PI23-025

RESOLUCIÓN Nº R24-045 DEL PROCEDIMIENTO DE INFRACCIÓN Nº PI23-025

Por la Agencia Vasca de Protección de Datos se ha instruido expediente de infracción PI23-025 (DN23-034) por la actuación del Departamento de Educación del Gobierno Vasco, en base a los siguientes,

HECHOS

PRIMERO. - Con fecha 11 de julio de 2023 tiene entrada en el Registro General de la Agencia Vasca de Protección de Datos escrito de reclamación en el que se denunciaba lo siguiente:

> *"II.- Que somos conocedores de que en el Consejo de Gobierno del Gobierno Vasco de 22 de febrero de 2022 se comunicó la suscripción de un Convenio con Google Cloud Emea Limited, para la utilización de los Servicios Google Workspace for Education en los centros docentes del Departamento de Educación (en adelante, "el Convenio") que se adjunta al presente escrito como DOCUMENTO N.° 2.*
>
> *III.- Que el Boletín Oficial del País Vasco de 21 de abril de 2022 (anuncio 1723) publicó la Resolución 42/2022, de 11 de abril, del Director de la Secretaría del Gobierno y de Relaciones con el Parlamento, que se adjunta como DOCUMENTO N.° 3 por la que se dispone la publicación del citado Convenio con Google, con su texto incorporado como anexo en el mismo Boletín.*
>
> *IV.- Esta parte entiende que el tratamiento de los datos de carácter personal de docentes y menores de edad por parte de Google en el marco del citato Convenio supone el incumplimiento de la normativa de protección de datos al llevarse a cabo transferencias internacionales de datos a Estados Unidos sin que se cumpla lo establecido en la normativa vigente de protección de datos. En este sentido, se adjuntan como DOCUMENTO N.° 4 los Términos del Servicio de Workspace for Education y la Adenda de Tratamiento de Datos.*
>
> *V.- A juicio de esta parte, el riesgo de un uso indebido de los datos personales es elevado ya que se involucran datos de carácter personal de personas menores de edad, que, como es sabido, requieren de una especial protección. En este sentido, con respecto a los Términos del Servicio de Workspace for Education cabe destacar lo siguiente:*
>
> - *Varias agencias de protección de datos de países europeos han concluido que el paquete Google Workspace no cumple el Reglamento General de Protección de Datos (RGPD) de la Unión Europea y han prohibido su uso en las escuelas. A modo de ejemplo, la Autoridad Danesa de Protección de Datos, entre otras, ha resuelto que el paquete de software Workspace basado en la nube de*

Google «no cumple con los requisitos» de las regulaciones de privacidad de datos GDPR de la Unión Europea.

- *El Anexo 1 del convenio, Términos del Servicio de Workspace for Education, en el apartado 5.2 indica que no incluirá Publicidad en los Servicios (de Workspace for Education), sin embargo podrá incluirla en otros productos del mismo grupo empresarial, como el buscador o Youtube, que serán la opción habitual al que se nos orientará si trabajamos en el entorno de Google Workspace for Education (GWE). Teniendo en cuenta que la mayoría de las personas afectadas por el convenio está en la edad escolar, esta parte considera que no recaer sobre menores de edad la responsabilidad de tener que evitar las intromisiones publicitarias descritas.*
- *La Adenda de Tratamiento de Datos puede ser modificada unilateralmente por Google, y según la cláusula 9.1 del convenio esta prevalece sobre los otros documentos.*
- *El punto 5.3 de la Adenda de Tratamiento de Datos, indica que sus condiciones no se aplican a los productos adicionales de Google y que estos podrán acceder a los datos personales gestionados por Google Workspace for Education.*
- *Una de las variantes de Google Workspace for Education ofrece investigar los documentos privados de los alumnos https://edu.google.com/intl/ALL_es/workspace-for-education/editions/compare-editions "herramientas para fomentar la integridad académica. Informes de originalidad ilimitados y la posibilidad de buscar coincidencias con trabajos previos de compañeros almacenados en un repositorio privado".*
- *A juicio de esta parte, no se ha realizado sobre el convenio la Evaluación de Impacto en la Protección de Datos Personales (EIPD) que requiere el articulo 35 del RGPD.*

En virtud de cuanto antecede,

SOLICITA que teniéndose por presentado este escrito junto con la documentación que lo acompaña se admita y teniéndose por formulada RECLAMACIÓN, previas las comprobaciones que se estime oportuno realizar, se abra el correspondiente expediente sancionador".

A dicho escrito se acompañó la documentación a que se hace referencia en la reclamación y la misma ha quedado incorporada al expediente.

SEGUNDO. - Con fecha 23 de julio 2023 se dio traslado a la Delegada de Protección de Datos de la Comunidad Autónoma de Euskadi de la reclamación recibida, y se le requirió para que en el plazo de quince días informara sobre el asunto y aportara cuanta documentación fuese relevante para su resolución.

TERCERO. - Con fecha 14 de septiembre de 2023 tiene entrada en esta Agencia Vasca de Protección de Datos escrito de la Delegada de Protección de Datos, al que se adjunta informe de la Dirección de Infraestructuras, Recursos y Tecnologías del Departamento de Educación del Gobierno Vasco.

