- **Expediente N.º: EXP202316010**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: Con fecha 17 de octubre de 2023, la empresa ***23ANDME, INC*** (en adelante, 23ANDME), con domicilio en ***349 OYSTER POINT BLVD - 94080 SOUTH SAN FRANCISCO - CALIFORNIA*** notificó a esta Agencia una brecha de seguridad en la que se habría producido una violación de la seguridad de los datos personales.

De acuerdo con la comunicación de la brecha, realizada por la empresa Greenberg Traurig, LLP (en adelante GREENBERG) como representante de 23ANDME, el 01/10/2023 se habría producido una brecha de confidencialidad debida a un ciberataque que afectó a 799 personas residentes en España, clientes de la empresa, en la que se expusieron datos de identidad, contacto y localización, imágenes y datos genéticos.

En la comunicación de la brecha, 23ANDME incluye la siguiente descripción del incidente (traducción no oficial realizada con la herramienta "Digital Europe Language Tools"):

"(…)"

Con fecha 30/10/2023, 23ANDME amplía la información relativa a la brecha. De acuerdo con esta nueva comunicación la brecha habría afectado a otras 1.843 personas en España y habría incluido, además de los datos mencionados anteriormente, datos que revelan el origen étnico.

En la descripción incluida en esta segunda comunicación indica lo siguiente (traducción no oficial realizada con la herramienta "Digital Europe Language Tools"):

"(…)"

SEGUNDO: Como consecuencia de los hechos conocidos, con fecha 31/10/2023, la Directora de la Agencia Española de Protección de Datos instó a la Subdirección General de Inspección de Datos (SGID) a iniciar las actuaciones previas de investigación a las que se refiere el artículo 67 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD).

TERCERO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE)

2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VIII, de la LOPDGDD.

Dado que 23ANDME es una entidad de nacionalidad estadounidense sin establecimiento principal en España y la brecha de datos afectaba a residentes en diferentes Estados, con fecha 25/03/2024, de acuerdo con el artículo 61 del RGPD, se solicitó, a través del "Sistema de información del Mercado Interior" (regulado por el Reglamento (UE) nº 1024/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012), información sobre la existencia, en su caso, de establecimiento de la empresa en otros Estados, constatando que la brecha había sido notificada a otros Estados y que no constaría un establecimiento principal en la Unión Europea.

El 27/03/2024 se realizó un requerimiento de información a 23ANDME, que fue recibido el 22/04/2024, en el que se solicitaba información adicional sobre el incidente, evaluación de riesgo en las operaciones de tratamiento realizadas, medidas de seguridad adoptadas antes y después del incidente y motivos de la demora en la notificación de la brecha a esta autoridad de control.

En respuesta al requerimiento, 23ANDME aporta información adicional sobre el incidente, afirmando lo siguiente (traducción no oficial realizada con la herramienta "Digital Europe Language Tools"):

"(…)"

En relación con la publicación de los datos en Internet afirma lo siguiente (traducción no oficial realizada con la herramienta "Digital Europe Language Tools"):

"(…)"

Respecto de las medidas de seguridad adoptadas antes y con posterioridad a la brecha, 23ANDME aporta copia de evaluaciones de impacto relativas a protección de datos y afirma lo siguiente (traducción no oficial realizada con la herramienta "Digital Europe Language Tools"):

"(…)"

Respecto de la notificación a esta autoridad de control con posterioridad a las 72 horas exigidas por el artículo 33 del RGPD, 23ANDME afirma lo siguiente (traducción no oficial realizada con la herramienta "Digital Europe Language Tools"):

"(…)"

Junto con su respuesta, 23ANDME aporta los textos de las comunicaciones que habría enviado a sus clientes, que varían en función de los datos expuestos. Asimismo, aporta copia de las evaluaciones de impacto realizadas.

En el marco de las actuaciones previas de investigación se ha comprobado la existencia de la publicación de un post en un blog de la página web de la empresa del comunicado sobre el incidente en la url ******URL.1***. En el post tiene fecha de creación del post 06/10/2023 y fecha de última actualización de 05/12/2023, según queda

diligenciado en el expediente. En él se observa la existencia de varias actualizaciones en las que se informa sobre la evolución de la investigación y las medidas que se han ido tomando respecto del acceso de los usuarios.

Asimismo, con fecha 26/03/2024 se han diligenciado en el expediente capturas de pantalla en las que figura la política de privacidad del sitio web https://www.23andme.com. Dicha información consta como actualizada a 14/12/2022 y se indica que es de aplicación a todas las páginas web propiedad y operadas por 23ANDME.

Dicha política incluye referencias a los datos personales de los clientes que son objeto de tratamiento por 23ANDME, el origen de los datos tratados, su utilización, los supuestos en que se comunican a terceros. En el apartado de “medidas de seguridad”, se indica lo siguiente (traducción no oficial realizada con la herramienta “Digital Europe Language Tools”):

> *“Medidas de seguridad*
>
> *Implementamos medidas físicas, técnicas y administrativas destinadas a prevenir el acceso no autorizado o la divulgación de su información personal. Nuestro equipo revisa y mejora regularmente nuestras prácticas de seguridad para ayudar a garantizar la integridad de nuestros sistemas y su información personal. Para obtener más información sobre nuestras prácticas, visite nuestra guía de atención al cliente.*
>
> *Por favor, reconozca que proteger su información personal también es su responsabilidad. Sea consciente de mantener su contraseña y otra información de autenticación a salvo de terceros, y notifique inmediatamente a 23andMe de cualquier uso no autorizado de sus credenciales de inicio de sesión. Su contraseña no es visible para el personal de 23andMe, y le recomendamos que no comparta su contraseña con 23andMe ni con terceros. 23andMe no puede proteger la Información personal que usted divulgue por su cuenta o que nos solicite que divulguemos.”*

Consta asimismo en el expediente diligencia de 08/01/2025 con impresión de capturas de pantalla de la página web https://eu.customercare.23andme.com/hc/en-us/articles/204712980-What-Countries-Do-You-Ship-To, en la que se indica a qué países realiza envíos 23ANDME, entre los que se encuentra España.

