- **N/Ref.: E/01659/2020**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad RIDE HIVE OPERATIONS S.L y teniendo como base los siguientes:

HECHOS

PRIMERO: El día 14 de enero de 2020, se recibió un escrito de notificación de brecha de seguridad de los datos personales remitido por RIDE HIVE OPERATIONS, S.L. (en adelante, HIVE), en el que informaba a la Agencia Española de Protección de Datos que, con fecha 9 de enero de 2020, la empresa ******EMPRESA.1*** les había notificado que ***(…)*** había sido publicada en internet. ***(…)***.

Los datos a los que se podían tener acceso correspondían a datos básicos y de contacto de aproximadamente 65.0000 clientes (195.000 registros afectados) y, aunque la notificación se había realizado ante la Agencia Española de Protección de Datos, podía haber usuarios de Austria, Grecia, Italia, Polonia y Portugal.

HIVE manifestaba que no se iba a comunicar la brecha a los interesados por bajo riesgo.

Asimismo, manifestaba que se había intentado la notificación a la Agencia el día 12 de enero, pero al presentar problemas técnicos se remitió la notificación a la dirección incidencias@aepd.es.

SEGUNDO: Con fecha 17 de febrero de 2020, la Directora de la Agencia Española de Protección de Datos ordenó a la subdirección General de Inspección de Datos realizar las oportunas investigaciones previas con el fin de determinar una posible vulneración de la normativa de protección de datos.

A través del "Sistema de Información del Mercado Interior" (en lo sucesivo IMI), regulado por el Reglamento (UE) nº 1024/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012 (Reglamento IMI), cuyo objetivo es favorecer la cooperación administrativa transfronteriza, la asistencia mutua entre los Estados miembros y el intercambio de información, con fecha 27 de febrero de 2020 esta Agencia se declaró Autoridad principal en el presente asunto.

Según las informaciones incorporadas al Sistema IMI, de conformidad con lo establecido en el artículo 60 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27/04/2016, 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 (en adelante, RGPD), actúan en calidad de "autoridad de control interesada" la autoridad de control de Austria, la autoridad alemana de Hamburgo, la autoridad de control de Italia y la de Portugal.

TERCERO: A la vista de los hechos expuestos, la Subdirección General de Inspección de Datos procedió a realizar actuaciones para su esclarecimiento, al amparo de los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 del RGPD, constatando lo siguiente:

Tal y como consta en el Registro Mercantil, la empresa RIDE HIVE OPERATIONS SL tiene por objeto social "el desarrollo, la facilitación y la comercialización de servicios de micromovilidad y de productos, servicios generales y servicios en el ámbito de los nuevos medios de comunicación…".

En relación con la empresa HIVE, en internet figura que "Daimler, que es el mayor accionista del que fuera MyTaxi, se alió con BMW para crear una nueva plataforma de movilidad urbana. Firmaron, en marzo de 2018, un acuerdo de colaboración para fusionar sus servicios de movilidad DriveNow y car2go y ahora MyTaxi es Free Now, una plataforma que ofrece desde servicios de taxi hasta transporte público pasando patinetes eléctricos compartidos. Entre sus activos se encuentra HIVE, una joven compañía de patinetes que ha instalado su campamento base en Barcelona".

HIVE ha ubicado en Barcelona su sede europea y de apoyo de estructura y estrategia a todos los países donde opera: Portugal, Grecia, Austria, Francia, Polonia y Bélgica y España.

Por su parte, en la web de ******EMPRESA.1*** figura que la empresa ofrece una plataforma tecnológica, información y un método para conectar conductores y pasajeros y no proporciona ningún servicio de transporte.

Con fecha 3 de marzo de 2020 se solicitó información a RIDE HIVE OPERATIONS SL y de la respuesta recibida se desprende lo siguiente:

Respecto de la empresa

HIVE y ******EMPRESA.1*** se encuentran vinculados comercialmente desde el 6 de noviembre de 2018.

La relación laboral se basa en un contrato de fecha 6 de noviembre de 2018, suscrito entre ******EMPRESA.1*** y MyTaxi Unipessoal Lda. que se encuentra vinculada a HIVE por ser ambas subsidiarias de la misma empresa holding y motivado por que en el momento de suscribir el contrato HIVE no estaba aún constituida por lo que comenzó a operar Mytaxi Unipessoal, Lda. en su nombre en Portugal. Al contrato se le ha incorporado un acuerdo de cooperación en la prestación de servicios de movilidad, así como también un acuerdo de responsabilidad en el manejo y control de los datos personales con Ride Hive Unipessoal, Lda. en Portugal, compañía que se encuentra participada en un 100% por Ride Hive Operations, SLU.