En el escrito de la Delegada de Protección de Datos se aportaron las siguientes consideraciones:

"-- Respecto a las transferencias internacionales:

- Previo al 1 de septiembre de 2023, Google Cloud EMEA utilizaba como mecanismo de transferencias internacionales de datos las cláusulas contractuales tipo (CCTs) en conformidad con la decisión de la Comisión del 4 de junio del 2021. Dichas cláusulas estaban incorporadas en el contrato a través de la adenda de protección de datos.

- Desde el 1 de septiembre de 2023 Google incorpora a través de la adenda de protección de datos el EU-U.S. Data Privacy Framework como mecanismo de transferencias internacionales de datos. Dicha adenda se encuentra incorporada automáticamente a través del Convenio; dado que, tras la decisión de la Comisión del 10 de julio, Google procedió a actualizar sus cláusulas contractuales. Así, las transferencias que se realizan a Google LLC (entidad basada en Estados Unidos) desde Google Cloud EMEA (Irlanda) estarían avaladas por el nuevo EU-U.S. Data Privacy Framework.

- Si el EU-U.S. Data Privacy Framework se invalidara en un futuro, Google volvería a utilizar CCTs o adoptaría una solución de transferencia alternativa e informaría a los clientes en cualquier caso según lo exige la adenda de protección de datos.

-- Consta informe favorable de la Agencia Vasca de Protección de Datos, Dictamen D21-018 relativo al Convenio de colaboración entre la Administración General de la CAPV y Google para la utilización de los servicios Google Workspace".

Y en el informe de la Dirección de Infraestructuras, Recursos y Tecnologías del Departamento de Educación del Gobierno Vasco se realizan, en síntesis, las siguientes alegaciones:

- "*<u>Necesidad de dotar de un entorno de trabajo digital al alumnado</u>:*

  Los centros educativos llevan muchos años incorporando tecnología digital en el aula e incluso utilizando, en momentos concretos, las plataformas educativas en la nube, pero se trataba de un impulso que surgía exclusivamente desde el propio centro educativo en virtud de su propia autonomía pedagógica.

  Desde el año 2021, momento en el que iniciamos la tramitación del Convenio, desde todos los organismos educativos Estatales y Europeos se está impulsando la transformación digital en la escuela:

  La creación y compartición de recursos digitales (eje tercero) ya requiere la gestión de identidades para controlar la edición, la creación, la validación de los recursos, y los accesos por parte del alumnado según etapa educativa o la clase a la que pertenece.

  Además de ello, con todas las inversiones realizadas y las previstas para los próximos meses, todo el alumnado de primaria, secundaria y bachillerato va a asistir a aulas totalmente digitalizadas.

  Se está formando a los docentes y habrá nuevas metodologías educativas (ejes primero y cuarto).

  El alumnado va a trabajar con documentos digitales, proyectará sus trabajos en el panel digital del aula. Necesitan un espacio digital en la nube para la elaboración y entrega de los trabajos, con acceso tanto desde el aula como

desde casa, desde las bibliotecas o cualquier otra ubicación donde estudien. Tendrán que trabajar en grupo simultáneamente con los mismos documentos, a los que tendrán acceso ciertos alumnos y alumnas. Se trata de que logren la competencia digital (eje primero). Para ello, la gestión de identidades, grupos, permisos, y la elección de una plataforma educativa en la nube que sea segura es requisito necesario".

- Una vez argumentada la necesidad de dotar de un entorno de trabajo digital al alumnado, el informe explica los motivos de optar por Google Workspace for Education como plataforma educativa:

  "[…] Además de las consideraciones legales, para comparar diferentes plataformas educativas tenemos que tener en cuenta los siguientes aspectos:

  Existen los ataques externos, el uso inapropiado por parte de los usuarios, la seguridad del dispositivo que utiliza el alumnado, la seguridad de los propios servicios de Google y la propia configuración de seguridad de la plataforma.

  En general, consideramos que Google Workspace for Education en combinación con el portátil Chromebook es actualmente la opción más segura de todas las disponibles en un entorno educativo:

  El equipo Chromebook tiene un sistema operativo reducido al mínimo necesario. Por ello es el que tiene menos vectores de ataque. El equipo se actualiza en el arranque en cuestión de segundos. El usuario no puede deshabilitar las actualizaciones (si se ha establecido así en la configuración de la plataforma). Los documentos del alumnado no se almacenan en el dispositivo, se encuentran en la nube. No los pierden en caso de pérdida o robo del equipo. Para los ladrones es un equipo con poco interés ya que no podrán utilizarlo sin sustituirle elementos hardware […]

  En el caso de los ataques externos, de forma muy activa los servicios de Google evitan el spam (especialmente grave en menores), ofrecen protección contra phishing y software malicioso, analizan archivos adjuntos sospechosos, detectan enlaces ocultos, analiza contenido malicioso en imágenes enlazadas, avisa cuando considera que un dominio no es de confianza, protege contra spoofing, contra correos no autenticados, etc.

  Para controlar y reducir en la medida de lo posible el uso inapropiado, Google Workspace for Education dispone de una consola de gestión donde se restringen y limita el software o los servicios disponibles para cada grupo de usuarios. Los administradores del Departamento reciben alertas de seguridad. Pueden acceder a los informes de seguridad, ver el estado de la seguridad global, y se disponen herramientas de investigación de sucesos.

  Además del propio esfuerzo que realizan los técnicos de Google, la empresa mantiene un programa de recompensas por encontrar vulnerabilidades en su software, sistemas operativos, navegador, servicios, etc. El año 2022 abonaron 12 millones de dólares por la detección y resolución de 2.900 incidencias de seguridad.