Por último, consta en el expediente el documento “23ANDME HOLDING CO. ANNUAL REPORT FISCAL 2023”, publicado en la página web de 23ANDME y firmado con fecha 25/05/2023 por la Presidenta y CEO de 23ANDME así como por otros responsables de la empresa. Dicho documento ofrece información sobre distintos aspectos de la actividad de la empresa.

En la página 13 de dicho documento, en el epígrafe “Privacy and Security Regulation” (Regulación de provacidad y seguridad), entre otra información, se afirma lo siguiente (traducción no oficial realizada con la herramienta “Digital Europe Language Tools”):

"Estamos comprometidos con un esfuerzo continuo de cumplimiento y supervisión de privacidad, también en relación con los requisitos de numerosas leyes, normas y regulaciones locales, estatales, federales e internacionales relacionadas con la privacidad y la seguridad de la información personal identificable directa o indirectamente (colectivamente, «Leyes de protección de datos»). Dichas leyes de protección de datos regulan la recopilación, el almacenamiento, el intercambio, el uso, la divulgación, el procesamiento, la transferencia y la protección de la información personal, incluida la información genética, y evolucionan con frecuencia en su alcance y aplicación.

(…)

Fuera de los Estados Unidos, numerosos países tienen sus propias leyes de protección de datos, incluidas, entre otras, la Ley Canadiense de Protección de Información Personal y Documentos Electrónicos ("PIPEDA") y el Reglamento General de Protección de Datos de la UE ("GDPR"), ahora también promulgadas en el Reino Unido ("RGPDG").

(…)

A nivel internacional, estamos sujetos, entre otras leyes de protección de datos, al RGPD, al RGPD del Reino Unido y a la PIPEDA, que regulan la recopilación, el almacenamiento, el intercambio, el uso, la divulgación y la protección de la información personal, e imponen requisitos estrictos con sanciones significativas y riesgos de litigio por incumplimiento. Al igual que los Estados Unidos, las leyes internacionales de protección de datos incluyen leyes nacionales, estatales o provinciales y locales, lo que significa que los costos de cumplimiento aumentan con cada estado, provincia o localidad a la que enviamos. El incumplimiento del GDPR (y el GDPR del Reino Unido) puede resultar en multas de hasta € 20 millones / £ 17,5 millones o hasta el 4% de los ingresos globales anuales del infractor, lo que sea mayor.

(…)

Además, en los Estados Unidos e internacionalmente, las empresas están obligadas a notificar a los clientes afectados cuya información personal ha sido revelada como resultado de una brecha de datos. Muchos países y / o estados requieren que las empresas mantengan salvaguardas y tomen ciertas medidas en respuesta a una violación de datos y pueden estar obligados a notificar también a las autoridades reguladoras aplicables."

En la página 50 de dicho documento, se indica lo siguiente en relación con las brechas de datos (traducción no oficial realizada con la herramienta "Digital Europe Language Tools"):

"El aumento de las amenazas globales a la seguridad informática y los delitos informáticos más sofisticados y selectivos suponen un riesgo para la seguridad de nuestros sistemas y redes y la confidencialidad, disponibilidad e integridad de nuestros datos. Ha habido varios casos recientes, muy publicitados en los que organizaciones de varios tipos y tamaños han reportado la divulgación no

autorizada de información confidencial del cliente u otra información confidencial, así como ciberataques que implicaban la difusión, el robo y la destrucción de información corporativa, propiedad intelectual, efectivo u otros activos valiosos.

También ha habido varios casos muy publicitados en los que piratas informáticos han solicitado pagos de «rescate» a cambio de no revelar información confidencial del cliente u otra información confidencial o por no inhabilitar el ordenador u otros sistemas de la empresa objetivo. Una violación de seguridad o violación de la privacidad que conduce a la divulgación no autorizada o la pérdida de uso no autorizado o modificación o que impide el acceso a o de otra manera afecta la confidencialidad, seguridad o integridad de la información sensible, confidencial o propietaria que nosotros o nuestro tercero proveedor de servicios mantienen o procesan, podría exigirnos cumplir con las leyes de notificación de incumplimiento y hacernos incurrir en costes significativos de reparación, multas, sanciones, notificación a particulares, medios de comunicación y autoridades gubernamentales, aplicación de medidas destinadas a reparar o sustituir sistemas o tecnologías, y a prevenir sucesos futuros, aumentos potenciales de los seguros primas y auditorías o investigaciones forenses de seguridad."

En relación con la actividad de 23ANDME en Europa, en la página 52 del documento, se afirma lo siguiente (traducción no oficial realizada con la herramienta "Digital Europe Language Tools"):

"Planeamos continuar expandiendo las operaciones en el extranjero donde tenemos una experiencia operativa limitada y podemos estar sujetos a mayores riesgos regulatorios y competencia local.

