- **Procedimiento Nº: E/11936/2019**

## RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes:

## HECHOS

**PRIMERO:** Las actuaciones de inspección se inician por la recepción de un escrito de notificación de brecha de seguridad de los datos personales remitido por FORVO MEDIA, S.L en el que informan a la Agencia Española de Protección de Datos que, con fecha 7 de diciembre de 2019, detectaron un ataque al servidor que ocasionó modificaciones y borrado de archivos contenidos en éste.

**SEGUNDO:** En fecha 13 de diciembre de 2019, la Directora de la Agencia Española de Protección de Datos ordena a la Subdirección General de Inspección de Datos que valore la necesidad de realizar las oportunas investigaciones previas con el fin de determinar una posible vulneración de la normativa de protección de datos, teniendo conocimiento de los siguientes extremos:

Fecha de notificación de la brecha de seguridad de datos personales: 10 de diciembre de 2019.

Entidad Investigada: FORVO MEDIA, S.L.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

En fecha 14 de enero de 2020, se solicita información a FORVO MEDIA, S.L, siendo reiterada el día 14 de abril, al no recibir respuesta de la anterior solicitud. De la respuesta recibida se desprende lo siguiente:

Respecto de la empresa:

FORVO MEDIA, S.L es titular de la página web ******URL.1***
******URL.1*** es un sitio web dedicado a mostrar un diccionario mundial de pronunciaciones de palabras o frases de un gran número de idiomas. Estas pronunciaciones son aportadas por los usuarios registrados en el sitio web, siendo accesible a cualquier persona que visita la página web y consulta cualquier pronunciación.
El acceso completo a los servicios de la web (en particular, a la incorporación de pronunciaciones al diccionario) requiere el registro como usuario de la persona interesada y supone el tratamiento de algunos datos personales de tipo identificativo aportados por el usuario registrado, tales como su voz, dirección de correo electrónico, edad, sexo e idioma nativo, que son registrados en una base de datos asociada.

Desde el punto de vista técnico, el sistema se compone de dos partes diferenciadas. Por una parte, como se ha dicho, la base de datos de usuarios registrados y, por otra, el contenedor o servidor en el que se encuentran alojados los archivos de audio (pronunciaciones). Es en este último donde se ha detectado la intrusión o acceso no autorizado.

Respecto de la cronología de los hechos:

El día 10 de diciembre de 2019 detectan que algunos ficheros que contienen archivos mp3 de pronunciaciones grabadas por los usuarios han desaparecido del sistema (servidores de alojamiento de contenidos) sin causa aparente. Detectan el borrado por la disminución del volumen de datos (archivos mp3) alojados. De forma preventiva, notifican de forma inmediata la brecha de seguridad a la Agencia Española de Protección de Datos.

Los días 10 y 11 de diciembre 2019 comienzan a trabajar en la determinación del alcance y características de los datos comprometidos. No pueden determinar inicialmente el número de grabaciones comprometidas y/o eliminadas, aunque se constata que es posible que el atacante haya podido tener acceso a la totalidad de estas. En todo caso, no les consta que durante la incidencia se hayan extraído o copiado grabaciones en sistemas ajenos, limitándose el ataque a la intrusión y compromiso del servidor de alojamiento, mediante la eliminación de un número indeterminado de registros, pero no se ha producido el acceso a la base de datos donde se encuentran los datos personales de los usuarios registrados.

Desde ese mismo momento, como primera medida se procede a la restauración y recuperación de todos los ficheros a través de las copias de seguridad tanto propias como las del proveedor de alojamiento OVH Hispano S.L. De forma paralela, se prepara un nuevo servidor de alojamiento dentro del mismo proveedor, con las últimas versiones de los paquetes de seguridad y se cambia la dirección IP del servidor.

El día 12 de diciembre 2019, como medida complementaria, se contrata la plataforma de seguridad proporcionada por la empresa CLOUDFLARE como sistema de detección y primera barrera frente a ataques.

Durante los días del 12 al 14 de diciembre 2019, se comienza a realizar el primer análisis interno de seguridad buscando brechas y bugs relacionados con el código fuente de la página web. El análisis revela la posible utilización de herramientas de intrusión del tipo “Cross site scripting”, “HTML form without CSRF protection” o “Blind SQL Injection”.

Durante los días del 14 al 24 de diciembre 2019, se hacen las correcciones oportunas de los agujeros de seguridad detectados.

Respecto de las causas que hicieron posible la brecha:

No se ha podido determinar la causa concreta que ha podido provocar la incidencia de seguridad, aunque probablemente sea debida a la utilización por el atacante de alguna técnica tipo “Cross site scripting”, “HTML form without CSRF protection” o Blind SQL Injection”.

Respecto de los datos afectados:

Se desconoce con exactitud el número de posibles afectados porque, ya que lo que se ha producido es la eliminación física (borrado) de un número indeterminado de archivos mp3 sin poder determinar exactamente cuáles.

La tipología de datos afectados son grabaciones de voz (pronunciaciones de frases o palabras en distintos idiomas, sin datos personales agregados o metadatos).