- En cuanto a las transferencias internacionales, alega el Departamento de Educación que no están prohibidas, y que la reclamante no explicita cuál es el incumplimiento de la normativa de protección de datos: si se refiere a que Google incumple alguna de las condiciones firmadas para

las transferencias internacionales sin decir cuáles, o si considera que las cláusulas no son suficientes.

La Administración reclamada destaca que el artículo 46 del RGDP posibilita las transferencias internacionales a falta de decisión de la Comisión, siempre que el responsable hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas, y entre las garantías adecuadas que no requieren autorización expresa de la autoridad de control se encuentran las cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2 del RGPD. Y se remite a la Decisión de Ejecución (UE) 2021/914 de la Comisión, de 4 de junio de 2021, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el RGPD.

Asimismo, la Administración reclamada argumenta la aplicación del artículo 45 del RGPD (Transferencias internacionales basadas en una decisión de adecuación) tras la Decisión de la Comisión Europea de 10 de julio de 2023 en virtud de la cual se pueden realizar transferencias de datos personales a las organizaciones de EEUU incluidas en la lista de empresas participantes en DPF (Data Privacy Framework), sin necesidad de recurrir a las disposiciones del artículo 46, y sin que la Decisión tenga que ser complementada con cláusulas adicionales.

- Ante la afirmación de la parte reclamante de un elevado riesgo de uso indebido de los datos personales al involucrarse datos de carácter personal de personas menores de edad, la Administración reclamada alega que la reclamante no ha sustanciado ese uso indebido, y que el tratamiento de datos de menores no lo convierte en un uso indebido.

  La Administración reclamada analiza en distintos apartados las afirmaciones realizadas en este sentido por la parte reclamante:

  - Se afirma por la reclamante que hay varias Agencias de protección de datos europeas que han concluido que el paquete Google Workspace no cumple con el RGPD. La Administración reclamada argumenta que no se dice cuáles son esas Agencias, y sólo pone como ejemplo, la Autoridad danesa. Y en ese supuesto, la Administración reclamada matiza que la Autoridad danesa no prohibió el uso de productos de Google en Ayuntamientos y colegios de Dinamarca, sino que su actuación se refería únicamente a un municipio y fue en base a la documentación aportada, no a los productos de Google en sí mismos, sin que la prohibición de uso para el municipio concreto haya llegado a ser efectiva. Con la decisión de la Comisión Europea de 10 de julio de 2023, las transferencias de datos a EEUU que pudiera haber en los servicios de Google Workspace for Education están preautorizadas.

- En cuanto a la publicidad en el buscador de Google o en Youtube, la Administración reclamada afirma que no hay anuncios en los servicios incluidos de Google Workspace for Education que son objeto de convenio con Google. Además de ello, los alumnos y alumnas de primaria y secundaria, cuando se validan con los usuarios creados por el Departamento en Google Workspace for Education no reciben publicidad en el buscador de Google.

  La Administración reclamada afirma que Youtube es un servicio adicional que no es objeto del Convenio. El centro educativo puede habilitar el acceso para grupo de docentes o de alumnos/as de su centro si estima que es necesario para un fin educativo. En este servicio sí puede haber anuncios, pero no serían personalizados ni en primaria ni en secundaria.

- La cláusula 9.1 del Convenio se refiere al orden de preferencia en caso de algún conflicto en la interpretación del Convenio, y la Adenda de Tratamiento de Datos tiene la mayor preferencia, y aunque Google pudiese modificar unilateralmente la Adenda, los cambios no pueden tener repercusión en la seguridad, en el ámbito de aplicación, ni tendrían un efecto adverso material en los derechos de los usuarios.

- El punto 5.3 de la Adenda de Tratamiento de Datos se refiere a servicios adicionales ajenos al ámbito del Convenio. Si el centro educativo considera que para su propósito educativo es necesario habilitar un producto adicional de Google (instalación de software o habilitación de un servicio) que no está incluido en Google Workspace for Education, entonces podría decidir si lo habilita en la consola de administración de Google. Si el centro habilita el servicio adicional, el producto al que accede el usuario podría necesitar algunos datos suyos por motivos de interoperación entre productos de Google. Un ejemplo sería Youtube. Por ejemplo, este servicio requiere saber la edad del usuario para poder evitar la publicidad personalizada en menores de 16 años.

- La reclamante informa de una de las variantes de Google Workspace for Education, que ofrece la posibilidad de analizar documentos privados de los alumnos/as. La Administración reclamada argumenta que en la actualidad hay 4 variantes, siendo dos las que permiten hacer informes de originalidad, y que la edición objeto del Convenio es la básica denominada “Fundamentals”, que no permite la posibilidad de obtener dichos informes.

- La Administración reclamada expone que en base a todos los informes previos y al Dictamen de la Agencia Vasca de Protección de Datos de fecha 16 de septiembre de 2021, el Departamento de Educación continuó la tramitación del Convenio hasta la publicación del texto en el Boletín Oficial del País Vasco el 21 de abril de 2022.

- Por último, la Administración reclamada, expone, a modo de conclusiones, lo siguiente:

  "[…] (la parte reclamante) realiza una acusación genérica contra Google sin aportar dato alguno sobre la implementación de Google Workspace for Education en los centros públicos de Euskadi. Tampoco han aportado los artículos concretos que supuestamente se infringen. Sin embargo, llegan a la conclusión de que existe una brecha de seguridad.