Si no tenemos éxito en los esfuerzos para expandirnos internacionalmente, nuestro negocio puede verse perjudicado. Las regulaciones existen o están bajo consideración en países fuera de los Estados Unidos, que limitan o impiden la venta de pruebas genéticas directas al consumidor. Algunos países, incluida Australia, requieren una revisión previa a la comercialización por parte de su organismo regulador similar a la requerida en los Estados Unidos por la FDA. Algunos países, incluidos Australia, Alemania, Francia y Suiza, requieren una receta médica para pruebas genéticas que proporcionen información de salud, limitando así nuestra oferta en esos países a una prueba solo de ascendencia. Otros países requieren asesoramiento genético obligatorio antes de las pruebas genéticas. Estas regulaciones limitan el mercado disponible para nuestros productos y servicios y aumentan los costos asociados con la comercialización de los productos y servicios donde podemos ofrecer nuestros productos. Los desarrollos legales en la UE han creado una serie de nuevas obligaciones de cumplimiento con respecto a las transferencias de datos personales de la Unión Europea a los Estados Unidos, incluidos GDPR y GDPR del Reino Unido, que se aplica a algunas de nuestras actividades relacionadas con los servicios que ofrecemos o podemos ofrecer a personas ubicadas en la UE. Se seguirán requiriendo esfuerzos y gastos significativos para garantizar el cumplimiento del RGPD y del RGPD del Reino Unido, y podrían hacernos cambiar nuestras prácticas comerciales. Además, los

requisitos bajo el GDPR y el GDPR del Reino Unido pueden cambiar periódicamente o pueden ser modificados por la legislación de la UE / Reino Unido y / o nacional. El GDPR y el GDPR del Reino Unido imponen estrictas obligaciones de cumplimiento con respecto al manejo de datos personales y han resultado en la emisión de sanciones económicas significativas por incumplimiento, incluidas posibles multas de hasta el 4% del volumen de negocios anual global para el año financiero anterior o € 20 millones / £ 17,5 millones (lo que sea mayor) para las violaciones más graves."

CUARTO: Con fechas 23/04/2025 y 07/05/2025 se recibieron sendas comunicaciones de la entidad OFFICE OF THE UNITED STATES TRUSTEE, en relación con el procedimiento de concurso de acreedores de 23ANDME en Estados Unidos.

QUINTO: Con fecha 29 de mayo de 2025, la Presidencia de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, por la presunta infracción de los artículos 5.1 f) y 33 del RGPD, tipificados en el artículo 83.5 a) y en el artículo 84.4 a) del RGPD, respectivamente.

SEXTO: Con fecha 24/06/2025 fue notificado el citado acuerdo de inicio, de acuerdo con el certificado expedido por Correos, conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP). Transcurrido el plazo otorgado para la formulación de alegaciones, se ha constatado que no se ha recibido alegación alguna por la parte reclamada.

El artículo 64.2.f) de la LPACAP -disposición de la que se informó a la parte reclamada en el acuerdo de apertura del procedimiento- establece que si no se efectúan alegaciones en el plazo previsto sobre el contenido del acuerdo de iniciación, cuando éste contenga un pronunciamiento preciso acerca de la responsabilidad imputada, podrá ser considerado propuesta de resolución. En el presente caso, el acuerdo de inicio del expediente sancionador determinaba los hechos en los que se concretaba la imputación, la infracción del RGPD atribuida a la reclamada y la sanción que podría imponerse. Por ello, tomando en consideración que la parte reclamada no ha formulado alegaciones al acuerdo de inicio del expediente y en atención a lo establecido en el artículo 64.2.f) de la LPACAP, el citado acuerdo de inicio es considerado en el presente caso propuesta de resolución.

SÉPTIMO: De acuerdo con el documento "23ANDME HOLDING CO. ANNUAL REPORT FISCAL 2023" (página 80), publicado en la página web de 23ANDME (https://investors.23andme.com/static-files/2f13f408-1924-4246-b3a9-ccb72af3a2ee), el volumen de negocio de la empresa en el año 2023 ascendió a **299.489.000 $**. (alrededor de 263 millones de euros).

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes,

HECHOS PROBADOS

PRIMERO: Con fecha 17/10/2023, la empresa 23ANDME, INC notificó a esta Agencia una brecha de seguridad en la que se habría producido una violación de la seguridad de los datos personales, cuya información amplió en una nueva notificación con fecha 30/10/2023.

SEGUNDO: La violación se produjo debido a un ciberataque que afectó a 2.642 personas residentes en España, clientes de la empresa, en la que se expusieron datos de identidad, contacto y localización, imágenes, datos de salud, datos genéticos y datos que revelaban el origen étnico de las personas. Una muestra de dichos datos fue publicada en un foro de Internet y un archivo con los datos puesto a la venta en la dark web.

TERCERO: El origen de la brecha fue el acceso a determinadas cuentas de clientes, conocido como "*credential stuffing*", en casos en que los clientes habían utilizado para su sitio web las mismas credenciales de inicio que para otros sitios web en otras organizaciones ya comprometidos.

CUARTO: En el momento de producirse la brecha, el acceso de los clientes de 23ANDME a sus cuentas, que permitía el acceso a sus datos personales y, en algunos casos, a los de posibles familiares, se realizaba mediante usuario y contraseña. Se ofrecía la posibilidad de utilizar la autenticación multifactor, pero con carácter voluntario. Asimismo, 23ANDME no tenía implementados límites para el acceso, solicitud o descarga de datos por IP.

QUINTO: El 01/10/2023, 23ANDME detectó un mensaje en Reddit poniendo a la venta información supuestamente de sus clientes y el 05/10/2023, confirmó que uno de los datos publicados pertenece a uno de sus clientes.

SEXTO: El 06/10/2023, 23ANDME publicó un comunicado de alerta en su página web.

SÉPTIMO: El 07/10/2023, 23ANDME notificó la brecha a las autoridades de EEUU.

OCTAVO: El 10/10/2023, 23ANDME envió un correo a todos sus clientes informando del incidente.

NOVENO: El 12/10/2023, 23ANDME confirmó la identidad de 799 clientes afectados por la brecha en España.

