

0050/2023

La consulta plantea la adecuación a la normativa de protección de datos de carácter personal -el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD en lo sucesivo), y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD en lo sucesivo)- del Acuerdo-Convenio que el Instituto Nacional de Tecnológicas Innovativas y Formación al Profesorado (INTEF en lo sucesivo) va a suscribir con la entidad Google Cloud EMEA Limited (Google en lo sucesivo) para que por parte de la Administración Educativa de las que es competente el Ministerio de Educación y Formación Profesional (las Ciudades Autónomas de Ceuta y Melilla) se implemente en las aulas el uso de la “Solución tecnológica Workspace for Education”.

La consultante plantea varias dudas sobre la adecuación de dicha Acuerdo-Convenio al marco jurídico actual de protección de datos, concretándose en las siguientes:

- Sobre el régimen jurídico aplicable al acuerdo. Existen varios documentos que resultarían de aplicación, como son el propio texto del Convenio, la Adenda de Protección de Datos y los Términos de Workspace. Se establecen unas reglas de prelación en caso de conflicto que pueden dificultar la interpretación de la relación jurídica, a lo que se añade la posibilidad de modificar términos contractuales de manera unilateral, es decir, sin la intervención de INTEF, lo que resultaría contrario al artículo 1256 del Código Civil.

Asimismo, se asume la aplicación de regulación no europea, si así se desprende de la aplicación de la Adenda de Protección de Datos.

- Sobre el objeto del acuerdo-convenio. Al consistir en el despliegue de un *paquete de herramientas diseñado para permitir que los educadores y los alumnos innoven y aprendan juntos*, las categorías de interesados serían muy amplias, como también lo serían las categorías de datos personales ya que

Jurídico

abarcarían datos identificativos (nombre, apellidos, correo electrónico, DNI, usuario y contraseña); centro educativo; datos académicos. Se incluirían, por tanto, datos de menores y datos necesarios para adaptaciones en el aula acordadas con distintas discapacidades; así como datos relativos a los menús escolares que podrían revelar de forma indirecta creencias religiosas.

Al ser un paquete de herramientas y proporcionar servicios adicionales no se pueden enumerar las finalidades concretas y las bases legitimadoras de las mismas, ni tampoco las categorías de datos personales que pudieran incluir, según lo indicado, categorías especiales.

- Sobre la necesidad del uso de la “Solución Tecnológica Workspace for Education”. No existe la necesidad de la contratación porque no aporta ninguna funcionalidad que no se provea desde la plataforma SED -Servicio Educativo Digital- *que tiene la misma finalidad y ninguno de los inconvenientes señalados. (sic)*

No supera el juicio de proporcionalidad (idoneidad, necesidad y proporcionalidad en sentido estricto). El uso de plataformas tecnológicas puede garantizar la prestación de servicios a los centros de manera global; sin embargo, no resulta necesario por la existencia del SED, y en cuanto a la proporcionalidad en sentido estricto, la implantación de la solución tecnológica de Google puede causar perjuicios sobre los datos personales de los menores de edad.

- El uso de diferentes servicios de la solución tecnológica. Se citan los servicios “ordinarios” y los servicios adicionales o “productos adicionales”, y respecto de éstos últimos no resulta claro si se les aplicarían las cláusulas del convenio, a pesar de que su utilización implica la recogida de datos personales.

- Los plazos para comunicar los incidentes de seguridad, que pueden ser superiores a 72 horas. No existe un compromiso en la adenda de protección de datos para notificar al cliente (es decir Google como encargado a INTEF como responsable) en dicho plazo.

- Las transferencias internacionales de datos que se contemplan en la cláusula 10 evidencian que se pueden realizar a cualquier país en el que Google o sus subencargados tengan instalaciones.

- En países del entorno europeo como Francia y Dinamarca se ha prohibido el uso de la solución tecnológica que ofrece Google.

I

Planteados los términos de la consulta, y teniendo en cuenta que la aplicación del Convenio objeto de análisis supondría el tratamiento de datos personales, resultará de aplicación el RGPD y la LOPDGDD.

El tratamiento de datos personales que se deriva de la implementación de Google Workspace en los Centros Educativos se ha de someter a los principios contenidos en el artículo 5 del RGPD, a cuyo tenor los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

Y en su apartado 2, se recoge el principio de responsabilidad proactiva:

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo

II

El principio de licitud es aquel que determina en qué supuestos o bajo qué condiciones un tratamiento de datos personales debe considerarse lícito. Así, los supuestos o bases jurídicas que legitiman el tratamiento de datos personales se encuentran en el artículo 6 del RGPD a cuyo tenor:

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) 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;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) 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;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

En el presente caso se hace necesario identificar cuál sería el supuesto de legitimación para llevar a cabo la implementación de aquellas soluciones tecnológicas que, implicando el tratamiento de datos personales en un entorno digital, coadyuven a ejercer la función educativa de la administración competente. Para ello hay que acudir al régimen jurídico que regula la educación, teniendo en cuenta que es un derecho fundamental previsto en el artículo 27 de la Constitución Española (CE) y en especial habrá que abordar la regulación del uso de las Tecnologías de la información y comunicación y las plataformas digitales.

La Ley Orgánica 2/2006, de 3 de mayo, de Educación (LOE en lo sucesivo) establece en su artículo 2.1 l) que:

El sistema educativo español se orientará a la consecución de los siguientes fines:

l) La capacitación para garantizar la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso seguro de los medios digitales y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente, con el respeto y la garantía de la intimidad individual y colectiva

Asimismo, en cuanto al uso de las Tecnologías de la Información y Comunicación, el artículo 111 bis LOE indica lo siguiente:

1 (...)

En el marco de la implantación de las citadas medidas, dentro de los sistemas de información propios de la gestión académica y administrativa se regulará un número identificativo para cada alumno o alumna, a fin de facilitar el intercambio de la información relevante, el seguimiento de las trayectorias educativas individualizadas, incluyendo

*las medidas educativas que en su caso se hubieran podido aplicar, y atender demandas de la estadística estatal e internacional y de las estrategias europeas para los sistemas de educación y formación. En cualquier caso, **dicha regulación atenderá a la normativa relativa a la privacidad y protección de datos personales.***

*2. Los entornos virtuales de aprendizaje que se empleen en los centros docentes sostenidos con fondos públicos facilitarán la aplicación de planes educativos específicos diseñados por los docentes para la consecución de objetivos concretos del currículo, y deberán contribuir a la extensión del concepto de aula en el tiempo y en el espacio. Por ello deberán, respetando los estándares de interoperabilidad, permitir a los alumnos y alumnas el acceso, desde cualquier sitio y en cualquier momento, a los entornos de aprendizaje disponibles en los centros docentes en los que estudien, con **pleno respeto a lo dispuesto en la normativa aplicable en materia de propiedad intelectual, privacidad y protección de datos personales.** Así mismo promoverán los principios de accesibilidad universal y diseño para todas las personas, tanto en formatos y contenidos como en herramientas y entornos virtuales de aprendizaje.*

3. El Ministerio de Educación y Formación Profesional impulsará, previa consulta a las Comunidades Autónomas, la compatibilidad de los formatos que puedan ser soportados por las herramientas y entornos virtuales de aprendizaje en el ámbito de los contenidos educativos digitales públicos, con el objeto de facilitar su uso con independencia de la plataforma tecnológica en la que se alberguen.

*4. El Ministerio de Educación, Cultura y Deporte **ofrecerá plataformas digitales y tecnológicas** de acceso a toda la comunidad educativa, que podrán incorporar recursos didácticos aportados por las Administraciones educativas **y otros agentes** para su uso compartido. Los recursos deberán ser seleccionados de acuerdo con parámetros de calidad metodológica, adopción de estándares abiertos y disponibilidad de fuentes que faciliten su difusión, adaptación, reutilización y redistribución y serán reconocidos como tales.*

*5. Las Administraciones educativas y los equipos directivos de los centros **promoverán el uso de las tecnologías de la información y la comunicación (TIC) en el aula como medio didáctico** apropiado y*

valioso para llevar a cabo las tareas de enseñanza y aprendizaje. Las Administraciones educativas deberán establecer las condiciones que hagan posible la eliminación en el ámbito escolar de las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red. Se fomentará la confianza y seguridad en el uso de las tecnologías prestando especial atención a la desaparición de estereotipos de género que dificultan la adquisición de competencias digitales en condiciones de igualdad.

(...)

En todo caso, las tecnologías de la información y la comunicación (TIC) y los recursos didácticos que se empleen, se ajustarán a la normativa reguladora de los servicios y sociedad de la información y de los derechos de propiedad intelectual, concienciando en el respeto de los derechos de terceros.

Teniendo en cuenta los preceptos que se acaban de citar, se puede afirmar que, con carácter general, la base jurídica para llevar a cabo el tratamiento de los datos personales de los miembros de la comunidad educativa que se vean afectados por la implementación de soluciones tecnológicas y plataformas digitales se encontraría en el artículo 6.1 c) RGPD, según el cual *el tratamiento es necesario para cumplir una obligación legal aplicable al responsable del tratamiento*. En este caso, resultan de especial relevancia los términos que aparecen en el artículo de la LOE tales como *facilitarán, deberán, impulsará*, de los que se deduce una clara obligación de hacer (Informe 74/2019).

Dicho tratamiento también podría entenderse basado en el artículo 6.1 e) RGPD, según el cual el tratamiento es lícito *cuando sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento*, por cuanto la educación es de un indudable interés público, descansa en un derecho fundamental ex artículo 27 de la CE y corresponde a los poderes públicos competentes su garantía y promoción.

III

Ahora bien, que exista base jurídica de legitimación para que los centros docentes traten datos de carácter personal de la comunidad educativa en, o a través de, entornos y plataformas digitales no significa que pueda llevarse a cabo de cualquier modo, sino que encontramos en distintos cuerpos normativos elementos o requisitos que operan como contrapeso y garantías frente a la posible injerencia que dichos tratamientos de datos suponen en el derecho a la protección de datos y en la privacidad de las personas.

Estas garantías cobran especial relevancia en el presente caso, por cuanto estamos ante una solución tecnológica cuya puesta en marcha e implementación supondría el tratamiento de datos personales de muy diversa índole que hacen referencia a menores de edad en un entorno digital a través de plataformas colaborativas y servicios de redes sociales. Ello puede incluir incluso datos relativos al “*origen y ambiente familiar y social, a características o condiciones personales*”, etc. como ahora a continuación mencionaremos.

En efecto, tanto en la LOE como en la propia LOPDGDD se establecen garantías y salvaguardas que se han de observar cuando estemos ante el tratamiento de datos personales, ya sea con carácter general, ya sea en el uso de entornos y plataformas digitales.

Respecto de este último, ya en el propio artículo 111 bis antes transcrito se hace referencia al pleno respeto a lo dispuesto en la normativa aplicable en materia de “privacidad y protección de datos personales”.

También hay que citar lo indicado en la Disposición adicional vigesimotercera que bajo la denominación “Datos personales de los alumnos” establece un mandato dirigido expresamente a los centros docentes:

*1. Los centros docentes **podrán recabar los datos personales de su alumnado que sean necesarios para el ejercicio de su función educativa.** Dichos datos podrán hacer referencia al origen y ambiente familiar y social, a características o condiciones personales, al desarrollo y resultados de su escolarización, así como a aquellas otras circunstancias cuyo conocimiento sea necesario para la educación y orientación de los alumnos.*

*2. Los padres o tutores y los propios alumnos deberán colaborar en la obtención de la información a la que hace referencia este artículo. La incorporación de un alumno a un centro docente supondrá el **tratamiento de sus datos** y, en su caso, la cesión de datos procedentes*

del centro en el que hubiera estado escolarizado con anterioridad, en los términos establecidos en la legislación sobre protección de datos. En todo caso, la información a la que se refiere este apartado será la estrictamente necesaria para la función docente y orientadora, no pudiendo tratarse con fines diferentes del educativo sin consentimiento expreso.

*3. En el tratamiento de los datos del alumnado se aplicarán normas técnicas y organizativas que garanticen su seguridad y confidencialidad. El profesorado y el resto del personal que, en el ejercicio de sus funciones, acceda a datos personales y familiares o que afecten al honor e intimidad de los menores o sus familias quedará sujeto al **deber de sigilo**.*

*4. **La cesión de los datos, incluidos los de carácter reservado, necesarios para el sistema educativo, se realizará preferentemente por vía telemática y estará sujeta a la legislación en materia de protección de datos de carácter personal.** (...)*

Por su parte, respecto de la LOPDGDD destaca en primer lugar lo dispuesto en el artículo 83, que bajo la denominación de “Derecho a la educación Digital” dispone lo siguiente:

1. El sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un consumo responsable y un uso crítico y seguro de los medios digitales y respetuoso con la dignidad humana, la justicia social y la sostenibilidad medioambiental, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales. (...)