  En ningún momento se ha puesto en contacto con el Departamento de Educación. No podemos revisar ninguna de las implementaciones ya que no citan ningún centro educativo concreto. Suponen que hemos habilitado todos los servicios de Google disponibles, pero no es así.

  No han aportado hechos ni incidencias ocurridas. Tampoco aporta ninguna brecha de seguridad de producto ni servicio alguno, ni evidencia alguna de ningún tipo. No ha realizado ninguna comparativa con otras plataformas educativas que podría ser un argumento para dejar de utilizar una para emplear otra más segura.

  Sin embargo, tras aportar una noticia con un titular falso, emitiendo sospechas de uso indebido por parte de Google, pero sin aportar ninguna evidencia de que se haya producido algo así en nuestros centros educativos, solicitan a la Agencia que abra un expediente sancionador contra el Departamento de Educación.

  Por nuestra parte solicitamos a la Agencia Vasca de Protección de Datos que tengan en cuenta este informe, y después de analizar la documentación aportada, proceda al archivo del expediente iniciado".

A este informe de la Dirección de Infraestructuras, Recursos y Tecnologías del Departamento de Educación del Gobierno Vasco se acompañó la documentación a que se hace referencia en el mismo, y la misma ha quedado incorporada al expediente.

CUARTO. - Con fecha 22 de noviembre de 2023, el Director de la Agencia Vasca de Protección de Datos dictó resolución acordando incoar procedimiento de infracción al Departamento de Educación del Gobierno Vasco por no haber realizado una evaluación de impacto relativo a la protección de datos personales asociada al tratamiento objeto de la reclamación, lo que puede suponer una infracción prevista en el artículo 83.4 a) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, (RGPD), y prevista asimismo en el artículo 73. t) de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

QUINTO. - El día 28 de noviembre de 2023, la Agencia notificó a la Administración reclamada el acuerdo de inicio del procedimiento de infracción, y con fecha 22 de diciembre de 2023, tiene entrada escrito de alegaciones de la Administración reclamada en la que se hace constar, entre otros, lo siguiente:

> "(…) *Los hechos que dan lugar a la denuncia por la que se inicia el procedimiento de infracción es la suscripción del "Convenio de colaboración entre Google Ireland Limited y el Gobierno Vasco para el uso de los servicios Workspace for Education por parte de los centros docentes y de apoyo de la Comunidad Autónoma del País Vasco".*

En dicho Acuerdo, entre otros aspectos, se resuelve iniciar el procedimiento de infracción al Departamento de Educación. El Fundamento de Derecho Segundo concreta la imputación, citando que «De la información y documentación aportada por la Administración reclamada, obrante en el expediente, no consta que se haya realizado una Evaluación de Impacto relativa a la protección de datos asociada al tratamiento objeto de reclamación en aplicación del artículo 35 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, (RGPD), lo que puede suponer una infracción prevista en el artículo 83.4 a) del mismo texto legal, y prevista asimismo en el artículo 73. t) de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)».

Si bien es verdad que en la tramitación del referido convenio no se realizó expresamente la evaluación de impacto relativa a la protección de datos contemplada en el artículo 35 del Reglamento General de Protección de Datos, entendiendo que el tratamiento podía entrañar riesgo, sí que se realizó la consulta previa recogida en el artículo 36.1 del mismo Reglamento: «el responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo».

Dicha consulta se realizó con fecha 22 de junio de 2021, tras la cual esa Agencia a la que me dirijo emitió el dictamen D21-018

(…)

No obstante, actualmente, dicho tratamiento de datos tiene realizada la evaluación de impacto referida en el artículo 35 del RGPD.

Por todo lo anterior, esta Administración estima fundada la no aplicación del artículo 83.5.a) del Reglamento General de Protección de Datos y el 73.t) de la LO 3/2018 de Protección de Datos Personales y garantía de los derechos digitales, por lo que se solicita de esa Agencia Vasca de Protección de Datos una resolución absolutoria en el procedimiento abierto y el archivo de las actuaciones".

A dicho escrito se acompañó informe de evaluación de impacto en la protección de datos (EIPD): "*Plataforma Google Workspace (GWS) del Departamento de Educación del Gobierno Vasco*" de fecha 21 de diciembre de 2023, que en su apartado XI establece:

"En base a los resultados obtenidos en términos de riesgo residual para los derechos y libertades de los interesados, la conclusión de la evaluación de impacto es favorable y se considera que el riesgo residual, tras aplicar las medidas, es aceptable".

La evaluación de impacto describe el proyecto en su apartado I en los siguientes términos:

"El proyecto consiste en la puesta a disposición de los centros escolares dependientes del Departamento de Educación, y por consiguiente de su personal docente y alumnado, de la plataforma "Google Workspace for Education", un paquete de herramientas diseñado para permitir que los educadores y los alumnos innoven y aprendan juntos, ya que pueden compartir un espacio seguro y común para trabajar y transferir datos.

El Departamento de Educación pretende facilitar a los centros docentes y de apoyo de la Comunidad Autónoma del País Vasco (CAPV) el acceso a servicios y herramientas adecuadas para poder impartir clases de forma total o parcialmente telemática, tanto para docentes como para el alumnado. Para ello, acude a una plataforma ya

consolidada en el mercado1, como es "Google Workspace for Education", basada en almacenamiento y computación "en la nube".