DÉCIMO: El 13/10/2023, 23ANDME comunicó la brecha a 799 afectados residentes en España localizados inicialmente.

UNDÉCIMO: El 24/10/2023, 23ANDME comunicó la brecha a los 1.843 afectados residentes en España localizados posteriormente.

FUNDAMENTOS DE DERECHO

I

Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para resolver este procedimiento la Presidencia de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: *"Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."*

II
Cuestiones previas

El artículo 4.1) del RGPD, define «dato personal» como: "*toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*".

El artículo 4.2) del RGPD, define «tratamiento» como: "*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción*."

El artículo 4.7) del RGPD, define al «responsable del tratamiento» o «responsable» como: *"la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros"*.

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 y 4.2 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que 23ANDME realiza, entre otros tratamientos, la recogida, almacenamiento y comunicación de datos personales de personas físicas, clientes de la empresa, incluyendo datos identificativos, datos de contacto y localización, imágenes, datos genéticos, datos de salud y datos que revelan su origen étnico.

23ANDME realiza esta actividad en su condición de responsable, dado que, en virtud del artículo 4.7 del RGPD, es quien determina los fines y medios del tratamiento.

Por su parte, el artículo 3 del RGPD regula su ámbito territorial de aplicación, estableciendo en su apartado segundo lo siguiente:

> *Artículo 3. Ámbito territorial*
>
> *(…)*
>
> *2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:*
> *a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o*
> *b) el control de su comportamiento , en la medida en que este tenga lugar en la Unión.*

En el presente caso, 23ANDME es un responsable no establecido en la Unión Europea que realiza actividades de tratamiento relacionadas con la oferta de servicios a interesados en la Unión, en concreto los servicios consistentes en la realización de pruebas genéticas y el análisis de los datos obtenidos. Por ello, resultan de aplicación a dicho tratamiento las obligaciones que impone el RGPD al responsable.

III

Obligación incumplida. Integridad y confidencialidad

La letra f) del artículo 5.1 del RGPD propugna:

> *"1. Los datos personales serán:*
> *(…)*
> *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»)."*

En el presente caso se ha producido una brecha de confidencialidad en los datos personales de los clientes de 23ANDME. Sobre esta brecha consta la información comunicada por 23ANDME en la notificación de la brecha de 17/10/2023 y en su ampliación de 30/10/2023, así como la información adicional facilitada por la empresa en respuesta al requerimiento realizado por la SGID en el marco de las actuaciones previas de investigación.

Según las notificaciones y la respuesta de 23ANDME, la brecha afectó a datos de clientes de la empresa, 2.642 de los cuales serían interesados en España. Los datos comprometidos son datos identificativos, de contacto y localización, imágenes, datos genéticos, datos de salud y datos que revelan el origen étnico de los afectados. Una

muestra de dichos datos fue publicada en un foro de Internet y un archivo con los datos puesto a la venta en la dark web.

Procede determinar, por tanto si, de acuerdo con la obligación que establece el artículo 5.1 f) del RGPD, 23ANDME, como responsable del tratamiento, aplicó medidas técnicas y organizativas apropiadas para garantizar una seguridad adecuada de los datos frente a incidentes como el que se habría producido.

En ese análisis, cabe tener en cuenta, en primer lugar, que parte de los datos que eran objeto de tratamiento eran de categoría especial, de acuerdo con el artículo 9 del RGPD. En concreto datos genéticos, que eran analizados para obtener información sobre salud y sobre el origen étnico de los clientes de 23ANDME, comparándolos con los de otros clientes de la empresa, posibles familiares, como se recoge en la política de privacidad reproducida en los antecedentes.

El hecho de que se trate de datos de especial categoría es relevante para este procedimiento, ya que el RGPD prevé una especial protección para ese tipo de datos y establece, con carácter general en cuanto a las obligaciones de los responsables de tratamiento, un enfoque basado en el riesgo. De acuerdo con este enfoque, tiene especial relevancia el tipo de datos que se tratan y las consecuencias que puede tener para los interesados una pérdida de confidencialidad de los mismos.

A este respecto, el considerando 51 del RGPD establece lo siguiente:

> *"(51) Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen racial o étnico"*

El artículo 24.1 del RGPD menciona específicamente los riesgos cuando alude a la obligación del responsable de establecer medidas apropiadas:

> *"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."*

Por su parte, el artículo 32, en relación con la seguridad del tratamiento, se refiere a los "*riesgos de probabilidad y gravedad variables para los derechos y libertades*", estableciendo lo siguiente:

> *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.

Asimismo, el artículo 35 del RGPD establece la obligación de contar con una evaluación de impacto relativa a la protección de datos (en adelante, EIPD) previa al tratamiento, cuando sea probable que éste entrañe un alto riesgo para los derechos y libertades de las personas. En desarrollo del apartado 4 de este artículo, la AEPD publicó en 2019 un listado de tipos de tratamientos que requieren EIPD, en la que se incluyó específicamente "*tratamientos que impliquen el uso de datos genéticos para cualquier fin*".

En definitiva, de acuerdo con el RGPD, la adopción de medidas por parte del responsable debe tener en cuenta, entre otras cuestiones, el tipo de datos que son objeto de tratamiento y, en consecuencia, el riesgo que supone para los interesados una eventual pérdida de confidencialidad. En el presente caso, dado que algunos de los datos son especialmente sensibles (datos genéticos, datos de salud y datos que revelan en origen étnico), sería exigible un especial celo en el establecimiento de medidas en el tratamiento. En este marco cabe analizar si las medidas desplegadas por 23ANDME eran adecuadas.