***Las Administraciones educativas deberán incluir en el desarrollo del currículo la competencia digital** a la que se refiere el apartado anterior, así como los elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red.*

En segundo lugar, el mandato del artículo 92, que bajo la rúbrica “Protección de datos de los menores en Internet” cita expresamente a los centros docentes:

*Los **centros educativos** y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad*

*garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente **el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información.***

*Cuando dicha publicación o difusión fuera a tener lugar a través de servicios de redes sociales o servicios equivalentes deberán contar con el **consentimiento** del menor o sus representantes legales, conforme a lo prescrito en el artículo 7 de esta ley orgánica.*

En el presente caso también hay que tener en cuenta lo indicado en el artículo 8 del RGPD por cuanto se pretende someter a tratamiento los datos personales de los menores en un contexto de servicios de la sociedad de la información. Nos indica el citado precepto lo siguiente:

1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó. Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

(...)

El legislador nacional, al amparo de la habilitación que a la que se refiere el apartado 1 del citado artículo 8 del RGPD, estableció lo siguiente en el artículo 7 de la LOPDGDD bajo la denominación “Consentimiento de los menores de edad”.

2. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.

Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

2. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

IV

A todas estas consideraciones debe añadirse la regulación “general” del RGPD y de la LOPDGDD en cuanto al mandato dirigido al responsable del tratamiento de modo expreso en el artículo 24.1:

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

Y también recordar lo dispuesto en el artículo 32 del RGPD, que dispone que:

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

- a) la seudonimización y el cifrado de datos personales;*
- b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
- c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;*

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

(...)

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

Por su parte, el artículo 35 del RGPD dispone lo siguiente:

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

(...)

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

(...)

7. La evaluación deberá incluir como mínimo:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

(...)

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

De acuerdo con lo expuesto, no podemos olvidar que estamos en un contexto de herramientas digitales que sirven a la función educativa, con la consecuencia de tratar datos personales a gran escala de colectivos especialmente vulnerables, y que, en ocasiones, esos tratamientos pueden incluir categorías especiales de datos, por lo que se identifican multitud de elementos que hacen obligatoria la evaluación de impacto.

Finalmente, resulta esencial para el caso que nos ocupa destacar lo indicado en el artículo 28 apartado 2 de la LOPDGDD, que muestra los elementos que

tanto el responsable como el encargado del tratamiento deben tener en cuenta a la hora de aplicar lo indicado en los artículos 24 y 32 del RGPD parcialmente transcritos. En concreto, dicho precepto indica que:

2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.

d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

(...)

V

Descrito el marco jurídico al que debe ajustarse la Solución Tecnológica de Google (o Google Workspace en lo sucesivo), conviene analizar cuál sería el objeto del convenio, es decir, en qué consisten los servicios que va a ofrecer Google, qué datos o categorías de datos son objeto de tratamiento, y a qué finalidad sirven.

Con carácter previo, es conveniente indicar que la consultante aporta como elementos de análisis el Convenio y sus Anexos I y II, que son los Términos del Servicio y la Adenda de Protección de Datos, y, conviene adelantar ya, que en los mismos no consta información que este Gabinete Jurídico considera esencial para no solo poder formarse una opinión y realizar adecuadamente el análisis propuesto, sino también para el propio consultante a la hora de obligarse por medio del convenio, y en especial a la hora de cumplir sus obligaciones como responsable del tratamiento.

Comenzando por el propio CONVENIO, su objeto está definido en los siguientes términos:

1.1. El presente Convenio tiene un doble objeto:

1.1.1. Por un lado, establecer las condiciones de colaboración entre las Partes para el uso de los Servicios de Google Workspace for Education, según se definen más abajo, por parte del INTEF respecto de los centros docentes de Ceuta y Melilla.

1.1.2. Por otro lado, establecer un marco de colaboración entre las Partes para promover la innovación tecnológica y el desarrollo de la competencia digital educativa de alumnos y profesores en el territorio español.

Pues bien, la solución tecnológica Google Workspace se define en el apartado II del Exponen del convenio, según el cual la *solución tecnológica Workspace for Education, es un paquete de herramientas diseñado para permitir que los educadores y los alumnos innoven y aprendan juntos.*

Y respecto de los servicios en que se concreta dicha solución debe indicarse que de la lectura de la documentación se deduce que existen productos o servicios denominados *principales* y productos o servicios denominados *adicionales*. Ahora bien, no se encuentran definidos en la documentación contractual, por lo que la Parte contratante, al menos en un primer estadio de la contratación, desconoce a qué hacen referencia dichos términos.

Para concretarlos hay que acudir a otros elementos de información, como la página web de Google en la que publicita Google Workspace.

Los servicios *principales* están definidos en un apartado de dicha web denominado “Resumen de Servicios”¹ en dónde se enumeran y se ofrece una breve explicación de para qué sirven.

Respecto de los *servicios o productos adicionales*, tampoco se definen en los documentos que se aportan a la consulta, (Convenio, Términos y Adenda), sino que, para su concreción, aunque sea aproximada, hay que acudir a otras URLs:

En el sitio “Resumen de Servicios” de la página web workspace.google.com hay una breve referencia a los *productos adicionales* en los que se indica expresamente que:

No están sujetos al Contrato de Google Workspace y no se consideran Servicios de Google Workspace. El uso de los Productos Adicionales está sujeto a los Términos de los Productos Adicionales, disponibles en https://workspace.google.com/terms/additional_services.html. Además, el uso de los siguientes Productos Adicionales está sujeto a más términos

Esta inaplicación de los términos del convenio a dichos productos o servicios se recoge expresamente en los Anexos del Convenio:

Anexo I Términos del Servicio.

¹ https://workspace.google.com/intl/es/terms/user_features.html

3.5 Productos Adicionales. Google pone Productos Adicionales a disposición del Cliente y de sus Usuarios Finales. El uso de Productos Adicionales está sujeto a los Términos de Productos Adicionales. El Cliente puede habilitar o inhabilitar Productos Adicionales en cualquier momento a través de la Consola de Administración. El Cliente deberá obtener un consentimiento parental para recoger y utilizar información personal en los Productos Adicionales que quiera habilitar antes de permitir que ningún Usuario Final menor de 18 años acceda a ellos o los utilice.

Anexo II Adenda Protección de Datos.

5.3 Productos adicionales. Si Google, a su discreción, pone a disposición del Cliente cualquier Producto adicional de acuerdo con las Condiciones del mismo, y si el Cliente opta por instalar o utilizar dichos Productos adicionales, los Servicios podrán permitir que estos accedan a los Datos personales del cliente según sea necesario para la interoperación de los Productos adicionales con los Servicios. Para mayor claridad, las presentes Condiciones del tratamiento de datos no se aplican al tratamiento de datos personales en relación con la provisión de ningún Producto adicional utilizado por el Cliente, incluidos los datos personales transmitidos desde ese Producto adicional o hacia el mismo. El Cliente puede activar o desactivar los Productos adicionales, ya que no se requiere la utilización de dichos productos para hacer uso de los Servicios.

Es decir, son servicios que no forman parte del Google Workspace, pero que, en principio se pueden utilizar siempre y cuando se obtenga el consentimiento de los menores de 18 años por parte del centro docente (el administrador) y que recogen datos personales de los servicios principales “según sea necesario” para la interoperabilidad de ambos, es decir, para la interoperabilidad de los servicios principales y los servicios adicionales.

Ahora bien, **no se concretan en qué consisten**, lo que resulta esencial para que el firmante del convenio y sobre todo, el responsable del tratamiento, pueda hacerse una idea, aunque sea aproximada del peso o necesidad de uso que van a tener estos productos adicionales en los servicios principales que constituyen el GW.

En efecto, el responsable del tratamiento debe conocer si estos productos adicionales son o no fundamentales para explotar de manera óptima la solución tecnológica.

Dicho de otro modo, si no se utilizan estos productos esenciales ¿puede el Centro Educativo sacar el máximo partido a Google Workspace? ya que si la respuesta es negativa -como más adelante se explica- y por tanto resulta fundamental su uso, aunque este aparezca como opcional en el Convenio, resultarían de facto obligatorio, con las consecuencias que ello conlleva para la protección de datos de los usuarios.

Que, recordemos, quedarían fuera del Convenio y por tanto sujetos a las condiciones generales de cualquier usuario cuando usa los servicios de Google.

Y no podemos olvidar que estamos ante menores de edad y que la información personal que se usa es de muy diversa índole y de especial sensibilidad, pudiendo incluir, por ejemplo, categorías especiales de datos.

Pues bien, y sin perjuicio de que no consta en la documentación aportada (en definitiva, en el negocio jurídico, convenio, contrato) en qué consisten estos productos adicionales, otra vez hay que acudir a las distintas páginas webs de la compañía donde publicitan Google Workspace, en concreto en las condiciones de privacidad² se indica lo siguiente:

Los servicios adicionales de Google Workspace for Education incluyen servicios que ponemos a disposición de todos los consumidores de forma general, como la Búsqueda de Google, Maps y YouTube, a los que los usuarios de Workspace for Education pueden tener acceso con sus cuentas de Workspace.

En la “Ayuda de administrador de Google Workspace”³ se indica lo siguiente:

Los servicios adicionales, como YouTube, Google Maps y Blogger, se han diseñado para los usuarios de cuentas personales y se pueden utilizar de forma opcional con las cuentas de Google Workspace for Education si el administrador del dominio de cada centro autoriza su uso con fines educativos.

² https://workspace.google.com/intl/es/terms/education_privacy.html

³ <https://support.google.com/a/answer/6356441>

De la lectura de estas cláusulas se observa que productos como el buscador de Google, Maps y YouTube, quedan fuera de la regulación del convenio y que, por tanto, se aplicaría las condiciones generales para cualquier usuario.

Es decir, la información que se ofrece en el Convenio y en los Anexos respecto de estos servicios *adicionales* y la relevancia de su interoperabilidad con los servicios *principales*, no se ofrece con la claridad que se requiere, por cuanto algo que se muestra como voluntario en realidad va a resultar necesario para prestar el servicio en óptimas condiciones.

Esto resulta fundamental desde la óptica del derecho a la protección de datos, y desde el respeto al **principio de lealtad** (art. 5.1.a) RGPD), por cuanto el responsable del tratamiento debe tener toda la información posible del tratamiento que realizará su encargado para valorar la injerencia que supone el tratamiento en la privacidad de los afectados cuyos datos están siendo tratados por su cuenta, y así poder trasladar la información necesaria a los titulares de los datos personales que van a ser objeto del tratamiento.

El responsable del tratamiento no tendría que acudir, per se, a elementos de información externos para realizar una valoración de en qué medida va a ser necesario usar los servicios adicionales que suponen un tratamiento de datos en un entorno menos controlado y que dada la información que se ofrece -de nuevo en otros sitios web- sobre qué datos recoge y el régimen jurídico bajo el que se sitúan, resulta más invasivo en la privacidad de los afectados.

VI

Definido el objeto del convenio con las consideraciones que se han indicado previamente, procede abordar qué datos van a ser objeto de tratamiento.

Para ello, lo primero es acudir a la información contractual que se aporta con la consulta.

La única referencia a qué datos o categorías de datos van a ser objeto de tratamiento es la que aparece en el Apéndice 1 del Anexo II referido a la Adenda de Protección de Datos, donde consta lo siguiente:

Categorías de datos

Datos relativos a personas proporcionados a Google a través de los Servicios, por (o bajo la dirección de) el Cliente o los Usuarios finales.

Es un aspecto esencial a la hora de que un responsable vaya a contratar con un tercero un servicio que conlleve el tratamiento de datos saber qué datos personales van a ser objeto de tratamiento, algo que en el presente caso no consta en la documentación contractual.

En efecto, el responsable del tratamiento debe conocer de antemano qué datos personales se tratarán derivado del servicio que encomienda a Google a través de Google Workspace, y de la información que consta en la documentación contractual resulta obvio que esta es insuficiente a este propósito.

De nuevo hay que acudir a elementos externos de información para conocer qué datos van a ser objeto de tratamiento.

En el AVISO DE PRIVACIDAD⁴ de Google Workspace se informa sobre la recogida de los siguientes datos a partir de la diferenciación de Servicios Principales y Servicios Adicionales:

Servicios principales:

Cosas que proporciona o crea a través de los servicios principales

Recibimos datos de los clientes a través de los servicios principales y los procesamos de acuerdo con las instrucciones de la escuela (el cliente). Estos datos de clientes incluyen todo lo que usted o su escuela envíen, almacenen, envíen o reciban a través de los servicios principales.