Ambas entidades van a suscribir un nuevo acuerdo marco para incluir a todas las empresas de Ride Hive Operations, SLU.

Ride Hive Operations, SLU ha aportado copia de los documentos mencionados como Adjuntos 1 y 2.

Respecto del Sistema de Información

- El sistema de intercambio de ******EMPRESA.1*** utiliza datos personales de los clientes para proporcionar un servicio de alquiler a demanda. Los clientes pueden registrarse una vez y alquilar los vehículos a través de la aplicación móvil. Después de la realización del viaje, el cliente realizará el abono a través del sistema.

- ******EMPRESA.1*** proporciona el software, pero los datos son propiedad del operador de intercambio HIVE.

  (…)

Respecto de la cronología de los hechos. Medidas de minimización del impacto de la brecha de seguridad

- El 9 de enero de 2020 a las 13:30, ******EMPRESA.1*** informó a HIVE del incidente de seguridad ya que un tercero ***(…)*** les había indicado que había descubierto que ***(…).***

- El 11 de enero se ***(…)***.

- El día 12 de enero, el tercero confirmó el acceso a los datos de ***(…),*** pero informó que no se descargaron ni se compartieron.

  Se notificó la incidencia a la Agencia Española de Protección de Datos, la cual fue remitida por correo electrónico después de contactar con la propia Agencia, al no poder presentarse electrónicamente, y el día 14 se presentó finalmente a través de la sede. A este respecto, han aportado impresión de pantalla de la Sede Electrónica de la Agencia de fecha 13 de enero de 2020 donde se indica un error de “Servidor no disponible”.

- El 27 de enero se ***(…).***

Respecto de las causas que hicieron posible la brecha de seguridad

- HIVE manifestó que el motivo por el cual se produjo la incidencia fue debido a que ***(…)***.

- HIVE manifestó que después de la investigación realizada como consecuencia de la incidencia consideran que ***(…)***.

Respecto de los datos afectados

- HIVE manifestó que no hubo clientes afectados y que los clientes potenciales afectados fueron 668.483.

- También manifestó que los datos de los clientes corresponden con datos descriptivos de los viajes realizados con HIVE y la información relacionada con la solicitud del viaje y que no se va a comunicar la incidencia ya que no ha habido clientes afectados.

- El tercero informó ***(…)***, y confirmó que los datos del usuario no se descargaron ni compartieron.

Respecto de las medidas de seguridad implantadas con anterioridad a la brecha de seguridad

- ***(…)***

Respecto de las medidas implementadas con posterioridad a la brecha de seguridad

- ***(…)***

CUARTO: Siguiendo el proceso establecido en el artículo 60 del RGPD, el 13/04/2021 se subió al sistema IMI proyecto de resolución de archivo de actuaciones y se les hizo saber a las autoridades de control interesadas que tenían cuatro semanas desde la consulta para formular objeciones pertinentes y motivadas. Transcurrido el plazo a tal efecto, ninguna autoridad de control formuló objeción alguna en los términos del artículo 60 del RGPD.

FUNDAMENTOS DE DERECHO

I – Competencia

De acuerdo con lo dispuesto en el artículo 60.8 del RGPD, es competente para adoptar esta resolución la Directora de la Agencia Española de Protección de Datos, de conformidad con el artículo 12.2, apartado i) del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos (en adelante, RD 428/1993) y la Disposición transitoria primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo, LOPDGDD).

II - Sistema de Información del Mercado Interior (IMI)

El Sistema de Información del Mercado Interior se encuentra regulado por el Reglamento (UE) nº 1024/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012 (Reglamento IMI), y su objetivo es favorecer la cooperación administrativa transfronteriza, la asistencia mutua entre los Estados miembros y el intercambio de información.

III - Establecimiento principal, tratamiento transfronterizo y autoridad de control principal

El artículo 4.16 del RGPD define «establecimiento principal»:

"a) en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal;

b) en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento"

Por su parte el artículo 4.23 del RGPD considera «tratamiento transfronterizo»:

"a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro,

o b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro"

El RGPD dispone, en su artículo 56.1, para los casos de tratamientos transfronterizos, previstos en su artículo 4.23), en relación con la competencia de la autoridad de control principal, que, sin perjuicio de lo dispuesto en el artículo 55, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado con arreglo al procedimiento establecido en el artículo 60.

En el caso examinado, como se ha expuesto, HIVE tiene su establecimiento principal en España, por lo que la Agencia Española de Protección de Datos es la competente para actuar como autoridad de control principal.