De acuerdo con la respuesta de 23ANDME al requerimiento realizado por esta autoridad de control, reproducida en los antecedentes de hecho, el origen de la brecha habría sido el acceso a determinadas cuentas de clientes, conocido como "*credential stuffing*", en casos en que los clientes habían utilizado para su sitio web las mismas credenciales de inicio que para otros sitios web en otras organizaciones ya comprometidos. Cabe analizar, por tanto, qué medidas técnicas y organizativas había adoptado 23ANDME, en particular, en relación con el acceso de sus clientes a sus cuentas.

De acuerdo con la respuesta de 23ANDME, el acceso de los clientes a sus cuentas, que permitía el acceso a sus datos personales y, en algunos casos, a los de posibles familiares, se realizaba mediante usuario y contraseña. En el momento en que se produce la brecha, 23ANDME ofrecía la posibilidad de utilizar la autenticación multifactor, pero con carácter voluntario:

"***(…)***"

No consta en la información remitida por 23ANDME que existiera algún requisito concreto en cuanto al formato de la contraseña en relación con la robustez de la misma ni exigencia de modificarla periódicamente.

En la política de privacidad de 23ANDME, publicada en su página web y que se ha transcrito en los antecedentes, solo hay una referencia a las credenciales de acceso a las cuentas, en los siguientes términos:

> *"Por favor, reconozca que proteger su información personal también es su responsabilidad. Sea consciente de mantener su contraseña y otra información de autenticación a salvo de terceros, y notifique inmediatamente a 23andMe de cualquier uso no autorizado de sus credenciales de inicio de sesión. Su contraseña no es visible para el personal de 23andMe, y le recomendamos que no comparta su contraseña con 23andMe ni con terceros. 23andMe no puede proteger la Información personal que usted divulgue por su cuenta o que nos solicite que divulguemos."*

De lo anterior, puede concluirse que las medidas adoptadas por 23ANDME en relación con el acceso de los clientes a sus cuentas no eran adecuadas al nivel de riesgo para los derechos y libertades de las personas que los datos objeto de tratamiento implica.

El robo de credenciales de usuario es uno de los ciberataques más habituales. A modo de ejemplo, cabe citar el informe de la Agencia de Ciberseguridad de la Unión Europea (ENISA) en el que se recoge anualmente las principales amenazas en materia de seguridad. En su informe publicado en 2022, "ENISA THREAT LANDSCAPE 2022" (el anterior a la brecha objeto de este procedimiento), señala el uso de credenciales robadas como el principal vector de ataque en el caso de brechas de datos, alcanzando el 40% de los casos. En su apartado de recomendaciones y estándares de seguridad, se refiere específicamente al uso de contraseñas únicas y robustas, al uso de múltiple factor de autenticación (MFA) para fortalecer el proceso de autenticación y a la concienciación de los usuarios.

Por su parte, 23ANDME también hace referencia a las brechas de datos en su informe para inversores, anterior a la brecha y publicado en su página web, parcialmente reproducido en los antecedentes, cuando se refiere al aumento de las amenazas de seguridad y al riesgo de acceso y divulgación de información confidencial de sus clientes.

En este contexto, 23ANDME realizaba un tratamiento de datos especialmente sensibles, por lo que sería exigible la aplicación de medidas especialmente reforzadas. En lo que afecta a las credenciales de usuario, siendo este un conocido vector de ataque en las brechas de datos y dando acceso, en el caso de las cuentas de 23ANDME, al visionado y descarga de datos genéticos, de salud y datos que revelan el origen étnico de sus clientes, las medidas que podrían considerarse adecuadas implicarían necesariamente un análisis de la política de acceso y unas medidas de seguridad al respecto.

Sin embargo, la información aportada por 23ANDME y la publicada en su página web, pone de manifiesto que no existían unos requisitos específicos para el establecimiento

de contraseñas robustas, ni para su modificación en el tiempo. La política de seguridad y privacidad publicada en su página web, no cuenta además con instrucciones o recomendaciones más allá de recordar la responsabilidad del usuario en el uso de sus credenciales.

Según la información aportada por 23ANDME, había implementado en su web un sistema de múltiple factor de autenticación, lo que pone de manifiesto que 23ANDME era consciente de que podía ser una medida de seguridad adecuada. Sin embargo, estaba configurado como de carácter no obligatorio para los usuarios, por lo que 23ANDME no garantizaba con él un nivel reforzado de seguridad para sus clientes.

Por otro lado, un uso responsable de las credenciales implica al usuario, como indica la política de privacidad de 23ANDME, antes reproducida. Sin embargo, el análisis de riesgos y la adopción de medidas de seguridad adecuadas para proteger los datos personales de sus clientes es exigible a 23ANDME como responsable del tratamiento y no puede descargarse dicha responsabilidad exclusivamente en el usuario.

Por otro lado, una vez el usuario había accedido a la cuenta, no había implementados límites o controles adicionales para el acceso o la descarga de los datos especialmente sensibles, como pone de manifiesto la respuesta de 23ANDME, en la que se indica que este tipo de limitaciones se han incorporado con posterioridad a la brecha:

> ***(…)***

Este hecho, dificultó la detección de los accesos a las cuentas y facilitado la descarga de la información objeto de la brecha.

Por todo lo anterior, se considera que los hechos probados son constitutivos de una infracción, imputable a 23ANDME, por vulneración del artículo transcrito anteriormente.