Los responsables de los tratamientos de datos (a quienes en conjunto podremos referirnos, en este informe, como Departamento de Educación del Gobierno Vasco) realizados dentro de la plataforma son:

- *Viceconsejería de Educación: Determina los fines del tratamiento: DOCUMENTO DE ACTIVIDAD EDUCATIVA (DAE).*
- *Dirección de Centros y Planificación: Determina los fines del tratamiento: ADMISIÓN Y MATRÍCULA DE ALUMNADO DE CENTROS ESCOLARES.*
- *Dirección de Planificación y Organización: Determina los fines del tratamiento: ADMISIÓN Y MATRÍCULA DE ALUMNADO DE CICLOS FORMATIVOS DE FORMACIÓN PROFESIONAL.*
- *Dirección de Gestión de Personal: Determina los fines del tratamiento: GESTIÓN DE PERSONAL.*
- *Dirección de Infraestructuras, Recursos y Tecnologías: Determina los medios corporativos dispuestos para realizar total o parcialmente dichos tratamientos de datos. En concreto: Plataforma Google Workspace GWS.*

Como encargados del tratamiento en este sistema figuran:

- *EJIE, la Sociedad Informática del Gobierno Vasco.*
- *GOOGLE CLOUD EMEA LIMITED ("Google"), sociedad constituida de conformidad con la legislación irlandesa, con domicilio social en 70 Sir John Rogerson's Quay, Dublin 2, Irlanda.*

El alberge de los datos se produce en servidores de Google, ubicados en el Espacio Económico Europeo (EEE) y en EE.UU, y, aunque el Gobierno Vasco pierde en parte el control de los datos al encargar su tratamiento a Google, este país actualmente cuenta con una Decisión de Adecuación de la Comisión Europea en materia de protección de datos personales que equipara su nivel de protección al de cualquier estado miembro de la Unión Europea [COMMISSION IMPLEMENTING DECISION of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework].

Respecto a las conclusiones del análisis de necesidad, idoneidad y proporcionalidad del tratamiento y de las bases jurídicas que legitiman el tratamiento de los datos, los datos requeridos en el sistema son los mínimos datos necesarios para lograr los objetivos pretendidos: la transformación digital de la educación, y la adaptación de los sistemas y recursos informáticos del sistema educativo a las exigencias de la sociedad de la información.

Para lograr de otra forma los fines previstos, bien pudiera utilizarse una plataforma similar a la que es objeto de esta Evaluación de Impacto, Google Workspace, sin embargo probablemente los costes derivados de su utilización serían más elevados. Además, la curva de aprendizaje de la plataforma sería bastante mayor tanto para el profesorado como para el alumnado.

Según el análisis del contexto descrito anteriormente, se obtienen más ventajas o beneficios, que desventajas pudieran existir, ya que el sistema propuesto contribuye al desarrollo de las competencias de estas áreas del Departamento de Educación, lo

cual repercute positivamente tanto en el sistema educativo, y en consecuencia, sobre alumnado y personal, como en la sociedad".

A destacar en la Evaluación de Impacto aportada, el apartado VII sobre identificación y análisis de los factores de riesgo, que en su apartado A, precisa lo siguiente:

"(…) Por último, en cuanto a posibles riesgos de incumplimiento:

- El Registro de Actividades de Tratamiento de los Responsables de Tratamiento ***no contiene la información necesaria respecto al sistema analizado*** *(por ejemplo, metadatos de las comunicaciones electrónicas y los contenidos inespecíficos derivados de las actividades docentes). La mitigación consiste en actualizar el RAT con la información pertinente.*

- Incorporación tardía de los expertos en protección de datos (en particular, de la delegada de protección de datos) al proyecto. La mitigación consiste en atender las indicaciones de la Delegada de Protección de Datos y corregir la situación generada.

- Dificultades para comprobar o supervisar que el encargado y los subcontratistas cumplen las instrucciones y, especialmente, las medidas de seguridad. El nivel de riesgo es medio. La mitigación consiste en establecer acuerdos de nivel de servicio y controles periódicos".

Revisado el Registro de Actividades de Tratamiento del Departamento de Educación, que aparece publicado en la página web del Gobierno Vasco:

https://www.euskadi.eus/web01-aprat/es/ac34aRatWebWar/control/arbol?locale=es

En los diferentes registros dependientes de dicho Departamento, entre ellos, a los que se alude por la Administración reclamada en la evaluación de impacto, no se encuentra referencia alguna al tratamiento de datos personales del alumnado y docentes que supone la puesta en práctica de la plataforma educativa Google Workspace For Education (transferencias internacionales, comunicación/cesión de datos personales, finalidades, base jurídica, etc):

- Admisión y matrícula de alumnado de centros escolares
- Admisión y matrícula de alumnado de ciclos formativos de Formación Profesional
- Alumnado con necesidades específicas de apoyo educativo
- Gestión de personal

SEXTO. - Con fecha 4 de marzo de 2024, por el instructor del procedimiento se adoptó propuesta de resolución en el sentido de apercibir al Departamento de Educación del Gobierno Vasco por haber infringido el artículo 35 del RGPD, lo que constituye una infracción prevista en el artículo 83.4.a) del RGPD; por haber infringido el principio de lealtad y transparencia proclamado en el artículo 5.1.a) del RGPD, lo que constituye una infracción prevista en el artículo 83.5.a) del mismo texto legal; y asimismo, por haber infringido el artículo 30 del RGPD y el artículo 30 de la LOPDGDD, lo que constituye una infracción prevista en el artículo 83.4 a) del RGPD y en el artículo 74 l) de la LOPDGDD.