Cuando se crea una cuenta de Google Workspace for Education, la escuela proporciona a Google cierta información personal sobre sus estudiantes y educadores que incluye el nombre del usuario, la dirección de correo electrónico y la contraseña. Las escuelas también pueden optar por compartir cosas como la dirección de correo electrónico secundaria, el número de teléfono y la dirección de un usuario. Y los usuarios también pueden agregar información a su cuenta, como un número de teléfono adicional y una foto de perfil.

⁴ https://workspace.google.com/intl/es/terms/education_privacy.html

Las cosas que puede crear a través de los servicios incluyen correos electrónicos que escribe y recibe mientras usa Gmail o documentos que redacta y almacena en Drive.

Los datos de los clientes se utilizan para proporcionar los servicios principales; por ejemplo, Google procesa su dirección de correo electrónico para enviar y entregar mensajes entre profesores y alumnos.

Información que recopilamos a medida que utiliza los servicios principales

Como se describe completamente en el Aviso de privacidad en la nube de Google, también recopilamos datos de servicio a través de los servicios principales, que incluyen:

- La información de su cuenta, que incluye elementos como el nombre y la dirección de correo electrónico.*
- Su actividad mientras usa los servicios principales, que incluye cosas como ver e interactuar con contenido, personas con las que se comunica o comparte contenido y otros detalles sobre su uso de los servicios.*
- Su configuración, aplicaciones, navegadores y dispositivos. Recopilamos información sobre su configuración y las aplicaciones, navegadores y dispositivos que utiliza para acceder a nuestros servicios. Esta información incluye el tipo de dispositivo y navegador, la configuración de los ajustes, los identificadores únicos, el sistema operativo, la información de la red móvil y el número de versión de la aplicación. También recopilamos información sobre la interacción de sus aplicaciones, navegadores y dispositivos con nuestros servicios, incluida la dirección IP, los informes de fallas, la actividad del sistema y la fecha y hora de su solicitud.*
- Tu información de ubicación. Recopilamos información sobre su ubicación determinada por diversas tecnologías, como la dirección IP y el GPS.*
- Sus comunicaciones directas. Mantenemos registros de las comunicaciones cuando usted o su administrador brindan comentarios, hacen preguntas o buscan soporte técnico.*

- *Y para los administradores, recopilamos datos sobre pagos y transacciones.*

Respecto de los servicios o productos adicionales, que, si bien se ofrecen como voluntarios, pero que tal como se ha indicado antes resultan “de facto” esenciales para que la solución Google Workspace *resulte eficiente para que los alumnos adquieran conocimientos TIC*, se indica en el citado AVISO DE PRIVACIDAD de Google Workspace que al utilizarlos se recoge la siguiente información:

Servicios adicionales

Cosas que usted proporciona o crea a través de servicios adicionales

Como se describe con más detalle en la Política de privacidad de Google, recopilamos información cuando los estudiantes y los educadores utilizan los servicios adicionales, incluidos los elementos que nos proporciona, el contenido que se crea o carga y el contenido que se recibe de otros. Por ejemplo, si inicia sesión en un servicio adicional con una cuenta de Workspace, usaremos su nombre de Workspace y la información de su perfil para identificar su cuenta. También puede optar por guardar su contenido con Google, cosas como fotos y videos.

Información que recopilamos a medida que utiliza servicios adicionales

La Política de privacidad de Google también describe la información que recopilamos a medida que utiliza nuestros servicios adicionales, que incluye:

- *Su actividad mientras usa servicios adicionales, que incluye cosas como los términos que busca, los videos que ve, el contenido y los anuncios que ve y con los que interactúa, información de voz y audio cuando usa funciones de audio, actividad de compra y actividad en sitios de terceros y aplicaciones que utilizan nuestros servicios.*

- *Tus aplicaciones, navegadores y dispositivos. Recopilamos la información sobre sus aplicaciones, navegador y dispositivos descritos anteriormente en la sección de servicios principales.*
- *Tu información de ubicación. Recopilamos información sobre su ubicación según lo determinado por varias tecnologías que incluyen: GPS, dirección IP, datos del sensor de su dispositivo e información sobre cosas cercanas a su dispositivo, como puntos de acceso Wi-Fi, torres de telefonía celular y dispositivos habilitados para Bluetooth. Los tipos de datos de ubicación que recopilamos dependen en parte de su dispositivo y la configuración de su cuenta.*

La información sobre qué datos personales se tratan no sólo consta en el extracto del aviso de privacidad que se acaba de transcribir, sino también en otras páginas web, como, por ejemplo, en el proceso de alta para usar Google Workspace que tiene que realizar cualquier Centro Educativo⁵:

Información que recogemos

Las cuentas de Google Workspace para Centros Educativos son cuentas de Google creadas y gestionadas por un centro educativo para que las utilicen los alumnos y los profesores. Al crear estas cuentas, el centro podría facilitar a Google información personal de los alumnos y los profesores, generalmente nombres de usuario, direcciones de correo electrónico y contraseñas; sin embargo, si lo estima conveniente, también podría incluir direcciones, números de teléfono y direcciones de correo electrónico secundarias. Google también podría recabar información personal directamente de los usuarios de las cuentas de Google Workspace para Centros Educativos, como su número de teléfono, la foto de perfil u otros datos que añadan a sus cuentas en este servicio.

Google también recoge información basada en el uso de nuestros servicios, como por ejemplo la siguiente:

- *Información del dispositivo, como el modelo de hardware, la versión del sistema operativo, los identificadores únicos de dispositivo e información de la red móvil, incluido el número de teléfono del usuario*

⁵ <https://workspace.google.com/edu/signup/welcome?hl=es>

- *Información del registro, incluidos detalles de cómo ha utilizado el usuario nuestro servicio, datos de los eventos del dispositivo y la dirección del protocolo de Internet (IP) del usuario*
- *Información de la ubicación, según determinen distintas tecnologías (p. ej., la dirección IP, el GPS y otros sensores)*
- *Números exclusivos de la aplicación (como el número de la versión de la aplicación)*
- *Cookies o tecnologías similares, que se utilizan para recoger y almacenar información sobre un navegador o dispositivo, como el idioma preferido u otros ajustes.*

Finalmente, y siguiendo con los datos que van a ser objeto de tratamiento por parte de Google a la hora de proporcionar la herramienta Google Workspace, especial atención merece información que **tampoco se ofrece en los documentos contractuales, y que es la referida a la compartición de información**. En concreto, en la ya citada política de privacidad alojada en la web antes indicada, consta el siguiente apartado:

Compartiendo tu información

Cuando compartes tu información

El administrador de su escuela puede permitir que los estudiantes accedan a los servicios de Google, como Google Docs y YouTube, que tienen funciones que permiten a los usuarios compartir información con otros o públicamente. Por ejemplo, si deja una reseña en Google Play, su nombre y foto aparecen junto a su actividad. Y si comparte una foto con un amigo que luego hace una copia o la vuelve a compartir, esa foto puede seguir apareciendo en la cuenta de Google de su amigo incluso después de que la elimine de su cuenta de Google. Recuerde, cuando comparte información públicamente, su contenido puede volverse accesible a través de motores de búsqueda, incluida la Búsqueda de Google.

Cuando Google comparte tu información

Tal como se describe en detalle en la Política de privacidad de Google y el Aviso de privacidad de Google Cloud, no compartimos su información

personal con empresas, organizaciones o personas ajenas a Google, excepto en los siguientes casos:

- *Con el administrador de su escuela: su administrador y los revendedores que administran su cuenta Workspace o la de su organización tendrán acceso a su información. Por ejemplo, pueden ser capaces de:*

- o Ver información, actividad y estadísticas de la cuenta;*

- o Cambiar la contraseña de su cuenta;*

- o Suspender o cancelar el acceso a su cuenta;*

- o Acceder a la información de su cuenta para cumplir con la ley, regulación, proceso legal o solicitud gubernamental aplicable;*

- o Restrinja su capacidad para eliminar o editar su información o su configuración de privacidad.*

- *Con su consentimiento: compartiremos información personal fuera de Google cuando tengamos su consentimiento o el de sus padres.*

- *Para procesamiento externo: compartimos información personal con nuestros afiliados y otros proveedores externos de confianza para que la procesen por nosotros tal como les indicamos y de conformidad con nuestra Política de privacidad, el Aviso de privacidad de Google Cloud y cualquier otra medida de confidencialidad y seguridad adecuada.*

- *Por motivos legales: compartimos información personal fuera de Google si creemos de buena fe que el acceso, uso, conservación o divulgación de la información es razonablemente necesario por motivos legales, incluido el cumplimiento de las solicitudes gubernamentales exigibles y la protección de usted y de Google.*

Resulta fundamental que esta información sobre compartición de información sea conocida tanto por el responsable del tratamiento, como por los titulares de los datos que van a ser objeto de tratamiento, antes de usar Google Workspace, tanto por lo que respecta a los servicios principales como a los servicios adicionales, por cuanto supone, por un lado, que los datos personales puedan ser revelados a terceros ajenos a la comunidad educativa y por otro,

que el propio centro educativo acceda a información personal, incluso en algunos casos a información íntima de los titulares de las cuentas de usuario de Google Workspace. Téngase en cuenta que los administradores van a poder, por ejemplo, cambiar la contraseña de la cuenta, lo que permitiría el acceso a toda información personal.

En definitiva, la información sobre los datos que se recaban, tanto en su aspecto cuantitativo como cualitativo, constituye un elemento clave para que el responsable del tratamiento pueda cumplir con el principio de responsabilidad proactiva y el de transparencia y derecho a la información, como más adelante se analiza, y también para abordar la injerencia en el derecho a la protección de datos en relación con la finalidad que se persigue, y en definitiva para analizar la adecuación al principio de proporcionalidad tal como se explica posteriormente.

VII

En cuanto a la *finalidad* que perseguirían los tratamientos derivados de la implementación del Google Workspace, su análisis va a resultar relevante por cuanto cualquier tratamiento de datos tiene que ser “necesario” para cumplir la finalidad que persigue, ya que de otro modo el tratamiento de datos no debe llevarse a cabo.

Así nos lo recuerda el Considerando 39 del RGPD al indicar que: *Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios.*

Asimismo, el concepto de “necesidad” cobra especial relevancia a la hora de definir las distintas bases jurídicas de legitimación del tratamiento, ya que salvo la relativa al consentimiento (letra a) del art. 6.1. RGPD), en las restantes, letras b) a f) del apartado 1 del artículo 6 del RGPD, la “necesidad del tratamiento para” es un requisito ineludible.

Dicho esto, y atendiendo a la documentación contractual aportada con la solicitud de este Informe, únicamente se aborda la finalidad en el Apéndice 1 de la Adenda de protección de datos, de la que resulta que la información sobre la finalidad es la siguiente:

Naturaleza y finalidad del tratamiento

Google tratará los Datos personales del cliente con el fin de proporcionar los Servicios y TSS al Cliente de conformidad con la Adenda de Tratamiento de Datos.

Sucede de nuevo que **otro aspecto tan relevante como la finalidad del tratamiento tiene esa escasa mención en la documentación contractual**. Otra vez, el firmante del convenio y, en su caso, el responsable del tratamiento, se van a ver desprovistos de información fundamental, que requiere su previa determinación en la concreción de su vinculación jurídica con el encargado del tratamiento.

Es decir, el responsable del tratamiento, al determinar “el propósito del tratamiento” debe de disponer de toda la información necesaria en relación con lo que va a realizar “por su cuenta” el encargado del tratamiento.

Como sucede respecto de otros elementos fundamentales que deberían figurar por contrato, hay que acudir a fuentes externas.

En la información sobre los servicios o productos principales, del ya citado Aviso de Privacidad alojado en la web de Google Workspace for Education se puede extraer la siguiente información sobre la finalidad (a pesar de no estar definida o denominada dicha información como tal):

En el apartado relativo a los *servicios principales* consta lo siguiente:

Los datos de servicio se usan principalmente para brindar los servicios que usan las escuelas y los estudiantes, pero también se usan para mantener y mejorar los servicios; hacer recomendaciones para optimizar el uso de los servicios; proporcionar y mejorar otros servicios que solicite; dar apoyo; proteger a nuestros usuarios, clientes, el público y Google; y cumplir con las obligaciones legales. Consulte el Aviso de privacidad de Google Cloud para obtener más información.

En el apartado relativo a los *servicios adicionales* consta lo siguiente:

Los datos que recopilamos en los servicios adicionales se utilizan en todos nuestros servicios para brindar, mantener y mejorar nuestros servicios; desarrollar nuevos servicios; brindar servicios personalizados; medida de rendimiento; comunicarse contigo; y proteger a Google, a

nuestros usuarios y al público. Consulte la Política de privacidad de Google para obtener más detalles.