IV
Tipificación de la infracción del artículo 5.1.f) del RGPD y calificación a efectos de prescripción

El artículo 83.5 del RGPD tipifica como infracción administrativa la vulneración del artículo siguiente, que se sancionará, de acuerdo con el apartado 2, con multas administrativas de 20.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

> *"a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;"*

Por su parte, la LOPDGDD en su artículo 71, Infracciones, señala que:

> *"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica".*

A los solos efectos del plazo de prescripción, el artículo 72.1 de la LOPDGDD establece lo siguiente:

> *"En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:*
> *a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679."*

V

Sanción por la infracción del artículo 5.1 f) del RGPD

A fin de determinar la multa administrativa a imponer se han de observar las previsiones de los artículos 83.1 y 83.2 del RGPD, preceptos que señalan:

> *"1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 9 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.*
>
> *2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:*
> *a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;*
> *b) la intencionalidad o negligencia en la infracción;*
> *c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;*
> *d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;*
> *e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;*
> *f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;*
> *g) las categorías de los datos de carácter personal afectados por la infracción;*
> *h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;*
> *i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;*

j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y
k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción".

Por su parte, el artículo 76 *"Sanciones y medidas correctivas"* de la LOPDGDD dispone:

"1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:
a) El carácter continuado de la infracción.
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.
f) La afectación a los derechos de los menores.
g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.
h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado".

En el presente caso, considerando la gravedad de la posible infracción, atendiendo especialmente a las consecuencias que su comisión provoca en los afectados, correspondería la imposición de multa.

La multa que se imponga deberá ser, en cada caso, individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el artículo 83.1 del RGPD. Para garantizar estos principios, se considera, con carácter previo, el volumen de negocio de 23ANDME de 299.489.000 $ (alrededor de 263 millones de euros) en el año 2023.

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, procede graduar la sanción a imponer de acuerdo con las circunstancias siguientes, contempladas en los preceptos antes citados.

Con carácter previo, se estima que la infracción sería grave, en la medida en que concurren las circunstancias siguientes:

- La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate, así como el número de interesados afectados y el nivel de los daños y perjuicios

que hayan sufrido (artículo 83.2, letra a), del RGPD). En el presente caso, destaca no solo el elevado número de afectados, que asciende a 2.642 personas interesados en España.

- Las categorías de los datos de carácter personal afectados por la infracción (artículo 83.2, letra g), del RGPD). En el presente caso, además de datos identificativos, de contacto y localización, se han visto afectados por la brecha datos de carácter especialmente sensible, como son los datos genéticos, datos de salud y datos que revelan el origen étnico de las personas afectadas, lo que supone un elevado riesgo para sus derechos y libertades.

Asimismo, se considera como factor de graduación en calidad de agravante la vinculación de la actividad del infractor con la realización de tratamientos de datos personales (artículo 76.2, letra b), de la LOPDGDD). La actividad de 23ANDME consistía en buena medida en el tratamiento de datos personales especialmente sensibles de sus clientes, como parte del servicio que ofrecía la empresa de realización de test genéticos y de análisis de sus resultados.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 5.1.f) del RGPD, permite fijar una sanción de multa administrativa de 2.000.000,00 euros.

VI
Obligación incumplida. Notificación de una violación de la seguridad de los datos personales a la autoridad de control

El artículo 33 del RGPD establece lo siguiente:

"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.

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.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:
a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;
d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo."

Cabe destacar en primer lugar, que la obligación de notificación de una brecha no es una mera obligación formal, sino una medida de responsabilidad proactiva vinculada a los daños que las violaciones de seguridad de los datos personales pueden suponer para las personas afectadas. En este sentido se manifiesta en el considerando 85 del RGPD insistiendo en la necesidad de notificar la violación sin dilación "*a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas".*

Asimismo, en el considerando 87 del RGPD se señala la necesidad de que la autoridad de control verifique que dicha notificación se ha realizado, en los siguientes términos:

(87) Debe verificarse si se ha aplicado toda la protección tecnológica adecuada y se han tomado las medidas organizativas oportunas para determinar de inmediato si se ha producido una violación de la seguridad de los datos personales y para informar sin dilación a la autoridad de control y al interesado. Debe verificarse que la notificación se ha realizado sin dilación indebida teniendo en cuenta, en particular, la naturaleza y gravedad de la violación de la seguridad de los datos personales y sus consecuencias y efectos adversos para el interesado. Dicha notificación puede resultar en una intervención de la autoridad de control de conformidad con las funciones y poderes que establece el presente Reglamento.

En el presente caso, de acuerdo con la información aportada por 23ANDME en la notificación de la brecha y en la respuesta al requerimiento de la SGID en las actuaciones previas de investigación, transcrita anteriormente en los antecedentes de hecho, la cronología del incidente, las actuaciones realizadas por 23ANDME y su notificación a esta autoridad de control ha sido la siguiente:

- 01/10/2023, 23ANDME detecta un mensaje en Reddit poniendo a la venta información supuestamente de sus clientes

- 05/10/2023, confirma que uno de los datos publicados pertenece a uno de sus clientes
- 06/10/2023, publica un comunicado de alerta en su página web
- 07/10/2023, notifica la brecha a las autoridades de EEUU
- 09/10/2023, cierra sesiones de clientes y obliga a resetear contraseñas
- 10/10/2023, envía un correo a todos sus clientes informando del incidente
- 12/10/2023, confirma la identidad de los clientes afectados por la brecha
- 13/10/2023, comunica a los 799 afectados residentes en España localizados inicialmente
- 17/10/2023, GREENBERG TRAURIG, en representación de 23ANDME, notifica la brecha a la AEPD
- 24/10/2023, 23ANDME comunica a los 1.843 afectados localizados posteriormente
- 30/10/2023, GREENBERG TRAURIG amplía la información de la brecha

De acuerdo con dicha cronología, la notificación, desde que se conoce que existe una brecha que afecta a datos personales, excede ampliamente el plazo de 72 horas establecido en el artículo 33 del RGPD.