No hay constancia de que las grabaciones de voz se hayan extraído o trasladado a sistemas de terceros. En todo caso, todos los archivos de audio en formato mp3 que existen en el sistema son accesibles “en abierto” y de forma ordenada a cualquier usuario o visitante de la página web ******URL.1***

El análisis de seguridad ha determinado que no se han comprometido datos personales asociados a las grabaciones de voz, es decir, sólo las grabaciones de voz sin metadatos asociados como direcciones IP, direcciones de email, nombres de usuario, etc., han podido ser accedidas. No se ha visto comprometida la base de datos de usuarios registrados. Estas circunstancias han llevado a considerar que no era preciso comunicar esta incidencia a los usuarios potencialmente afectados, dado que sus datos personales, claves de acceso, direcciones IP, etc., no se han visto comprometidas por la incidencia.

Respecto de las acciones tomadas para la resolución final de la brecha:

Restauración de los contenidos comprometidos y cambio a un nuevo servidor con una nueva dirección IP.

Implementación de la plataforma de seguridad de CLOUDFLARE dentro de los sistemas de Forvo Media S.L., para aplicar una capa de seguridad por encima de los sistemas de seguridad del servidor. CLOUDFLARE detiene el tráfico malicioso antes de que llegue al servidor web de origen y analiza las amenazas potenciales en las solicitudes de los visitantes en función de una serie de parámetros: dirección IP del visitante, recursos solicitados, carga y frecuencia de solicitudes, y reglas de firewall definidas por el cliente.

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

El mantenimiento de los sistemas de información se realiza con los propios medios internos de Forvo Media S.L. Tan sólo están externalizadas aquellas labores de mantenimiento propias de nuestro proveedor de alojamiento de contenidos (OVH HISPANO, S.L)
Aportan copia del Registro de Actividad, Información sobre el Análisis de Riesgos básico efectuado al tratamiento y Política de seguridad que incluye un procedimiento básico ante brechas de seguridad.

Respecto de las medias implementadas con posterioridad la brecha:

- Añaden una capa de seguridad por encima de los sistemas de seguridad del servido (CLOUDFLARE).

## FUNDAMENTOS DE DERECHO

**I**

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

**II**

El RGPD define, de un modo amplio, las "violaciones de seguridad de los datos personales" (en adelante quiebra de seguridad) como *"toda violación de la seguridad que ocasione 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, se produjo una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una posible brecha de confidencialidad, de integridad y de disponibilidad, como consecuencia del ataque al código fuente del servidor, modificando y posteriormente borrando archivos que contienen grabaciones de pronunciación de palabras en distintos idiomas, subidas a la web por los usuarios registrados en la misma.

El RGPD establece en su Considerando (26):

*"Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. (…) Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos."*

Por su parte el art. 4 apartado 1) del RGPD define "datos personales" con una gran amplitud:

*1) «datos personales»: 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."*

En consecuencia, la voz de una persona es un dato personal, al igual que lo será cualquier información que permita determinar, directa o indirectamente, su identidad.

En este sentido cabe destacar la Sentencia del Tribunal Supremo 815/2020 (Sala de lo Contencioso, Sección 3ª) de 18 de junio de 2020 (recurso 1074/2019), por la que se fija doctrina casacional en relación con la voz como dato de carácter personal. Señala la Sentencia que en este caso la grabación de la voz es un dato de carácter personal sujeto a la normativa de protección del tratamiento automatizado de los mismos, al estar asociada a otros datos como el número de teléfono o su puesta a disposición de otras personas que pueden identificar a quien pertenece.

**III**

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

Asimismo, contaba con protocolos de actuación para afrontar un incidente como el ahora analizado, lo que ha permitido de forma diligente la identificación, análisis y clasificación de la brecha de seguridad de datos personales así como la diligente reacción ante la misma al objeto de notificar, minimizar el impacto e implementar nuevas medias razonables y oportunas para evitar que se repita la incidencia en el futuro a través de la puesta en marcha y ejecución efectiva de un plan de actuación por las distintas figuras implicadas como son el responsable del tratamiento y el Delegado de Protección de Datos.

En consecuencia, disponía de forma previa de medidas técnicas y organizativas razonables en función del nivel de riesgo para evitar este tipo de incidencia y que al resultar insuficientes han sido actualizadas de forma diligente, procediendo a restaurar los contenidos comprometidos y usando un nuevo servidor con nueva dirección IP.

Asimismo, con ocasión de la incidencia se ha añadido una capa de seguridad por encima de los sistemas de seguridad del servidor (CLOUDFLARE).

No constan reclamaciones ante esta Agencia por parte de terceros.

Por último, se recomienda elaborar, un Informe final sobre la trazabilidad del suceso y su análisis valorativo, en particular, en cuanto al impacto final. Este Informe es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos y servirá para prevenir la reiteración de una brecha de similares características como la analizada.

**IV**

A la vista de las actuaciones practicadas, se ha acreditado que la actuación de FORVO MEDIA, S.L, como entidad responsable del tratamiento, ha sido acorde con la normativa sobre protección de datos personales analizada en los párrafos anteriores.

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 presentes actuaciones.

**SEGUNDO:** **NOTIFICAR** la presente resolución a FORVO MEDIA, S.L con NIF B20987541 y con domicilio en ******DIRECCIÓN.1***, ******LOCALIDAD.1***, GIPUZCOA.

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.

940-0419

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