Algunos servicios adicionales muestran anuncios. Pero si usa su cuenta de Google Workspace for Education en escuelas primarias y secundarias no le mostramos anuncios personalizados, lo que significa que no usamos información de su cuenta o actividad anterior para orientar los anuncios. Sin embargo, podemos mostrar anuncios en función de factores generales como su consulta de búsqueda, la hora del día o el contenido de una página que está leyendo.

(...).”

En definitiva, para los servicios *principales*, las finalidades del tratamiento serán, con carácter general, la prestación de los servicios, pero también existen otras finalidades adicionales como las siguientes: *mejorar los servicios; hacer recomendaciones para optimizar el uso de los servicios; proporcionar y mejorar otros servicios que solicite; dar apoyo; proteger a nuestros usuarios, clientes, el público y Google.*

Respecto de las finalidades de los productos *adicionales*, deben destacarse aquellas como *brindar servicios personalizados, medida de rendimiento, y la muestra de anuncios en función de factores generales como las búsquedas realizadas, la hora del día o el contenido de una página que este siendo visualizada, así como la combinación de la información personal de un servicio con la que se recoja de otro.*

Como puede observarse, hay finalidades que no sirven al propósito del responsable del tratamiento -sino únicamente al “encargado”- y además están definidas en términos ambiguos e inconcretos (*mejorar servicios, dar apoyo, etc.*) y de otras se infiere que se producen a partir de la elaboración de perfiles, (*muestra de anuncios en función de factores generales*).

Es decir, si las finalidades no sirven al propósito del tratamiento, que es el derecho a la educación, y en cambio responden a finalidades del encargado, la consecuencia será que éste se convierte en responsable del tratamiento y debe encontrar otra base jurídica que la que legitima al responsable “primario”, es decir, a la administración educativa.

Dicho de otro modo, si Google, a través de Google Workspace, realiza tratamientos de datos personales para finalidades propias que nada tienen que

ver con el derecho a la educación, ya no puede legitimar su tratamiento en el artículo 6.1 c) y/o e) del RGPD como lo hace la administración educativa.

Dicho lo anterior, sobre la cuestión referida a la muestra de anuncios en función de factores generales, que conlleva un perfilado para acciones publicitarias, es preciso recordar lo indicado en el Reglamento 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022, -Reglamento de Servicios Digitales-, aplicable a partir del 17 de febrero de 2024, que impone las siguientes obligaciones a los prestadores de plataformas en línea en relación con el perfilado realizado a partir de datos personales de menores de edad:

Artículo 28 Protección de los menores en línea

1 Los prestadores de plataformas en línea accesibles a los menores establecerán medidas adecuadas y proporcionadas para garantizar un elevado nivel de privacidad, seguridad y protección de los menores en su servicio.

2 Los prestadores de plataformas en línea no presentarán anuncios en su interfaz basados en la elaboración de perfiles, tal como se define en el artículo 4, punto 4, del Reglamento (UE) 2016/679, mediante la utilización de datos personales del destinatario del servicio cuando sean conscientes con una seguridad razonable de que el destinatario del servicio es un menor.

3 El cumplimiento de las obligaciones establecidas en el presente artículo no obligará a los prestadores de plataformas en línea a tratar datos personales adicionales a fin de evaluar si el destinatario del servicio es un menor.

4. La Comisión, previa consulta a la Junta, podrá proporcionar directrices para guiar a los prestadores de plataformas en línea en la aplicación del apartado 1.

En cualquier caso, el responsable del tratamiento no está en condiciones de conocer a priori y sin ambages las finalidades que perseguiría la implementación de Google Workspace, ni a partir de la información que se ofrece en los documentos contractuales, ni tampoco a partir de las fuentes de información externas.

Y como se ha dicho antes, que el responsable del tratamiento conozca con total claridad elementos que son fundamentales para dicho tratamiento, como

el objeto del convenio, los datos que se van a tratar, o la finalidad del tratamiento, resulta esencial, tanto para cumplir con el nuevo modelo de cumplimiento del RGPD, que descansa en la responsabilidad proactiva, como para saber qué información ha de ofrecer a los titulares de los datos sobre el tratamiento que va a realizar, pasando por el análisis del contexto del tratamiento y determinar con acierto las medidas de seguridad adecuadas.

VIII

De acuerdo con lo expuesto en los apartados anteriores del presente informe se concluye que, en la medida en que estamos ante un paquete de herramientas digitales que está formado por distintos servicios, -principales y los denominados adicionales-, y que por tanto, y en función de los que se usen -previa determinación por Google y no por INTEF, tal como se deduce del propio Convenio y sus anexos, donde se establece que los servicios, tanto principales como adicionales, dependen de lo que se ofrezca en cada momento- se pueden tratar diferentes tipos de datos personales y en consecuencia abarcar diversas finalidades, resulta difícil establecer la base jurídica de legitimación del tratamiento de datos en los apartados c) y e) del artículo 6.1 del RGPD.

En efecto, ya que el Convenio y anexos, y en otras fuentes de información, se ofrece una información en la que en ocasiones se mezclan finalidades propias del responsable (satisfacer el derecho a la educación en entornos digitales) con las propias del supuesto encargado del tratamiento, y en otras ocasiones claramente sirven a los propósitos del encargado del tratamiento, no es posible legitimar dichos tratamientos en los apartados c) y e) del artículo 6.1 del RGPD.

Nos dice el apartado 6.3 del RGPD que:

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por: a) el Derecho de la Unión, o b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento. La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al

responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

Por su parte, el artículo 8 de la LOPDGDD nos indica, bajo la denominación “Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos” que:

1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.

2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley.

En efecto, en el artículo 27 de la Constitución, en las leyes de transferencias de competencias del Estado en favor de las CCAA, y en los artículos 2.1 l) y 111 bis y disposición adicional vigesimotercera de la LOE, podríamos encontrar la base jurídica para el tratamiento de datos en el ámbito educativo a través de

Jurídico

herramientas tecnológicas y entornos digitales para la adquisición de competencias TIC.

Es decir, estaríamos ante los supuestos de legitimación previstos en las letras c) y e) del artículo 6 apartado 1 del RGPD.

Ahora bien y como se ha mencionado antes, en lo que se refiere al objeto del convenio y a los tratamientos que se llevarían a cabo como consecuencia de su firma, dado que existen finalidades que exceden del ámbito educativo y que sirven únicamente a los intereses de la parte que según convenio se instituye en “encargado del tratamiento”, no puede legitimarse dicho tratamiento en el artículo 6.1 e) del RGPD por cuanto un hipotético interés público se vería supeditado o condicionado al interés privado y particular del supuesto encargado del tratamiento, situación que debe rechazarse por completo.

Igual sucedería con el cumplimiento de una obligación legal aplicable al responsable del tratamiento como base jurídica prevista en el artículo 6.1 c) del RGPD, sencillamente porque tratamientos con finalidades como *mejorar servicios*, o *mostrar anuncios en función de factores generales*, obviamente no resultan obligatorios para el verdadero responsable del tratamiento -la administración educativa- y menos aún están previstos como tal en una norma con rango de ley (art. 8.2 LOPDGDD).

IX

Una vez analizado el objeto del convenio, los datos que se recaban, la finalidad que persigue y cómo se informa acerca de ella, es preciso analizar el instrumento jurídico que prevé el propio Convenio para mostrar la aquiescencia del uso de los servicios que ofrece la herramienta de Google por parte de los centros educativos.

En el Anexo I del convenio, referido a los Términos del Servicio Google Workspace (GW), consta lo siguiente:

3.3 Privacidad. El Cliente es responsable de obtener los consentimientos y de proporcionar los avisos necesarios para permitir:

- a) *el uso y la recepción de los Servicios por parte del Cliente; y*
- b) *el acceso, almacenamiento y tratamiento por parte de Google de los datos proporcionados por el Cliente (incluidos los Datos del Cliente) en virtud del Convenio.*

Es decir, recae en el firmante del convenio, en INTEF, la obligación de que a la hora de implementar GW se haya otorgado el consentimiento tanto del cliente (que sería el Centro Educativo) como de los usuarios (que sería cualquier miembro de la comunidad educativa que fuera destinatario de la solución tecnológica, como el administrador, profesores, y alumnos, ya sean menores de 14 años o no).

En este aspecto es preciso traer a colación la información que se muestra durante el proceso de alta del servicio⁶ por parte de un Centro Educativo, en el que bajo la denominación “Consentimiento del centro para el uso de Google Workspace para Centros Educativos” figura lo siguiente:

Para que los alumnos puedan utilizar los Servicios Principales de Google Workspace para Centros Educativos (“Servicios Principales”), es requisito imprescindible que los centros den su consentimiento.

Revisa la siguiente información sobre nuestras prácticas de obtención, uso y divulgación de los datos relacionados con Google Workspace para Centros Educativos y muestra tu conformidad a continuación. Google no recabará, utilizará ni divulgará de manera intencionada la información personal de los alumnos a menos que hayas dado tu consentimiento.

Ten en cuenta que también es necesario que los centros educativos obtengan el consentimiento de los padres o tutores sobre cualquier servicio adicional que pongan a disposición de los alumnos menores de 18 años. Asimismo, como práctica recomendada, puede ser conveniente que los centros reciban el consentimiento de los padres o tutores sobre el uso de los Servicios Principales que ofrecen a los alumnos. Consulta los recursos que hay disponibles para obtener el consentimiento de los padres o tutores, entre ellos una plantilla que puedes personalizar y utilizar en tu caso concreto.

(...)

⁶ <https://workspace.google.com/edu/signup/tos?hl=es>
c. Jorge Juan 6
28001 Madrid

La página web tiene otros subepígrafes, relativos a “Información que recogemos” y “como utilizamos la información que recogemos” que antes se han transcrito, para concluir con un último apartado denominado “Consentimiento” en el que consta lo siguiente:

Al hacer clic en "Acepto", das tu consentimiento, en nombre de tu institución, a que Google procese la información personal de los alumnos en los Servicios Principales tal y como se ha descrito anteriormente y de acuerdo con el aviso de privacidad de Google Workspace para Centros Educativos y la política de privacidad de Google, y aceptas obtener el consentimiento de los padres o tutores sobre cualquier servicio adicional que pongas a disposición de los alumnos menores de 18 años.

De la lectura de estas cláusulas se observa que el Cliente, es decir, INTEF, se compromete, con la firma del convenio, a recabar los consentimientos y a realizar los avisos necesarios para poder usar Google Workspace y, en consecuencia, para poder someter a tratamiento por parte de Google aquella información que contiene datos personales de los alumnos y de los docentes.

La manera de articular esa obtención de los consentimientos se produciría a través de varias etapas o estadios.

Tal como se deduce de la información que se muestra en el proceso de alta del servicio, lo primero que sucedería es que la persona que realiza el alta da el consentimiento en nombre de la institución, es decir, del Centro Educativo, para que Google trate los datos de los alumnos y obviamente, en un momento posterior, recaba el consentimiento de los alumnos.

Por tanto, primero se autoriza por parte del centro educativo la utilización del servicio Google Workspace, y para su puesta en marcha el Centro Educativo asume frente a Google el compromiso de recabar el consentimiento de los titulares de los datos.

Respecto de esa autorización o consentimiento que tiene que prestar el Centro Educativo, resulta obvio que no estamos ante el consentimiento al que se refieren los artículos 4.11, 6.1 a) y 7 del RGPD, sino que debe entenderse como una autorización contractual o un compromiso para obligarse a hacer algo, ya que obviamente nunca podría dicho Centro Educativo -tal como está redactada la cláusula- otorgar el consentimiento de unos terceros para el tratamiento de sus datos personales.

Por lo tanto, estamos ante una autorización por parte del Centro Educativo, para obligarse o someterse a las condiciones de uso de Google Workspace.

Es decir, estamos ante una suerte de “consentimiento para contratar” con la naturaleza jurídica del consentimiento -como requisito de los contratos- al que se refiere el artículo 1261 del Código Civil, y que debe ser libre de error (artículos 1265 y 1266 del Código Civil), para lo que resulta fundamental disponer de toda la información necesaria, que como hemos visto en el presente caso, no se ofrece con la firma del convenio.

Dicho lo anterior, la segunda fase o paso a seguir es que el Centro Educativo solicite de los padres, y en su caso, de los alumnos, el consentimiento para el uso de Google Workspace. Este consentimiento al que se refiere Google, lo pretende articular como una de las bases jurídicas que legitime este tratamiento; ahora bien, como se ha indicado antes, la base jurídica para el tratamiento de datos personales derivado de la implantación de soluciones tecnológicas y el uso de entornos digitales por parte de la administración educativa la encontramos en el artículo 6.1 e) del RGPD, y en ocasiones también en el apartado c) de dicho artículo, y no en el consentimiento.

