disponible, en particular tras la revisión a que se refiere el apartado 3 del presente artículo, muestre que un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado a tenor del apartado 2 del presente artículo, la Comisión, mediante actos de ejecución, derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión a que se refiere el apartado 3 del presente artículo. Dichos actos de ejecución se adoptarán de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2. Por razones imperiosas de urgencia debidamente justificadas, la Comisión adoptará actos de ejecución inmediatamente aplicables de conformidad con el procedimiento a que se refiere el artículo 93, apartado 3.

6. La Comisión entablará consultas con el tercer país u organización internacional con vistas a poner remedio a la situación que dé lugar a la decisión adoptada de conformidad con el apartado 5.

7. Toda decisión de conformidad con el apartado 5 del presente artículo se entenderá sin perjuicio de las transferencias de datos personales al tercer país, a un territorio o uno o varios sectores específicos de ese tercer país, o a la organización internacional de que se trate en virtud de los artículos 46 a 49.

8. La Comisión publicará en el Diario Oficial de la Unión Europea y en su página web una lista de terceros países, territorios y sectores específicos en un tercer país, y organizaciones internacionales respecto de los cuales haya decidido que se garantiza, o ya no, un nivel de protección adecuado.

9. Las decisiones adoptadas por la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas por una decisión de la Comisión adoptada de conformidad con los apartados 3 o 5 del presente artículo."

El artículo 46 establece la posibilidad de transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas. El artículo siguiente regula las normas corporativas vinculantes y el artículo 49 establece las excepciones en las que se pueden transferir datos personales si se dan unas circunstancias específicas.

En la numerosa documentación aportada por la parte reclamada, se comprueba que tras la sentencia Schrems II la parte reclamada ha procedido a realizar actuaciones tendentes a reforzar las garantías adecuadas en los tratamientos efectuados y, en particular, los que supongan transferencias internacionales de datos; entre otras, se han encriptado los datos de los clientes. En el año 2020, la parte reclamada ha contratado el almacenamiento de datos en reposo en Europa, además de estar revisando las cláusulas contractuales tipo siguiendo las recomendaciones del EDPB.

De acuerdo con lo indicado en el apartado de Hechos y con la información de la que se dispone en este momento, no se tienen evidencias que acrediten el incumplimiento en lo referido a las transferencias internacionales.

III

Tras la amplísima respuesta facilitada por la entidad reclamada por el ahora recurrente, se constata que tras la Sentencia Schrems II, la mencionada entidad ha tomado medidas para que las transferencias internacionales que se pudiesen producir cumplan lo establecido por el RGPD.

Vistos los preceptos citados y demás de general aplicación,

La Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: DESESTIMAR el recurso de reposición interpuesto por Don ***A.A.A.*** contra la resolución de esta Agencia dictada con fecha 24 de noviembre de 2021, en el expediente de actuaciones previas de inspección E/10350/2020.

SEGUNDO: NOTIFICAR la presente resolución a Don ***A.A.A.***.

De conformidad con lo establecido en el artículo 50 de la LOPDPGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDPGDD, y de acuerdo con lo establecido en el artículo 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), los interesados podrán interponer recurso contencioso-administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada LPACAP. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

181-100820

Mar España Martí
Directora de la Agencia Española de Protección de Datos