Respecto de la notificación a esta autoridad de control con posterioridad a las 72 horas exigidas por el artículo 33 del RGPD, en la ampliación de la notificación de la brecha realizada el 30/10/2023, transcrita en los antecedentes de hecho, se indica lo siguiente (traducción no oficial realizada con la herramienta “Digital Europe Language Tools”):

(…)

Por otro lado, en su respuesta al requerimiento de la SGID, 23ANDME afirma lo siguiente (traducción no oficial realizada con la herramienta “Digital Europe Language Tools”):

(…)

En relación con dicha justificación, procede identificar en primer lugar en qué momento habría tenido 23ANDME la obligación de notificar la violación de los datos.

A este respecto cabe señalar que la obligación de notificación establecida en el artículo 33 del RGPD ha sido objeto de desarrollo por el Comité Europeo de Protección de Datos (en adelante, CEPD) a través de las Directrices 9/2022, sobre la notificación de las violaciones de la seguridad de los datos personales en el marco del RGPD.

Dichas Directrices se refieren en particular al momento en el que el responsable “tiene constancia” de la violación y, por tanto, tiene la obligación de notificar una violación de datos personales. Así, en sus apartados 31 y establecen lo siguiente:

> *31. Como se ha explicado anteriormente, el RGPD establece que, en caso de una violación, el responsable del tratamiento lo notificará sin dilación indebida y, de ser posible, a más tardar setenta y dos horas después de que haya tenido constancia de ella. Esto puede plantear la cuestión de cuándo puede considerarse que un responsable del tratamiento «tiene constancia» de una violación. El CEPD piensa que debe considerarse que el responsable del tratamiento «tiene constancia» cuando tenga un grado razonable de certeza de que se ha producido un incidente de seguridad que compromete datos personales.*

Siguiendo las Directrices, en el presente caso, el día 05/10/2023 23ANDME tuvo constancia de la existencia de una violación, dado que confirmó que uno de los datos publicados pertenecía a uno de sus clientes. Tenía, por tanto, un grado razonable de certeza de que el incidente comprometía datos personales del tratamiento del que era responsable. En el mismo sentido apuntaría el hecho de que al día siguiente, 06/10/2023, 23ANDME publica un comunicado de alerta en su página web, el 07/10/2023 notifica la brecha a las autoridades de EEUU y el 09/10/2023 cierra todas las sesiones de sus clientes y les obliga a resetear contraseñas, como medida de seguridad reactiva. Además, el 12/10/2023 ya conocía que entre los afectados existían interesados en España. Sin embargo, no procedió a la notificación a esta autoridad de control hasta el día 17/10/2023.

La necesidad de inmediatez en la notificación no es trivial, sino que está relacionada con la eficacia de esta medida en relación con los daños que una violación puede suponer para los afectados. En este sentido, el propio artículo 33 del RGPD prevé expresamente que en un primer momento no se disponga de toda la información sobre lo ocurrido y se pueda ir aportando de forma gradual.

A este respecto cabe citar de nuevo las Directrices 9/2022 del CEPD, cuando señalan lo siguiente:

> *35. Una vez que el responsable del tratamiento tenga constancia de una violación notificable, esta deberá notificarse sin dilación indebida y, de ser posible, en un plazo máximo de setenta y dos horas. Durante este período, el responsable del tratamiento deberá evaluar el posible riesgo para las personas a fin de determinar si se aplica el requisito de notificación, así como las medidas necesarias para hacer frente a la violación.*
>
> *(…)*
>
> *40. Por consiguiente, debe quedar claro que el responsable del tratamiento está obligado a actuar a partir de cualquier alerta inicial y a determinar si se ha producido o no una violación. Este breve período permite que se realicen algunas investigaciones y que el responsable del tratamiento reúna pruebas y otros detalles pertinentes. No obstante, una vez que el responsable del tratamiento haya establecido con un grado razonable de certeza que se ha*

> *producido una violación, si se cumplen las condiciones del artículo 33, apartado 1, del RGPD, deberá notificarlo a las autoridades de control sin dilación indebida y, de ser posible, en un plazo máximo de setenta y dos horas. Si un responsable del tratamiento no actúa de manera rápida y resulta evidente que se ha producido una violación, esto podría considerarse una falta de notificación de conformidad con el artículo 33 del RGPD.*

Por otro lado, 23ANDME señala que, una vez identificados los clientes cuyos perfiles habían sido afectados, "*23andMe comenzó inmediatamente a determinar las obligaciones de notificación de brechas en las 62 jurisdicciones en las que se encuentran los clientes afectados".* Dicha afirmación pondría de manifiesto una falta de diligencia en relación con sus obligaciones de los responsables de tratamientos a los que les es de aplicación en RGPD.

La obligación de notificación, como se ha dicho, es una medida vinculada a la seguridad de los datos personales y debe realizarse con carácter inmediato. La afirmación de que, solo después de identificadas las personas afectadas, se comiencen a determinar qué obligaciones existen en cada país, ya que desde el día 12/10/23 tenía conocimiento de la existencia de personas afectadas por la brecha residentes en España y la obligación de notificación, de acuerdo con el apartado 73 de las citadas Directrices "*la violación deberá notificarse a todas las autoridades de control respecto de las cuales los interesados afectados residan en su Estado miembro*".

Más aún cuando se trata de un tratamiento que entraña un alto riesgo, al implicar datos genéticos, de salud y sobre el origen étnico de los afectados, como el propio responsable indica en las EIPD que acompaña a su respuesta, ya que una violación de dichos datos en todo caso supondría una obligación de notificar, en cuanto implica un riesgo elevado para los derechos y libertades de las personas afectadas.