Estamos ante distintos tratamientos que exceden de la función educativa y que sirven en buena medida a Google para sus propios intereses -es decir al supuesto encargado del tratamiento, lo que le convierte pues en responsable del tratamiento-, por eso no puede situarse como base jurídica lo indicado en el artículo 6.1 c) y e) del RGPD.

Cuestión distinta es que Google -aunque sea de modo indirecto- “proponga” el consentimiento como instrumento jurídico que legitime el tratamiento que vaya a realizar, tal como se deduce de los términos contractuales y aquellos que se encuentran en las distintas fuentes informativas que se han ido citando.

Dicho lo anterior, el consentimiento como base jurídica del tratamiento encuentra su definición en el artículo 4.11 del RGPD que considera como tal:

toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen

El Considerando 43 del RGPD nos indica que:

(43) Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibrio claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aun cuando este no sea necesario para dicho cumplimiento.

De acuerdo con la definición, y en relación con el uso de Google Workspace por parte de los alumnos, debemos detenernos en primer lugar en la nota de *libertad*.

En las Directrices 5/2020 sobre el consentimiento en el sentido del RGPD, de 4 de mayo de 2020, del Comité Europeo de Protección de Datos (CEPD), nos indica lo siguiente:

3. En general, el consentimiento solo puede ser una base jurídica adecuada si se ofrece al interesado control y una capacidad real de elección con respecto a si desea aceptar o rechazar las condiciones ofrecidas o rechazarlas sin sufrir perjuicio alguno. Cuando solicita el consentimiento, el responsable del tratamiento tiene la obligación de evaluar si dicho consentimiento cumplirá todos los requisitos para la obtención de un consentimiento válido. Si se obtiene en pleno cumplimiento del RGPD, el consentimiento es una herramienta que otorga a los interesados el control sobre si los datos personales que les conciernen van a ser tratados o no. Si no es así, el control del interesado será meramente ilusorio y el consentimiento no será una base jurídica válida para el tratamiento, lo que convertirá dicha actividad de tratamiento en una actividad ilícita.

(...)

13. El término «libre» implica elección y control reales por parte de los interesados. Como norma general, el RGPD establece que, si el sujeto

no es realmente libre para elegir, se siente obligado a dar su consentimiento o sufrirá consecuencias negativas si no lo da, entonces el consentimiento no puede considerarse válido. Si el consentimiento está incluido como una parte no negociable de las condiciones generales se asume que no se ha dado libremente. En consecuencia, no se considerará que el consentimiento se ha prestado libremente si el interesado no puede negar o retirar su consentimiento sin perjuicio. La noción de desequilibrio entre el responsable del tratamiento y el interesado también se tiene en cuenta en el RGPD.

14. A la hora de valorar si el consentimiento se ha dado libremente, deben considerarse también las situaciones concretas en las que el consentimiento se supedita a la ejecución de contratos o a la prestación de un servicio tal y como se describe en el artículo 7, apartado 4. El artículo 7, apartado 4, se ha redactado de manera no exhaustiva mediante el uso de la expresión «entre otras cosas», lo que significa que puede haber otras circunstancias que entren en el ámbito de aplicación de esta disposición. En términos generales, el consentimiento quedará invalidado por cualquier influencia o presión inadecuada ejercida sobre el interesado (que puede manifestarse de formas muy distintas) que impida que este ejerza su libre voluntad.

Teniendo en cuenta lo indicado en las Directrices 5/2020, en el presente caso, no podemos entender que un hipotético consentimiento que se prestara por los padres de los alumnos, o incluso por éstos, si fueran mayores de catorce años, se otorgaría con plena libertad.

La razón resulta obvia: si el Centro Educativo va a utilizar las herramientas de Google Workspace como apoyo de las asignaturas curriculares y para la adquisición de competencias digitales, el alumno respecto del que no se haya obtenido el consentimiento quedaría automáticamente fuera de esta parte de la enseñanza, es decir, los contenidos y actividades que se impartieran utilizando las herramientas de Google Workspace no se le ofrecerían a dicho alumno, y se excluiría al alumno de las dinámicas de trabajo, sufriendo un agravio comparativo traducido en un incuestionable perjuicio.

Sensu contrario, sucedería igual si una vez otorgado el consentimiento, este se quisiera revocar. A este respecto las citadas Directrices nos indican que:

46. El responsable del tratamiento debe demostrar que es posible negar o retirar el consentimiento sin sufrir perjuicio alguno (considerando 42).

Por ejemplo, el responsable del tratamiento debe demostrar que la retirada del consentimiento no conllevará ningún coste para el interesado y, por tanto, ninguna clara desventaja para quienes retiren el consentimiento.

47. Otros ejemplos de perjuicio son el engaño, la intimidación, la coerción o consecuencias negativas importantes si un interesado no da su consentimiento. El responsable del tratamiento debe ser capaz de demostrar que el interesado pudo ejercer una elección libre o real a la hora de dar su consentimiento y que le era posible retirarlo sin sufrir ningún perjuicio.

48. Si el responsable del tratamiento puede demostrar que un servicio incluye la posibilidad de retirar el consentimiento sin que se produzca ninguna consecuencia negativa, por ejemplo, sin que disminuya el nivel en la prestación del servicio en detrimento del usuario, ello bastará para probar que el consentimiento se prestó libremente.

En este caso, si no existe otra alternativa a Google Workspace disminuiría el nivel de enseñanza que se le otorga al alumno que no diera o retirara el consentimiento.

Otro elemento que se analiza a la hora de valorar la libertad del consentimiento es el desequilibrio de poder. Nos dice las Directrices 5/2020 del CEPD que:

13 (...) Queda también claro en la mayoría de los casos que el interesado no dispondrá de alternativas realistas para aceptar el tratamiento (las condiciones de tratamiento) de dicho responsable. El CEPD considera que hay otras bases jurídicas que son, en principio, más adecuadas para el tratamiento de datos por las autoridades públicas

En el presente caso, el consentimiento se daría en un contexto de desequilibrio entre el responsable del tratamiento y el interesado, es decir, el centro docente por un lado y el alumno por otro, siendo el primero el responsable y frente al que se presta el consentimiento.

El responsable del tratamiento, para obtener un consentimiento libre, debería dar una alternativa equivalente al alumno que no otorgue su consentimiento para usar Google Workspace. Es decir, tendría que disponer de otras herramientas digitales similares, en el sentido de que el alumno que se

decantara por esta opción no sufriría un agravio comparativo ni perjuicio de ninguna clase.

Aquí también merece especial atención el tratamiento de los datos de los docentes, a quienes inevitablemente se les crearía una cuenta de usuario de Google Workspace. Tampoco sería adecuada en este caso la obtención del consentimiento como base jurídica para que sus datos fueran utilizados por Google. Así las Directrices 5/2020 del CEPD nos recuerdan que:

21. También en el contexto del empleo se produce un desequilibrio de poder. Dada la dependencia que resulta de la relación entre el empleador y el empleado, no es probable que el interesado pueda negar a su empleador el consentimiento para el tratamiento de datos sin experimentar temor o riesgo real de que su negativa produzca efectos perjudiciales. Parece poco probable que un empleado pudiera responder libremente a una solicitud de consentimiento de su empleador para, por ejemplo, activar sistemas de vigilancia por cámara en el lugar de trabajo o para rellenar impresos de evaluación, sin sentirse presionado a dar su consentimiento. Por tanto, el CEPD considera problemático que los empleadores realicen el tratamiento de datos personales de empleados actuales o futuros sobre la base del consentimiento, ya que no es probable que este se otorgue libremente. En el caso de la mayoría de estos tratamientos de datos en el trabajo, la base jurídica no puede y no debe ser el consentimiento de los trabajadores [artículo 6, apartado 1, letra a)] debido a la naturaleza de la relación entre empleador y empleado.

22. No obstante, esto no significa que los empleadores no puedan basarse nunca en el consentimiento como base jurídica para el tratamiento de datos. Puede haber situaciones en las que el empleador pueda demostrar que el consentimiento se ha dado libremente. Dado el desequilibrio de poder entre un empleador y los miembros de su personal, los trabajadores únicamente pueden dar su libre consentimiento en circunstancias excepcionales, cuando el hecho de que otorguen o no dicho consentimiento no tenga consecuencias adversas.

Además, dada la injerencia en la privacidad que se ha ido poniendo de manifiesto y la finalidad que persigue el tratamiento en cuestión, difícilmente tendría cabida el tratamiento de los datos de los empleados en el artículo 6.1 b)

del RGPD, -ejecución de un contrato-, ya que el quantum de “necesidad” para cumplir la relación jurídico-laboral, plantea dudas.

En este sentido nos recuerdan las Directrices 5/2020 del CEPD lo siguiente:

30. De acuerdo con el Dictamen 06/2014 del GT29, la expresión «necesario para la ejecución de un contrato» debe ser interpretada de manera estricta. El tratamiento debe ser necesario para cumplir el contrato con cada interesado. Esto puede incluir, por ejemplo, el tratamiento de la dirección del interesado con el fin de que puedan entregarse productos adquiridos en línea, o el tratamiento de los datos de la tarjeta de crédito para facilitar el pago. En el contexto laboral, este principio permitiría, por ejemplo, el tratamiento de la información sobre el salario y los datos de la cuenta bancaria para que pueda abonarse el sueldo. Debe existir un vínculo directo y objetivo entre el tratamiento de los datos y la finalidad de la ejecución del contrato.

Otra característica del consentimiento que resulta esencial es que sea un **consentimiento informado**.

Aquí cobra especial relevancia la circunstancia que ha planeado durante el análisis que se ha realizado en los anteriores apartados del presente informe, sobre el *objeto* del convenio (los servicios en que consiste), los *datos* que se recaban y la *finalidad* del tratamiento, y que no es otra que la escasa información -en algunos casos inexistente- que sobre estos aspectos ofrecía la documentación contractual (Convenio, Anexo I Términos del Servicio y Anexo II Adenda de protección de Datos).

Si el destinatario de la obligación de obtener el consentimiento informado — admitiendo a efectos meramente dialécticos que sea la administración educativa y que tiene que acudir al artículo 6.1 a) del RGPD y no al 6.1 e) RGPD—, carece del conocimiento de aspectos básicos del tratamiento que su encargado va a realizar, cómo va a poder el responsable ofrecer información suficiente a los titulares de los datos personales a los que va a solicitar el consentimiento.

A lo que hay que añadir que estamos ante el tratamiento de datos de menores de edad, tanto menores de 14 años como mayores de 14 años y menores de 18 años. Y la información que ha de ofrecerse debe ser adaptada a dicha edad. Nos dice el Considerando 58 del RGPD que:

Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender.

Facilitar información a los interesados antes de obtener su consentimiento es esencial para que puedan tomar decisiones informadas, comprender qué es lo que están autorizando y, por ejemplo, ejercer su derecho a retirar su consentimiento. Si el responsable no proporciona información accesible, el control del usuario será ilusorio y el consentimiento no constituirá una base válida para el tratamiento de los datos.

Sobre los requisitos mínimos para que se entienda que el consentimiento es *informado*, en las Directrices 5/2020 se recogen los siguientes:

- I. la identidad del responsable del tratamiento
- II. el fin de cada una de las operaciones de tratamiento para las que se solicita el consentimiento,
- III. qué (tipo de) datos van a recogerse y utilizarse,
- IV. la existencia del derecho a retirar el consentimiento,
- V. información sobre el uso de los datos para decisiones automatizadas de conformidad con el artículo 22, apartado 2, letra c), cuando sea pertinente, e
- VI. información sobre los posibles riesgos de transferencia de datos debido a la ausencia de una decisión de adecuación y de garantías adecuadas, tal y como se describen en el artículo 46.

En el presente caso se debería informar de, al menos, los requisitos que se acaban de indicar para que el consentimiento fuera informado.

Y respecto de *cómo* hay que informar, las Directrices 5/2020 señalan que:

67. Cuando solicitan el consentimiento, los responsables del tratamiento deben asegurarse de que utilizan un lenguaje claro y sencillo en todos los casos. es decir, el mensaje debe ser comprensible para un ciudadano medio y no únicamente para juristas. Los responsables del tratamiento no pueden utilizar políticas de privacidad muy extensas que sean difíciles de entender o declaraciones llenas de jerga jurídica. (...)

68. El responsable del tratamiento debe asegurarse de que el consentimiento se facilita sobre la base de información que permita a los interesados identificar fácilmente quién es el responsable y comprender qué es lo que están autorizando. El responsable debe describir claramente el fin del tratamiento de datos para el que se solicita consentimiento.

70. El responsable del tratamiento debe valorar el tipo de público que proporciona datos a su organización. Por ejemplo, en el caso de audiencias determinadas que incluyen interesados que son menores de edad, se espera que el responsable del tratamiento se asegure de que el lenguaje sea comprensible para dicho grupo. Tras determinar su audiencia, los responsables del tratamiento deben determinar qué información deben facilitar y, posteriormente, cómo presentarán dicha información a los interesados.

En definitiva, si se pretende el uso del consentimiento para poder utilizar Google Workspace -sin perjuicio de que la base jurídica sea el artículo 6.1 e) RGPD cuando las finalidades del tratamiento sean las educativas - debería ofrecerse información teniendo en cuenta que muchas familias pueden no tener suficientes conocimientos sobre la implicación que tiene el tratamiento de datos de sus hijos (sobre todo el almacenamiento, conservación y difusión) y en ocasiones los de los demás miembros de la familia que utilicen dispositivos y la misma conexión que el menor usuario de una cuenta de Google Workspace y que no disponen de información suficiente para tomar una decisión compleja y sopesada, e incluso pueden desconocer que pueden existir otras alternativas, otras herramientas digitales, para cumplir el mismo fin. Sólo teniendo en cuenta estos aspectos, en ese caso, estaríamos ante un consentimiento libre e informado.

Otro requisito del consentimiento es que debe ser específico para cada finalidad; debe ser una **manifestación de voluntad específica**. Referido a esto, las Directrices 5/2020 nos indican que:

55. (...) El requisito de que el consentimiento deba ser «específico» tiene por objeto garantizar un nivel de control y transparencia para el interesado. Este requisito no ha sido modificado por el RGPD y sigue estando estrechamente vinculado con el requisito de consentimiento «informado». Al mismo tiempo, debe interpretarse en línea con el requisito de «disociación» para obtener el consentimiento «libre». En

suma, para cumplir con el carácter de «específico» el responsable del tratamiento debe aplicar:

i la especificación del fin como garantía contra la desviación del uso,

ii la disociación en las solicitudes de consentimiento, y

iii una clara separación entre la información relacionada con la obtención del consentimiento para las actividades de tratamiento de datos y la información relativa a otras cuestiones.

(...)

57. Si el responsable del tratamiento se basa en el artículo 6, apartado 1, letra a), los interesados deberán siempre dar su consentimiento para un fin específico para el tratamiento de los datos, En consonancia con el concepto de limitación de la finalidad, con el artículo 5, apartado 1, letra b), y con el considerando 32, el consentimiento puede abarcar distintas operaciones, siempre que dichas operaciones tengan un mismo fin. Huelga decir que el consentimiento específico solo puede obtenerse cuando se informa expresamente a los interesados sobre los fines previstos para el uso de los datos que les conciernen.

58. (...). Si un responsable trata datos basándose en el consentimiento y, además, desea tratar dichos datos para otro fin, deberá obtener el consentimiento para ese otro fin, a menos que exista otra base jurídica que refleje mejor la situación.

60 (...) un responsable del tratamiento que busque el consentimiento para varios fines distintos debe facilitar la posibilidad de optar por cada fin, de manera que los usuarios puedan dar consentimiento específico para fines específicos.

61(...), los responsables del tratamiento deben facilitar, con cada solicitud de consentimiento separada, información específica sobre los datos que se tratarán para cada fin, con el objeto de que los interesados conozcan la repercusión de las diferentes opciones que tienen. De este modo, se permite a los interesados dar un consentimiento específico. Esta cuestión se solapa con el requisito de que los responsables faciliten información clara.

En el presente caso, y sin perjuicio de que en la documentación contractual únicamente se indica que la finalidad del tratamiento es para la prestación del servicio, tal como se ha puesto de manifiesto en el análisis de otras fuentes externas de información sobre Google Workspace, se observa que existen finalidades distintas que suponen, por ejemplo, la elaboración de perfiles o la difusión de los datos de los menores a través de servicios de la sociedad de la información, y que de acuerdo con lo expuesto, si se pretende obtener el consentimiento para todas ellas, debería de realizarse de modo individual, en el sentido de poder aceptar unas sin tener que aceptar las otras. Igualmente sucedería con la revocación.

En este sentido cobra especial relevancia lo indicado en el artículo 92 de la LOPDGDD antes citado a cuyo tenor:

Artículo 92. Protección de datos de los menores en Internet.

Los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información.

Cuando dicha publicación o difusión fuera a tener lugar a través de servicios de redes sociales o servicios equivalentes deberán contar con el consentimiento del menor o sus representantes legales, conforme a lo prescrito en el artículo 7 de esta ley orgánica.

Finalmente hay que indicar que el consentimiento ha de prestarse mediante una **clara acción afirmativa** y en ocasiones ha de ser un consentimiento **explícito**.

Esta última calificación (“explícito”) puede referirse a situaciones en las que existe un grave riesgo en relación con la protección de los datos y en las que se considera adecuado que exista un elevado nivel de control sobre los datos personales. En virtud del RGPD, el consentimiento explícito tiene una función importante en el artículo 9 sobre el tratamiento de categorías especiales de datos personales, en las disposiciones sobre la transferencia de datos a terceros países u organizaciones internacionales en ausencia de garantías adecuadas, como establece el artículo 49, y en el artículo 22 sobre decisiones

individuales automatizadas, incluida la elaboración de perfiles. (Apartado 91 de las Directrices 5/2020).

En el presente caso, al utilizar los servicios de Google Workspace se podrían someter a tratamiento categorías especiales de datos, como datos de salud o datos relativos al origen étnico o racial, así como podrían suceder, dados los términos de la documentación contractual que más adelante se analiza, transferencias internacionales de datos a países en ausencia de garantías, e incluso se producen elaboraciones de perfiles, tal como se deduce de la documentación y fuentes de información externas analizadas.

X

En otro orden de cosas, la consultante solicita el parecer de esta Agencia en relación con el régimen jurídico aplicable al acuerdo y en concreto sobre las previsiones acerca de la coexistencia de varios documentos que regularían la implementación de GW y la posibilidad de modificación unilateral de los mismos.

La documentación contractual está formada por el Convenio, el Anexo I Términos del Servicio, y el Anexo II relativo a la Adenda de Protección de Datos, donde se establecen reglas de prelación en caso de conflicto y la posibilidad de modificar los términos contractuales de manera unilateral por Google, es decir, sin la intervención de INTEF.

En el Convenio consta en el apartado 1.2 que:

1.2. Las Partes reconocen y aceptan que el uso de los Servicios está regulado por los siguientes acuerdos, que forman parte de, y están incorporados al, presente Convenio:

- *los Términos del Servicio de Workspace for Education que se incluyen como Anexo 1 ("Términos de Workspace for Education") a este Convenio, y*
- *la versión más actual de la Adenda de Tratamiento de Datos disponible en cada momento en https://workspace.google.com/terms/dpa_terms.html, cuya*

traducción de la versión vigente al momento de la firma del presente Convenio se incluye a efectos meramente de referencia como Anexo 2 a este Convenio.

Por su parte, en el apartado 9 constan las siguientes cláusulas:

9.1. Interpretación. En caso de conflicto entre las secciones que conforman este Convenio, éstas se interpretarán en el siguiente orden de preferencia (en orden decreciente de preferencia): la Adenda de Tratamiento de Datos, los Términos de Workspace for Education y las Cláusulas Generales del Convenio.

9.3. Divisibilidad. Si una cláusula de este Convenio (o parte de ella) fuera declarada inválida, ilegal o inaplicable, el resto de este Convenio seguirá estando en vigor.

En el Anexo I relativo a los Términos del Servicio de Workspace for Education, constan las siguientes cláusulas:

1.5 Modificaciones

(a) Servicios. Google puede realizar cambios comercialmente razonables en los Servicios cuando lo estime oportuno. Google informará al Cliente si realiza en los Servicios algún cambio material que afecte de manera sustancial al uso de los Servicios por parte del Cliente y este ha acordado con Google recibir información sobre tal cambio.

(...)

(d) Adenda de Tratamiento de Datos. Google solo puede modificar la Adenda de Tratamiento de Datos si los cambios en cuestión son necesarios para cumplir las leyes y normativas aplicables, una orden judicial o una directriz publicada por un ente regulador o una agencia gubernamentales; si los cambios en cuestión están permitidos expresamente en la Adenda de Tratamiento de Datos; o si los cambios en cuestión:

(i) son comercialmente razonables;

(ii) no conllevan la degradación de la seguridad general de los Servicios;

(iii) no amplían el ámbito de aplicación ni eliminan ninguna restricción del tratamiento de los "Datos Personales de los Clientes" por parte de Google, según se establece en la sección

"Ámbito de aplicación del Tratamiento" de la Adenda de Tratamiento de Datos; y
(iv) no tiene un impacto adverso material en los derechos del Cliente en virtud de la Adenda de Tratamiento de Datos.

En el Anexo II referido a la Adenda de Tratamiento de Datos, en el apartado Definiciones conviene destacar lo siguiente:

- *Por Resumen de servicios de Google Workspace se entenderá: la descripción vigente de los servicios de Google Workspace (incluidas las ediciones relacionadas), tal y como se establece en https://workspace.google.com/terms/user_features.html (que puede ser actualizada por Google oportunamente de conformidad con el Contrato de Google Workspace).*

Como puede observarse existen cláusulas, tanto en el propio Convenio como en los Anexos, en las que se permite que Google *motu proprio* modifique elementos esenciales que tienen una incuestionable incidencia en el tratamiento de datos personales.

Así, por ejemplo, se hace una remisión a la "*versión más actual de la Adenda de Tratamiento de datos disponible en cada momento*" algo que podría pugnar con lo dispuesto en el art. 1256 del Código civil, por cuanto, en caso de conflicto interpretativo, es precisamente dicho documento el que prevalece, y es un documento que puede modificar Google unilateralmente, aunque sea cuando en su opinión se den la condiciones previstas en el propio Anexo I del Convenio (apartado 1.5, letra d), apartados i) a iv), transcrito).

O también, cuando se permite a Google realizar cambios "comercialmente razonables en los Servicios cuando lo estime oportuno".

En cualquier caso, aun admitiendo estas cláusulas parece que estamos más bien ante Google como un responsable del tratamiento que como un encargado, (que es formalmente como se presenta), por cuanto asume una posición de toma de decisiones sin contar con la otra parte y que se imponen contractualmente con incuestionables consecuencias en el tratamiento de datos personales.

En este ámbito concreto de la protección de datos, que es en el que se desenvuelve exclusivamente este informe, ello supondría que el responsable del tratamiento desconocería, o en cualquier caso, puede desconocer, cómo van a ser tratados datos personales en cada momento por su cuenta. Por ello,

aunque se entendiera a título de hipótesis que las modificaciones que pudiera realizar Google unilateralmente no pugnan con el art. 1256 CC, sí que impiden reconocer que en esta situación Google sea pretendidamente encargado del tratamiento, ya que le impone al responsable unas condiciones contractuales que este último continuaría estando obligado a cumplir, lo que efectivamente no permite considerar que este es el verdadero responsable. Ello vaciaría de contenido la figura del responsable del tratamiento y no podríamos considerar que existe, en el caso concreto, un verdadero encargo del tratamiento.

En este aspecto, es preciso aclarar que no se está mostrando un criterio desfavorable a que los términos del contrato sean redactados, por una parte, y la otra únicamente pueda adherirse, tal como se prevé en el apartado 108 de las Directrices 7/2020: *(..) En ocasiones, los contratos entre responsables y encargados del tratamiento pueden ser redactados de manera unilateral por una de las partes. La redacción por una u otra parte puede depender de varios factores, como la posición de las partes en el mercado y su poder contractual, sus conocimientos técnicos y su acceso a servicios jurídicos. Por ejemplo, algunos prestadores de servicios tienden a fijar unas condiciones tipo, que incluyen acuerdos sobre el tratamiento de datos. (...)* sino que nuestro parecer es contrario a que pueda ser considerado responsable quien ha de soportar los cambios unilaterales de la relación jurídica por la otra parte, pretendidamente el encargado (sin entrar ahora, se reitera, en la validez, o no, puramente civil de dichas cláusulas).

respecto de la relación entre el responsable y encargado del tratamiento, ya en las citadas Directrices 7/2020 se dice que *El responsable del tratamiento determina los fines y medios del tratamiento; esto es, el porqué y el cómo del tratamiento. Debe decidir tanto sobre los fines como sobre los medios (...) o que “El encargado del tratamiento debe tratar los datos siguiendo exclusivamente las instrucciones del responsable”.*

Pues bien, atendiendo a la posibilidad de modificación unilateral del contrato por parte de Google y a la definición de unos términos cambiantes que resultan obligatorios para las partes, difícilmente puede el responsable del tratamiento decidir sobre los medios o que el encargado cumpla las instrucciones del responsable, porque de hacerlo, lo haría sobre unos tratamientos que aquel no ha determinado, sino que ha sido el propio encargado.

El control sobre el tratamiento es un elemento esencial para definir la figura del responsable del tratamiento. Las citadas Directrices 7/2020 indican que

25 (...) la calificación de una parte como «responsable del tratamiento» debe establecerse sobre la base de una evaluación de las circunstancias de hecho en que tiene lugar el tratamiento. Para alcanzar una conclusión acerca de si un ente concreto ejerce una influencia determinante en relación con el tratamiento de los datos personales en cuestión, deben tenerse en cuenta todas las circunstancias de hecho pertinentes. (...)

28. (...) Aun cuando el contrato no estipule quién es el responsable del tratamiento, puede contener elementos suficientes para inferir quién tiene el poder de decisión en relación con los fines y medios del tratamiento(...)

En el presente caso, tal como se presentan los términos contractuales (convenio y anexos) se desprende que Google tiene poder de decisión en relación con los medios del tratamiento. (y no nos referimos a medios no esenciales -apartado 38 de las Directrices 7/2020- , ya que la posibilidad de configurar la Adenda del Tratamiento sitúa a Google en un primer plano decisorio).

A lo que hay que añadir que, de las finalidades que se han analizado, existen algunas que sirven a fines propios de Google, y a este respecto, las finalidades deben circunscribirse al servicio contratado, es decir, al tratamiento que se ha “encargado”. En este sentido, nos recuerda el artículo 33.2 de la LOPDGDD en su último párrafo que: *Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades.* O el propio art. 28.10 RGPD: *Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento.*

En conclusión, la regulación sobre los términos aplicables a la relación jurídica que se desprende del Convenio y Anexos, y en su caso, la aplicación práctica de la misma resultarían contrarias al RGPD por las razones expuestas.

Jurídico

Otra cuestión que plantea la consultante es la referida a la regulación del subencargado del tratamiento y las posibilidades de que su elección conlleve transferencias internacionales de datos a países u organizaciones que no ofrezcan un nivel adecuado de protección.

En el Anexo II consta lo siguiente:

10.1 Almacenamiento de datos e instalaciones de tratamiento. De acuerdo con los compromisos de ubicación de datos de Google en virtud de los Términos específicos del servicio y el resto de este apartado (Transferencias de datos), los Datos del Cliente podrán ser tratados en cualquier país en el que Google o sus Subencargados del tratamiento tengan instalaciones.

Sobre las transferencias internacionales de datos, únicamente hay que indicar que, aunque resulte obvio, deben cumplir lo dispuesto en el RGPD y en especial en las Decisiones de Adecuación que resulten de aplicación a la transferencia concreta en cuestión, por lo que cualquier asunción de obligación por parte de INTEF debe tener en cuenta el marco normativo vigente en cada momento, lo que ha de ser determinante a la hora de aceptar por el responsable (INTEF) un subencargado del tratamiento

En este aspecto es preciso recordar lo indicado en las Directrices 7/2020 en su apartado 120:

120. El CEPD recomienda que el responsable del tratamiento preste la debida atención a este punto concreto, en especial cuando el encargado tenga la intención de delegar determinadas actividades de tratamiento en otros encargados o cuando cuente con divisiones o unidades establecidas en terceros países. Si las instrucciones del responsable del tratamiento no autorizan las transferencias o comunicaciones a terceros países, no se permitirá al encargado asignar el tratamiento a un subencargado de un tercer país ni tratar los datos en alguna de sus divisiones no establecidas en territorio de la UE.

Dicho lo anterior, respecto del régimen de subcontratación en la regulación en el Anexo II se indica lo siguiente:

11.1 Consentimiento para la contratación del Subencargado del tratamiento de datos.

El Cliente autoriza específicamente la contratación como Subencargados del tratamiento de datos de las entidades enumeradas a partir de la Fecha de entrada en vigor de la Adenda en la URL especificada en el apartado 11.2 (Información sobre los Subencargados del tratamiento de datos). Además, sin perjuicio del apartado 11.4 (Oportunidad de objetar a los cambios de los Subencargados del tratamiento de datos), el Cliente generalmente autoriza la contratación como Subencargados de cualquier otro tercero (“Nuevos Subencargados del tratamiento de datos”).

11.2 Información sobre los Subencargados del tratamiento de datos.

La información sobre los Subencargados del tratamiento de datos, incluidas sus funciones y ubicaciones, se encuentra disponible en <https://workspace.google.com/intl/en/terms/subprocessors.html> (actualizada periódicamente por Google de acuerdo con la presente Adenda de Tratamiento de Datos).

(...)

11.4 Oportunidad de oponerse a los cambios del Subencargado del tratamiento de datos.

a. Cuando se contrate a un nuevo Subencargado del tratamiento durante el Período de vigencia, Google notificará al Cliente la contratación (incluido el nombre y la ubicación del subencargado del tratamiento de datos correspondiente y las actividades que realizará), al menos 30 días antes de que el nuevo Subencargado del tratamiento de datos terceros comience el tratamiento de cualquier Dato personal del Cliente.

b. El Cliente puede, en un plazo de 90 días tras la notificación de la contratación de un nuevo Subencargado, oponerse rescindiendo inmediatamente el Contrato por conveniencia notificándose a Google.

Pues bien, la regulación a la que hay que atenerse es lo indicado en el artículo 28.2 del RGPD, a cuyo tenor:

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

En este sentido las Directrices 7/2020 indican que:

128. El acuerdo debe especificar que el encargado no podrá recurrir a otro encargado sin la autorización previa por escrito del responsable y si esta autorización será específica o general. En caso de que la autorización sea general, el encargado debe informar al responsable de cualquier cambio de los subencargados objeto de la autorización escrita y dar al responsable la oportunidad de oponerse al cambio. Se recomienda que el contrato prevea un procedimiento a tal efecto.

La regulación del Anexo II resultaría contraria al RGPD por varias cuestiones.

La primera se extrae de lo indicado en el artículo 28.2 RGPD y en el apartado 128 de las citadas Directrices, en los que resulta esencial el término “previo”.

En efecto, el responsable debe otorgar la autorización a la subcontratación con carácter previo a que esta se produzca y sin embargo, en la cláusula 11.4 se deduce que Google contrata primero al subencargado, y posteriormente lo comunica a INTEF, dándole 30 días de antelación al menos a la fecha en que el subencargado comience sus servicios.

A partir de ahí y el responsable tiene 90 días para oponerse (por tanto, no para “autorizar”), lo que significa que el responsable puede acabar oponiéndose (por ejemplo, a los 80 días), cuando el subencargado ya ha comenzado a prestar los servicios sin el consentimiento previo del responsable. Circunstancia que es contraria a la finalidad que busca el RGPD, que se concreta en este aspecto en que el responsable tenga el control del tratamiento que se realice por su cuenta, manifestándose entre otras cuestiones, en la elección del subencargado.

La segunda razón es porque, en puridad, no existe en el contrato una verdadera posibilidad de que el responsable se oponga (o autorice), por cuanto en caso de que el responsable muestre su negativa respecto de la subcontratación, la opción que le queda es resolver el contrato.

El encargado del tratamiento no puede forzar al responsable a que la única respuesta que pueda dar este ante un subencargado que no sea de su conveniencia, sea rescindir el contrato.

Esta forma de proceder también resulta contraria al control que debe tener el responsable respecto del tratamiento que se realice por su cuenta. Es decir, no puede decidir libremente oponerse a un concreto subencargado.

XII

Respecto de la posibilidad de aplicar una normativa no europea al tratamiento de datos personales derivado del convenio y sus anexos, en el apartado 4.2 de la Adenda de Tratamiento de Datos consta que:

4.2 Aplicación de la Regulación No Europea. Las partes reconocen que la Regulación de Protección de Datos No Europea también puede aplicarse al tratamiento de los Datos personales de los Clientes.

4.3 Aplicación de las condiciones. Excepto en la medida en que esta Adenda de Tratamiento de Datos disponga lo contrario, esta se aplicará independientemente de si la Regulación Europea de Protección de Datos o la Regulación de Protección de Datos No Europea se aplica al tratamiento de los Datos personales de los Clientes.

Estas cláusulas deben ser rechazadas y no asumidas por INTEF, toda vez que la interpretación de estas cláusulas se presta a confusión. Es evidente que el ámbito de aplicación territorial del RGPD (art. 3 RGPD) no puede verse modificado a voluntad de las partes. El RGPD es una norma que no admite disposición o inaplicación en este contexto, sino que es de obligado cumplimiento. Por ello, si esta cláusula se refiere a la no aplicación del RGPD cuando la normativa aplicable ha de ser el RGPD, no es aceptable por no ser posible.

Dicho esto, la cláusula 4.2 puede interpretarse en el sentido de que INTEF asume que “pueden” existir tratamientos respecto de los que no se aplique el RGPD (por ejemplo, en caso de transferencias internacionales de los datos cuando no hay Decisión de adecuación), pero esa cláusula no explicita cuales son esos casos, sino que sólo enuncia la “posibilidad de que ello ocurra”, sin

saber exactamente a qué se refiere.; En cualquier caso, , teniendo en cuenta los servicios que se prestan, que lo son por un responsable del tratamiento que forma parte de la administración general de un Estado Miembro de la UE, y los destinatarios de los mismos, que son la comunidad educativa de las Ciudades Autónomas de Ceuta y Melilla, dicha cláusula no sería aceptable, por ambigua y contraria a los intereses del responsable.

En conclusión, la recomendación de este Gabinete Jurídico es la eliminación de dichas cláusulas porque lejos de aportar valor a la regulación, resultan innecesarias, ambiguas, inconcretas y materialmente contrarias al RGPD si se refiere a la aplicación territorial del RGPD.

XIII

Otro aspecto que la consultante plantea es la gestión de las violaciones de seguridad, (en términos del convenio y anexos, “incidentes de seguridad”), y que, según ésta, no existe un compromiso de Google de notificar al responsable del tratamiento el incidente en menos de 72 horas.

En el apartado 7.2 de la Adenda de Protección de datos, consta lo siguiente:

7.2 Incidentes de datos.

7.2.1. Notificación de incidentes. Google notificará al Cliente a la mayor brevedad y sin retrasos indebidos en cuanto tenga conocimiento de un Incidente de datos, y tomará rápidamente medidas razonables para minimizar el daño y proteger los Datos personales del cliente.

Las obligaciones respecto de las “violaciones de datos” se asumen directamente por el responsable del tratamiento, tal como se deriva del artículo 33.1 del RGPD, de cuyo tenor resulta:

1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de

la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

Ahora bien, respecto del encargado, el apartado 2 indica que:

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

Es decir, no se establece un plazo determinado, sino que se dice sin dilación indebida. No obstante, la gestión de las violaciones de seguridad o, mejor dicho, la intervención en la gestión de violaciones de seguridad por parte del encargado es uno de los elementos que constituyen el contenido mínimo del contrato o acto jurídico que regule la relación responsable y encargado.

El artículo 28.3 f) del RGPD dice:

(...) Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

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

Es decir, en tanto que la participación del encargado en las violaciones de datos es una materia objeto de regulación en el contrato o acto jurídico que regule dicha relación responsable-encargado, y además el artículo 33.2 RGPD establece la obligación de notificación al responsable, y que además el responsable ha de notificar la violación a más tardar en 72 horas, dado que el encargado ha de ayudar al responsable a *garantizar* el cumplimiento de sus obligaciones en este aspecto, el encargado debe asimismo notificar al responsable la violación de manera que este pueda notificarla a su vez en 72 horas, luego el encargado ha de obligarse a comunicar al responsable dicha circunstancia en todo caso antes de las 72 horas. Si no fuera así, el encargado no estaría *garantizando* al responsable el cumplimiento de sus obligaciones. Por ello se recomienda que a juicio del responsable del tratamiento se estableciera un plazo máximo de notificación por parte del encargado, que le permitiera cumplir el plazo de 72 horas que, con carácter general, le impone el artículo 33.1 RGPD.

Como conclusión cabe indicar si bien no es obligatorio según el RGPD que el encargado notifique en un plazo concreto los incidentes de seguridad al responsable, y en la medida en que es materia objeto de negociación y contenido mínimo ex art. 28.3 f) RGPD, como práctica recomendada se estima adecuado la concreción de un término que permita al responsable cumplir sus obligaciones, lo que en última instancia redundaría en la gestión adecuada de las violaciones de seguridad.

XIV

Finalmente, procede abordar la adecuación al principio de proporcionalidad de las consecuencias que la implementación de los tratamientos de datos que conlleva la plataforma Google Workspace tendría en los datos personales de los destinatarios del citado paquete de herramientas de Google.

La consultante en este aspecto sostiene en síntesis que dicho tratamiento no superaría el juicio de proporcionalidad por no resultar necesaria la implementación de dicha plataforma -por diversas cuestiones- para cumplir con los objetivos de la enseñanza relacionados con la adquisición de competencias digitales y sobre la base de los perjuicios que dicho tratamiento puede ocasionar si lo ponemos en relación con los riesgos que se asumen con dicho tratamiento.

Pues bien, debe comenzarse el análisis teniendo en cuenta lo indicado en el Considerando 4 del RGPD que reconoce que:

el derecho a la protección de datos no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad.

En el presente caso, la adquisición de competencias digitales por los miembros de la comunidad educativa forma parte del derecho fundamental a la educación previsto en el artículo 27 de la Constitución Española, tal como se deduce de los artículos 2.1 l) y 11 bis de la LOE y en el artículo 83 de la LOPDGDD, todos ellos parcialmente transcritos al inicio del presente informe.

Por lo tanto, y sin perjuicio de que como se ha dicho antes, la solución Google Workspace sirve también a finalidades propias del encargado del tratamiento, conviene analizar en qué medida cumple los fines del derecho a la educación en los términos descritos y si su injerencia en el derecho a la protección de datos personales resulta proporcional.

El principio de proporcionalidad, recogido en la doctrina del Tribunal Constitucional, sirve para resolver si la injerencia en un derecho fundamental es conforme a derecho en relación con la preservación de otros derechos o bienes jurídicos o en aplicación de otras normas, cuando estemos ante un conflicto entre dos o más opciones que ofrezca el ordenamiento jurídico en su aplicación a un caso concreto.

La Sentencia del Tribunal Constitucional 14/2003, de 28 de enero, recuerda lo siguiente:

“En otras palabras, de conformidad con una reiterada doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan basta con recordar que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); sí, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto; SSTC 66/1995, de 8 de mayo, F. 5; 55/1996, de 28 de marzo, FF. 7, 8 y 9; 270/1996, de 16 de diciembre, F. 4.e; 37/1998, de 17 de febrero, F. 8; 186/2000, de 10 de julio, F. 6).”

Comenzando por el primer elemento a tener en cuenta, es decir, la idoneidad, que consiste en la relación de causalidad, de medio a fin, entre el medio adoptado y el fin propuesto. Por tanto, se trata del análisis de una relación medio-fin.

Para el supuesto que se cita en la consulta, y sin perjuicio del análisis que debe realizar el responsable del tratamiento, a título de ejemplo se podría afirmar

que la utilización de plataformas digitales por parte de la comunidad educativa puede resultar adecuada para lograr el objetivo de alcanzar competencias digitales y destrezas en entornos TIC.

Ahora bien, en el caso concreto del paquete de herramientas que ofrece Google Workspace, debe tenerse en cuenta cómo se relacionan en términos de eficacia los denominados servicios principales y los servicios adicionales.

En el sentido de que para optimizar el uso de Google Workspace, algunos de los servicios adicionales se muestran como esenciales -por ejemplo, la visualización de videos- y no están incluidos en el acervo contractual, sino que además de requerir una “contratación” adicional, como hemos visto, suponen una mayor injerencia en la privacidad de los alumnos. No quiere decir esto que sea obligatorio usar los servicios adicionales, es más se presentan como voluntarios o adicionales, sino que para alcanzar la eficacia completa de Google Workspace se necesita de su uso. Por tanto, en cuanto a la idoneidad se puede afirmar que la solución tecnológica puede cumplir el propósito, pero con los matices que se acaban de indicar.

En relación con la necesidad, ésta consistirá en examinar si existen otros medios alternativos al optado que no sean gravosos o al menos que lo sean en menor intensidad. Se trata del análisis de una relación medio-medio, esto es, de una comparación entre medios; el optado y el o los hipotéticos que hubiera podido adoptarse para alcanzar el mismo fin.

En este caso, conviene traer a colación lo indicado por la consultante:

Según se recoge en la resolución de la Secretaría de Estado de Educación, por la que se establecen las normas, protocolos y condiciones de uso del equipamiento tecnológico y plataformas de servicios en la nube de los centros educativos sostenidos con fondos públicos no universitarios de las ciudades de Ceuta y Melilla.

“... se ha dotado a la totalidad de los centros educativos públicos no universitarios de ambas ciudades de redes de cableado estructurado, con puntos de datos en cada una de las aulas y espacios educativos de los centros, redes inalámbricas de alta densidad, redes de comunicación con conexión a RedIris para la provisión de Internet, sistemas de navegación segura de contenidos, puestos de trabajo de aula y dispositivos portátiles y tabletas para su utilización indistintamente dentro y fuera de los recintos escolares.”

De manera simultánea, y a través de los objetivos del Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF), se ha facilitado a las escuelas la disponibilidad de plataformas de publicación de contenidos (CMS), plataformas de formación a distancia (LMS) y recursos educativos en abierto centrados en las diferentes materias y ámbitos curriculares (REA) así como itinerarios formativos de apoyo a las áreas. Todo ello constituye el llamado Sistema Educativo Digital (SED) que está a disposición de todos y cada uno de los centros educativos.

También proporciona entornos de gestión educativa (Alborán), gestión de inventarios tecnológicos y de incidencias (GLPI) y sistemas para el fomento de la lectura y gestión de bibliotecas escolares a través de ABIES.

Programas institucionales como Redes de cableado estructurado en centros docentes públicos, Escuela 2.0, Cultura Digital y Escuelas Conectadas y ahora Educa en Digital han aportado a los centros educativos del ámbito competencial del MEFP los recursos necesarios para la digitalización de la educación.”

Argumento que comparte este Gabinete Jurídico por cuanto es el propio Ministerio de Educación y Formación Profesional, el que conoce la disponibilidad de los recursos y por tanto quien está en mejores condiciones para conocer el grado de necesidad de la implementación de esta solución.

En este sentido, es preciso poner de manifiesto que existen otras soluciones tecnológicas destinadas a la comunidad educativa, al margen de Google Workspace que se han implantado en otros ámbitos territoriales, y que, junto con lo indicado por la propia consultante, hacen que no se perciba como “única y necesaria” la solución de Google.

Y finalmente, la proporcionalidad en sentido estricto o ponderación pasa por la comparación entre el grado de realización u optimización del fin y la intensidad de la intervención en el derecho. En este caso debería valorarse si se dan más ventajas o beneficios para el interés general que perjuicios para los usuarios.

Aquí resulta imprescindible conocer los posibles perjuicios que el uso de Google Workspace podría tener para los menores de edad, teniendo en cuenta, entre otras cuestiones, los riesgos que se asumirían con la implementación.

Resulta especialmente clarificador y que sirve como parámetro a tener en cuenta a la hora de valorar los posibles perjuicios derivados de los riesgos a asumir, lo indicado en el artículo 28.2 de la LOPDGDD cuando identifica los riesgos que se han de tener en cuenta a la hora de aplicar las medidas a las que se refieren los artículos 24 y 32 del RGPD, y que son los siguientes:

a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.

d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones

internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

En efecto, en el presente caso todos los elementos que se citan en el precepto cobran especial importancia por cuanto un estamos ante el tratamiento de datos en una plataforma digital en la que los principales usuarios (al margen del profesorado) son menores de edad. (y, *per se*, son un colectivo especialmente vulnerable)

Y que por las características de los servicios que se ofrecen tanto los ordinarios como los denominados adicionales, permiten un escenario de interacción y comunicación, en algunos casos similar a las redes sociales y en otros, como la plataforma YouTube, que son en sí mismos una red social.

No olvidemos que los alumnos estarían identificados a través de una cuenta de usuario y sería con la que interaccionen en los distintos servicios, ya sea entre alumnos, con el profesorado, o con usuarios externos a la organización -pudiendo mostrar sus preferencias expresas por contenidos a través de la replicación de contenidos, a través de interacciones de “me gusta”, o a través de la inclusión de comentarios respecto de los mismos en los que se admite libertad de texto y pudiendo ser compartido por terceros. Teniendo en cuenta estas posibilidades, se podría someter a tratamiento información sobre comportamientos psicológicos, como trastornos alimentarios, problemas de sociabilidad, comportamientos culturales y educativos, etc. de esos menores.

Así se desprende de los servicios que ofrece la solución tecnológica, tanto ordinarios como adicionales, que han sido objeto de análisis ut supra.

Por ello, los riesgos para los menores de edad en cuanto a la generación de situaciones de discriminación, daño para la reputación, pérdida de confidencialidad, resultan evidentes.

También, como acertadamente advierte la consultante, podríamos estar ante el tratamiento de categorías especiales de datos, por cuanto de las interacciones con la plataforma y los distintos servicios se podrían inferir datos de salud o de convicciones religiosas. Y esta información podría transferirse a terceros estados que no ofrecieran un nivel adecuado de protección.

A lo que hay que añadir la elaboración de perfiles que inevitablemente se daría respecto, por ejemplo, el rendimiento escolar, las preferencia o intereses, o incluso su geolocalización.

Asimismo, para valorar la injerencia en el derecho a la protección de datos, resulta un parámetro esencial el volumen de datos recogidos y su tipología. Según la información que ofrece propia entidad Google, se podrían recabar los siguientes:

- *el nombre del usuario, la dirección de correo electrónico y la contraseña.*
- *la dirección de correo electrónico secundaria, el número de teléfono y la dirección de un usuario.*
- *un número de teléfono adicional y una foto de perfil.*
- *Los correos electrónicos que escribe y recibe mientras usa Gmail o documentos que redacta y almacena en Drive.*
- *La actividad mientras usa los servicios principales, que incluye cosas como ver e interactuar con contenido, personas con las que se comunica o comparte contenido y otros detalles sobre su uso de los servicios.*
- *La configuración, aplicaciones, navegadores y dispositivos:*

Esta información incluye el tipo de dispositivo y navegador, la configuración de los ajustes, los identificadores únicos, el sistema operativo, la información de la red móvil y el número de versión de la aplicación.

información sobre la interacción de las aplicaciones, navegadores y dispositivos con sus servicios, incluida la dirección IP, los informes de fallas, la actividad del sistema y la fecha y hora de la solicitud.

- *Información de ubicación determinada por diversas tecnologías, como la dirección IP y el GPS, datos del sensor de su dispositivo e información sobre cosas cercanas a su dispositivo, como puntos de acceso Wi-Fi, torres de telefonía celular y dispositivos habilitados para Bluetooth*
- *La actividad mientras se usan servicios adicionales:*

los términos que busca, los videos que ve, el contenido y los anuncios que ve y con los que interactúa, información de voz y audio cuando usa funciones de audio, actividad de compra y actividad en sitios de terceros y aplicaciones que utilizan los servicios.

No cabe duda de que estamos ante una recogida invasiva de información personal para simplemente recibir parte de la educación a través de un entorno digital y adquirir competencias digitales.

No se respetaría pues el principio de minimización del artículo 5.1 del RGPD, ni en términos cuantitativos ni cualitativos y tampoco se observa que dada la cantidad de datos recopilados y el modo de hacerlo se haya tenido en cuenta lo indicado en el artículo 25 del RGPD en cuanto a la protección de datos desde el diseño y por defecto.

Y todo lo indicado en un entorno de recogida masiva de datos que implica a un gran número de afectados. Recordemos en este aspecto que la solución tecnológica se pretende implementar en aquellos territorios en los que el Ministerio de Educación y Formación no tiene transferidas sus competencias a las Comunidades Autónomas, es decir en las ciudades autónomas de Ceuta y de Melilla y que según el Informe de 2022 sobre el Estado del Sistema Educativo del Consejo Escolar del Estado⁷, durante el curso 2020-2021 hubo 22.497 y 23.123, alumnos matriculados respectivamente. Estas cifras sirven para aproximar la magnitud de los destinatarios a los que iría dirigida la solución tecnológica de Google y por tanto la multiplicación de las situaciones de riesgo o perjudiciales que se acaban de indicar.

A la vista de los razonamientos anteriores, y de los que pueda realizar el consultante, corresponde al responsable del tratamiento extraer las consecuencias conforme a su propio análisis de la afectación de dichos tratamientos al principio de proporcionalidad.

XV

⁷ <https://www.educacionyfp.gob.es/dam/jcr:a53b231c-bae6-41c2-b965-3b86a39b29b7/i22cee09-ceuta-melilla.pdf>

En conclusión, se informa desfavorablemente la firma del Convenio y Anexos planteados por parte de la consultante, por los motivos que se han ido poniendo de manifiesto durante el presente informe.