SÉPTIMO. - Con fecha 6 de marzo de 2024 se notificó dicha propuesta de resolución a la Administración reclamada, no habiendo presentado a esta fecha alegaciones a la misma.

HECHOS PROBADOS

De las actuaciones y documentos que obran en el expediente resulta acreditado que:

- Que el Gobierno Vasco, a través del Departamento de Educación, y Google suscribieron un convenio para la utilización de los servicios Google WorkSpace For Education en los centros docentes del Departamento de Educación, y que para su implementación la Administración reclamada no realizó una evaluación de impacto relativa a la protección de datos.
- Los datos personales de los usuarios finales de la plataforma (docentes y alumnado) pueden ser tratados por Google para el uso de servicios adicionales que no son objeto del Convenio.
- En los distintos registros de actividades tratamiento dependientes del Departamento de Educación publicados en la página web del Gobierno Vasco, no consta información en la que se prevea el tratamiento de datos personales que supone la ejecución de la citada plataforma educativa.

FUNDAMENTOS DE DERECHO

I

Se formula la presente Resolución de acuerdo con lo previsto en el artículo 39 de la Ley 16/2023, de 21 de diciembre, de la Autoridad Vasca de Protección de Datos en relación con el artículo 44 de la Ley 1/2023, de 16 de marzo, de la potestad sancionadora de las Administraciones Públicas Vascas.

II

Hay que partir de la consideración de que en la propuesta de resolución se dio respuesta detallada a todas y cada una de las alegaciones presentadas por la Administración reclamada al acuerdo de iniciación, y que se justificó convenientemente que, a la vista de los hechos declarados probados, los mismos han infringido los artículos 35, 5.1 a) y 30 del RGPD, y el artículo 30 de la LOPDGDD, conductas constitutivas de las infracciones previstas en los artículos 83.4.a), 83.5.a) y artículo 74 l) de la LOPDGDD.

Ante la ausencia de alegaciones a la propuesta de resolución, esta Autoridad se reitera en la argumentación jurídica que consta en ella.

La puesta en marcha de la plataforma educativa “Google Workspace For Education” regulada en el Convenio firmado entre la Administración reclamada y Google supone el tratamiento en un entorno digital de datos personales tanto del alumnado como del personal docente de los centros públicos escolares y de ciclos formativos de formación profesional de la Comunidad Autónoma del País Vasco, y que según reconoce la Administración reclamada, pueden llegar a ser en total unas 400.000 personas. El alumnado es menor de edad, y parte del mismo, menor de 14 años.

Ese tratamiento está sometido a los principios y preceptos del RGPD y de la LOPDGDD y a la normativa sectorial aplicable en materia educativa.

El artículo 35 del RGPD dedicado a la "Evaluación de impacto relativa a la protección de datos" establece:

> *"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.*
>
> *2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.*
>
> *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*
>
> *c) observación sistemática a gran escala de una zona de acceso público.*
>
> *4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68. (…)".*

En aplicación de lo dispuesto en el apartado 4 del artículo 35 del RGPD, la Agencia Vasca de Protección de Datos junto con la Agencia Española de Protección de Datos publicaron una lista orientativa de tipos de tratamiento que requieren una evaluación de impacto relativa a la protección de datos, entre los que se encuentran:

- Tratamientos que impliquen el uso de datos a gran escala.
- Tratamientos de datos de sujetos vulnerables o en riesgo de exclusión social, incluyendo **datos de menores de 14 años**, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes y personas que estén bajo su guardia y custodia.
- Tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas.

La implementación de la plataforma educativa adoptada por la Administración reclamada y regulada en el citado convenio abarcaría, al menos, los tres tipos de tratamiento citados, al tratar datos personales a gran escala de colectivos especialmente vulnerables, como es el

alumnado, menores de edad, y parte de él, menores de catorce años, tratamientos que implican la utilización de nuevas tecnologías como son las herramientas digitales.

En las alegaciones al acuerdo de inicio anteriormente reseñadas, la Administración reclamada reconoció que no se realizó evaluación de impacto relativa a la protección de datos en la tramitación de dicho convenio, pero que sí se realizó la consulta previa del artículo 36.1 del RGPD.

El artículo 36.1 del RGPD prevé la consulta previa a la autoridad de control antes de proceder al tratamiento cuando una **evaluación de impacto** relativa a la protección de datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo. Es decir, la consulta previa del artículo 36.1 requiere la realización previa de una evaluación de impacto, presupuesto que, como reconoce la propia Administración, no se dio cuando consultaron a esta Autoridad.

Por ello, siendo así que la realización de la evaluación de impacto era obligatoria y la misma no se realizó, como así lo reconoce la Administración reclamada, se ha infringido la obligación contenida en el artículo 35 del RGPD.

En cuanto a la Evaluación de Impacto en la Protección de Datos (EIPD) remitida por el Departamento de Educación junto con las alegaciones al Acuerdo de Inicio del procedimiento de infracción, y realizada con posterioridad al mismo, pasamos a hacer las siguientes consideraciones:

En las EIPD, cuando proceda, el responsable recabará la opinión de las personas interesadas 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. En el caso que nos ocupa, no se ha considerado, por parte del responsable del tratamiento, el Departamento de Educación, recabar la opinión de las personas interesadas o sus representantes.

La EIPD debe contemplar, entre otras cosas, una descripción sistemática de las operaciones de tratamiento previstas, los fines del tratamiento, así como la base jurídica que ampare el tratamiento.

A esta fecha, y como se indicará en el siguiente Fundamento, en el Registro de Actividades de Tratamiento (RAT) del Departamento de Educación, no existe un tratamiento que contemple la utilización específica de la plataforma educativa “Google Workspace for Education (GWS)”, si bien, en la EIPD del Departamento de Educación que estamos analizando se apunta:

> *“Mediante la plataforma educativa GWS no se tratarán nuevos datos con respecto a los que ya se estaban tratando previamente y que están catalogados en el Registro de Actividades de Tratamiento del Departamento de Educación, salvo ciertos metadatos”.*

Se entiende que el tratamiento referido al uso de la plataforma educativa GWS tiene la suficiente envergadura como para que se registre en el RAT del Departamento de Educación del Gobierno Vasco. Si bien en el plan de acción de la gestión de riesgos del EIPD aportado por el Departamento de Educación, en las alegaciones al acuerdo de inicio, se incluye, como medida de cumplimiento, “actualizar el RAT con la información pertinente”; esto es, incluir este tratamiento, el uso de la plataforma educativa GWS, en el RAT del Departamento de Educación.

El RAT debe de entenderse como parte de la descripción básica e inicial del tratamiento y como un activo de base en para la gestión del riesgo o el proceso de gestión de los tratamientos, y como la EIPD, cualquier tratamiento debe de registrarse antes de iniciar dicho tratamiento.

La EIPD debe contemplar también una evaluación de los riesgos para los derechos y libertades de los interesados; en la EIPD presentada por el Departamento de Educación esta evaluación de riesgos no se ha presentado (se hace referencia a un fichero adjunto en formato Excel: ARDyL_GWS_v1.0.xlsx, que no se ha adjuntado). Al existir, dentro de los datos personales tratados en un entorno digital de plataformas colaborativas y servicios de redes sociales, datos de menores de edad, deberían incluirse medidas de protección frente a las posibles amenazas que se puedan materializar (a tener en cuenta que el tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años).

Los plazos para comunicar los incidentes de seguridad (incluidas las brechas o quiebras de seguridad que afecten a datos personales) pueden ser superiores a 72 horas, ya que no existe un compromiso en el Convenio para notificar al Departamento de Educación del Gobierno Vasco las quiebras de seguridad que afecten a datos personales en un plazo máximo de 72 horas, y sólo dice que "el personal de seguridad de Google reaccionará rápidamente a los incidentes de seguridad".

Llama la atención que en la Evaluación de Impacto remitida se contemple dentro de los controles para la reducción del riesgo (Apartado IX) la implicación de la Delegada de Protección de Datos en los procedimientos de decisión y definición de los tratamientos, y que en dicha Evaluación no se haya incluido, por entender que **"no procede"**, ni la visión de la DPD ni las conclusiones y recomendaciones de la DPD a los responsables.

El RGPD en su artículo 35.2 establece claramente que "*el responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos*".

III

Un aspecto fundamental que destacar de la reclamación planteada es la referida al tratamiento de los datos personales que puede realizar Google, como encargada del tratamiento, para el uso tanto de servicios principales como de servicios adicionales, quedando estos últimos fuera del ámbito de la plataforma educativa y, por tanto, del Convenio.

En cuanto a los servicios en que se concreta la plataforma educativa debe precisarse que a la vista del Convenio y sus Anexos (Términos del servicio y Adenda de tratamiento de datos) existen productos o servicios principales y productos o servicios adicionales, sin que los mismos se hallen definidos y determinados en el citado Convenio.

La definición de dichos servicios se encuentra en otros lugares externos al Convenio, como la página web de Google en la que se refiere a Google Workspace.

Los servicios principales aparecen concretados en un apartado de dicha web denominado "Resumen de Servicios" y se ofrece una breve explicación de para qué sirven. En este

mismo sentido, aparecen en la evaluación de impacto aportada al presente expediente tras el acuerdo de inicio de procedimiento de infracción.

En el sitio "Resumen de Servicios" de la página web workspace.google.com se refieren a los productos adicionales, indicando expresamente lo siguiente:

> *"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".*

Los Anexos del Convenio se refieren a los servicios o productos adicionales para dejarlos fuera de la plataforma educativa Google Workspace for Education:

- *"Anexo I Términos del Servicio (…) 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 2 Adenda de tratamiento 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".*

Tal y como se ha hecho constar en los antecedentes, la Administración reclamada informó a requerimiento de esta Autoridad lo siguiente:

> *"El punto 5.3 se refiere a servicios adicionales* ***ajenos*** *al ámbito del Convenio. Si el centro educativo considera que para su propósito educativo es necesario habilitar un producto adicional de Google (instalación de software o habilitación de un servicio) que no está incluido en Google Workspace for Education, entonces podría decidir si lo habilita en la consola de administración de Google.*
>
> *Si el centro habilita el servicio adicional, el producto al que accede el* ***usuario podría necesitar algunos datos suyos por motivos de interoperación entre productos de Google****. Un ejemplo sería Youtube. Por ejemplo, este servicio requiere saber la edad del usuario para poder evitar la publicidad personalizada en menores de 16 años".*

Los productos adicionales 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 16 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 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 la plataforma educativa Google Workspace for Education.

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

Y además, los servicios adicionales, una vez habilitados por considerar el centro educativo que pueden servir a un fin educativo, pueden tener otras finalidades que se escapan del ámbito del Convenio y de la plataforma educativa Google Workspace for Education, y que por tanto no quedan determinadas.

A esto se añade, como reconoce la propia Administración reclamada, que determinados servicios adicionales (Youtube) incluyen publicidad, aunque no personalizada para menores de 16 años.

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 a los principios de lealtad y transparencia (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; circunstancia que no se produce a la vista de lo anteriormente expuesto con la consiguiente vulneración de los citados principios de lealtad y transparencia.

Y esta falta de información, a su vez, se ha visto reflejada, como ya hemos indicado, en la falta de constancia a esta fecha de actividades de tratamiento de datos personales que se deriven del desarrollo de la plataforma educativa en los registros de actividades publicados en la web del Gobierno Vasco (https://www.euskadi.eus/web01-aprat/es/ac34aRatWebWar/control/arbol?locale=es).

En virtud del artículo 31.4 de la LOPDGDD, la Administración reclamada está obligada a **hacer público** el inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del RGPD y su base legal.

Según el artículo 30 del RGPD, dicha información es la siguiente:

a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;

b) los **fines del tratamiento**;

c) una descripción de las categorías de interesados y de las **categorías de datos personales**;

d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;

e) en su caso, **las transferencias de datos personales a un tercer país** o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;

f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;

g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

Aspectos fundamentales como las categorías de datos, finalidades, transferencias internacionales, que se derivan del uso de la plataforma educativa Google Workspace for Education, no constaban a la fecha de la propuesta de resolución en los registros de actividades de tratamiento del Departamento de Educación publicados en la página web correspondiente del Gobierno Vasco, lo que supone una infracción del artículo 30 del RGPD y del artículo 30 de la LOPDGDD, tipificadas en el artículo 83.4 a) del RGPD y en el artículo 74 l) de la LOPDGDD.

A la fecha de la presente resolución, la página web del Gobierno vasco que hace públicos los registros de actividades de tratamiento del Departamento de Educación, dentro de la Dirección de Aprendizaje e Innovación Educativa, tiene publicado un registro denominado "*Uso de plataformas educativas propias del Departamento de Educación*" (https://www.euskadi.eus/web01-aprat/es/ac34aRatWebWar/control/fichaRat/1590).

La referencia a plataformas educativas "*propias*" y la no previsión de transferencias internacionales de datos parece que no se corresponde con las herramientas educativas a las que se refiere el Convenio firmado entre Google y el Departamento de Educación.

A la vista de lo anteriormente expuesto, se hace necesario por parte del responsable del tratamiento concretar aspectos fundamentales del tratamiento de datos personales que se derivan de la plataforma educativa y que se vean trasladados al Convenio, como son los servicios principales y adicionales, los datos personales que se tratan, las finalidades concretas y la bases jurídicas de los diferentes tratamientos para así dar cumplimiento a los principios de lealtad y transparencia consagrados en el artículo 5.1 a) del RGPD.

IV

Por todo lo cual, vistos los preceptos citados, la Ley 1/2023, de 16 de marzo, de la potestad sancionadora de las Administraciones Públicas Vascas, y demás normativa de general y pertinente aplicación, el Presidente de la Autoridad Vasca de Protección de Datos

RESUELVE

PRIMERO. - Apercibir al Departamento de Educación por haber infringido el artículo 35 del RGPD, lo que constituye una infracción prevista en el artículo 83.4.a) del mismo texto legal.

SEGUNDO. - Apercibir al Departamento de Educación por haber infringido el principio de lealtad y transparencia proclamado en el artículo 5.1.a) del RGPD, lo que constituye una infracción prevista en el artículo 83.5.a) del mismo texto legal

TERCERO. - Apercibir al Departamento de Educación por haber infringido el artículo 30 del RGPD y el artículo 30 de la LOPDGDD, lo que constituye una infracción prevista en el artículo 83.4 a) del RGPD y en el artículo 74 l) de la LOPDGDD.

CUARTO.- Requerir al responsable del tratamiento para que adopte las medidas organizativas necesarias para dar cumplimiento a los principios de lealtad y transparencia, así como a la obligación de hacer público el inventario de actividades de tratamiento en los términos recogidos en el artículo 30 de la LOPDGDD, y para que notifique a la Autoridad Vasca de Protección de Datos dichas medidas en el plazo de un mes desde la notificación de la resolución.

QUINTO. - Notificar la presente resolución a la parte reclamante y al Departamento de Educación del Gobierno Vasco.

SEXTO. - Comunicar la presente resolución al Ararteko de conformidad con lo establecido en el artículo 28.8 de la 16/2023, de 21 de diciembre, de la Autoridad Vasca de Protección de Datos.

La presente resolución agota la vía administrativa y frente a la misma podrán las partes interponer recurso potestativo de reposición ante el Presidente de la Autoridad Vasca de Protección de Datos en el plazo de un mes a contar desde el día siguiente al de su notificación (artículos 123 y 124 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las Administraciones Públicas), o directamente recurso contencioso-administrativo ante el Juzgado de lo contencioso-administrativo en el plazo de dos meses contados desde el día siguiente al de la notificación de este acto (artículos 8.3 y 46 de la Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso-Administrativa).

En Vitoria - Gasteiz, a 9 de mayo de 2024