IV - Autoridad de control interesada

De conformidad con lo dispuesto en el artículo 4.22) del RGPD, es Autoridad de control interesada, la autoridad de control a la que afecta el tratamiento de datos personales debido a que:

a.- El responsable o encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control;

b.- Los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o

c.- Se ha presentado una reclamación ante esa autoridad de control.

En el presente procedimiento actúan en calidad de “autoridad de control interesada” la autoridad de control de Austria, la autoridad alemana de Hamburgo, la autoridad de control de Italia y la de Portugal.

V - Procedimiento de cooperación y coherencia

En este caso se ha seguido en la tramitación de la notificación de la brecha de seguridad de datos personales el procedimiento previsto en el artículo 60 del RGPD, que dispone en sus apartados 3 y 8, lo siguiente:

“*3. La autoridad de control principal comunicará sin dilación a las demás autoridades de control interesadas la información pertinente a este respecto. Transmitirá sin dilación un proyecto de decisión a las demás autoridades de control interesadas para obtener su dictamen al respecto y tendrá debidamente en cuenta sus puntos de vista.*”

“8*. No obstante lo dispuesto en el apartado 7, cuando se desestime o rechace una reclamación, la autoridad de control ante la que se haya presentado adoptará la decisión, la notificará al reclamante e informará de ello al responsable del tratamiento.”*

VI - Cuestión tramitada y razonamientos jurídicos

En este caso, la Agencia Española de Protección de Datos ha tramitado la notificación de la brecha de seguridad de datos personales de HIVE, por una presunta vulneración del artículo 32 RGPD.

El resultado de las actuaciones ha sido reflejado en el Hecho tercero.

El RGPD define, de un modo amplio, las “violaciones de seguridad de los datos personales” (en adelante quiebra de seguridad) como “*todas aquellas violaciones de la seguridad que ocasionen 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.*”

En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una posible brecha de confidencialidad, como consecuencia del posible acceso indebido por terceros ajenos a la base de datos de HIVE.

De las actuaciones de investigación se desprende que HIVE disponía de razonables medidas técnicas y organizativas preventivas a fin de evitar este tipo de incidencias y acordes con el nivel de riesgo.

Asimismo, HIVE ha afrontado de forma diligente la identificación y corrección de la brecha, análisis y clasificación del supuesto incidente de seguridad de datos

personales así como la diligente reacción ante la misma al objeto de notificar, minimizar el impacto e implementar nuevas medidas razonables y proporcionales para evitar que se repita la supuesta incidencia en el futuro.
No constan reclamaciones ante esta AEPD por parte de los clientes afectados.

No obstante, teniendo en cuenta la no implementación de la metodología del doble factor de autenticación y el error humano que llevó a esta brecha de seguridad, se recomienda considerar la adopción de las siguientes medidas:

a) Definir de forma clara las políticas que rigen la compartición de información entre HIVE y ******EMPRESA.1***, centrándose necesariamente en las cuestiones técnicas de seguridad de la información, ***(…);***

b) Llevar a cabo acciones de formación para empoderar a los interlocutores que operan los mecanismos de compartición implementados, de acuerdo con las políticas definidas y los eventuales procedimientos internos, mostrándoles los errores más comunes que potencialmente podrían llevar a brechas de seguridad de protección de datos;

c) Implementar rutinas de análisis de vulnerabilidades de seguridad diseñadas para identificar, analizar, mitigar y proveer protección adicional contra amenazas conocidas, virus, código malicioso y debilidades documentadas, a fin de fortalecer y aumentar el nivel de protección de los sistemas existentes;

d) Y, finalmente, implementar acciones de formación, *centradas específicamente en mecanismos de interoperabilidad de sistemas, con el objetivo de cimentar buenas prácticas sobre el desarrollo de las APIs y la gestión y protección de las claves API (Claves API) en los contextos más diversos.*

En consecuencia, por todo lo expuesto, se considera que la actuación de HIVE, como entidad responsable del tratamiento, ha sido acorde con la normativa sobre protección de datos personales y que no procede el inicio de un procedimiento sancionador al haber implantado nuevas medidas de seguridad proporcionales al riesgo evaluado para evitar la repetición de incidentes similares en el futuro, por lo que se procede a acordar el archivo de las actuaciones realizadas.

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos
SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las actuaciones realizadas contra RIDE HIVE OPERATIONS S.L.

SEGUNDO: NOTIFICAR la presente resolución a RIDE HIVE OPERATIONS S.L. con NIF B67374991.

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

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

1131-310820

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