Por otro lado, 23ANDME era consciente de la necesidad del cumplimiento de la normativa de protección de datos en la Unión Europea y de las obligaciones que impone el RGPD a los responsables del tratamiento de los datos. Así lo pone de manifiesto el documento "23ANDME HOLDING CO. ANNUAL REPORT FISCAL 2023", publicado en la página web de 23ANDME. En este documento, anterior a la brecha, se hace referencia a la actividad de la compañía en países en los que es de aplicación el RGPD y en él constan diferentes referencias al RGPD, como se ha transcrito en los antecedentes de hecho, e incluso se hace mención expresa a la posibilidad de que la empresa pudiera ser sancionada en caso de incumplimiento.

Al respecto, cabe citar de nuevo las Directrices 9/2022 del CEPD, que señalan lo siguiente en relación con responsables no establecidos en la Unión Europea:

> *72. Cuando un responsable del tratamiento que no está establecido en la UE esté sujeto a lo dispuesto en el artículo 3, apartados 2 o 3, del RGPD, y tenga conocimiento de una violación, seguirá estando obligado a cumplir las obligaciones de notificación previstas en los artículos 33 y 34 del RGPD. El artículo 27 del RGPD exige que el responsable del tratamiento (y el encargado) designe a un representante en la UE cuando sea de aplicación el artículo 3, apartado 2, del RGPD.*

Por todo lo anterior, se considera que los hechos probados son constitutivos de una infracción, imputable a 23ANDME, por vulneración del artículo transcrito anteriormente.

VII

Tipificación de la infracción del artículo 33 del RGPD y calificación a efectos de prescripción

El artículo 83.4 del RGPD tipifica como infracción administrativa la vulneración del artículo siguiente, se sancionará, de acuerdo con el apartado 2, con multas administrativas de 10.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

> *"a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;"*

Por su parte, la LOPDGDD en su artículo 71, Infracciones, señala que:

> *"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica".*

A los solos efectos del plazo de prescripción, el artículo 73 de la LOPDGDD establece lo siguiente:

> *"En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:*
> *r) El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.*

VIII

Sanción por el incumplimiento del artículo 33 del RGPD

A fin de determinar la multa administrativa a imponer se han de observar las previsiones de los artículos 83.1 y 83.2 del RGPD y del artículo 76 de la LOPDGDD, transcritos anteriormente en el fundamento tercero.

En el presente caso, considerando la gravedad de la posible infracción, atendiendo especialmente a las consecuencias que su comisión provoca en los afectados, correspondería la imposición de multa.

La multa que se imponga debe ser, en cada caso, individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el artículo 83.1 del RGPD. Para garantizar estos principios, se considera, con carácter previo, el volumen de negocio de 23ANDME de 299.489.000 $ en el año 2023.

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, procede graduar la sanción a imponer de acuerdo con las circunstancias siguientes, contempladas en los preceptos antes citados.

Con carácter previo, se estima que la infracción sería grave, en la medida en que concurren las circunstancias siguientes:

- La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido (artículo 83.2, letra a), del RGPD): En el presente caso, destaca no solo el elevado número de afectados, que asciende a 2.642 personas en España.

- Las categorías de los datos de carácter personal afectados por la infracción (artículo 83.2, letra g), del RGPD): Además de datos identificativos, de contacto y localización, han sino afectados por la brecha datos de carácter especialmente sensible, como son los datos genéticos, datos de salud y datos que revelan el origen étnico de las personas afectadas, lo que supone un elevado riesgo para sus derechos y libertades.

Asimismo, se considera como factor de graduación en calidad de agravante la vinculación de la actividad del infractor con la realización de tratamientos de datos personales (artículo 76.2, letra b), de la LOPDGDD): La actividad de 23ANDME consistía en buena medida en el tratamiento de datos personales especialmente sensibles de sus clientes, como parte del servicio que ofrecía la empresa de realización de test genéticos y de análisis de sus resultados.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 33 del RGPD, permite fijar una sanción de multa administrativa de 400.000,00 euros.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada, la Presidencia de la Agencia Española de Protección de Datos

RESUELVE:

PRIMERO: IMPONER a ***23ANDME, INC***, por las presuntas infracciones de los artículos 5.1 f) y 33 del RGPD, tipificadas, respectivamente, en los artículos 83.5 y 83.4 del RGPD, una multa administrativa de **DOS MILLONES CUATROCIENTOS MIL EUROS (2.400.000,00 euros)**, correspondiente a las siguientes infracciones:

- Por la infracción del artículo 5.1 f) del RGPD, tipificada en el artículo 83.5, multa de 2.000.000,00 euros
- Por la infracción del artículo 33 del RGPD, tipificada en el artículo 83.4, multa de 400.000,00 euros

SEGUNDO: NOTIFICAR la presente resolución a ***23ANDME, INC -***.

TERCERO: Esta resolución será ejecutiva una vez finalice el plazo para interponer el recurso potestativo de reposición (un mes a contar desde el día siguiente a la notificación de esta resolución) sin que el interesado haya hecho uso de esta facultad. Se advierte al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP), en el plazo de pago voluntario establecido en el art. 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº ***IBAN: ES00-0000-0000-0000-0000-0000 (BIC/Código SWIFT: CAIXESBBXXX)***, abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A.. En caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

De conformidad con lo establecido en el artículo 76.4 de la LOPDGDD y dado que el importe de la sanción impuesta es superior a un millón de euros, será objeto de publicación en el Boletín Oficial del Estado la información que identifique al infractor, la infracción cometida y el importe de la sanción.

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

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Presidencia 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.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través

del Registro Electrónico de la Agencia [https://sedeaepd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-101025

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos