- **Procedimiento Nº: E/09977/2020**

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: La reclamación interpuesta por ***A.A.A.*** (en adelante, el reclamante) tiene entrada con fecha 19 de octubre de 2020 en la Agencia Española de Protección de Datos. La reclamación se dirige contra **SOCIEDAD DE PROCEDIMIENTOS DE PAGO, S.L.,** con CIF B87599478 (en adelante, el reclamado). La reclamación se basa en el hecho, de que a través de la app de BIZUM, se puede conocer si el titular de un número de teléfono móvil está inscrito en el servicio, y extraer sus datos identificativos (nombre, iniciales y, en algunas ocasiones, alguno o los dos apellidos). El reclamante sostiene que esta operación podría automatizarse con un script, lo que permitiría recopilar los datos de identidad de los aproximadamente 9 millones de usuarios de los que dispone el servicio

SEGUNDO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos objeto de la reclamación, teniendo conocimiento de los siguientes extremos:

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se han investigado las siguientes entidades:

SOCIEDAD DE PROCEDIMIENTOS DE PAGO, S.L. con CIF B87599478

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Con fecha 26 de octubre de 2020, en el marco de las actuaciones de referencia E/08452/2020, se dio traslado de la denuncia al reclamado. En el escrito de respuesta, el reclamado alega lo siguiente:

"El servicio Bizum sobre el que se solicita información por parte de la AEPD en requerimiento con N/Ref: E/08452/2020, es un servicio informacional que se apoya sobre el servicio bancario de transferencias inmediatas que las entidades de crédito ofrecen a sus clientes, con objeto de darles la posibilidad de realizar a través de la web y aplicaciones móviles que ponen a disposición de éstos, entre otros casos de uso, envíos y solicitudes de fondos entre particulares.

Los envíos y solicitudes de dinero entre particulares (siempre y cuando ambos estén dados de alta en el servicio ofrecido por su entidad de crédito), se produce de forma inmediata y de cuenta a cuenta, sin necesidad de incluir en el momento de su realización el número de cuenta IBAN del destinatario.

Cabe remarcar que es indispensable para hacer uso del Servicio que ambos usuarios intervinientes en la operación (ordenante y beneficiario) estén registrados en el mismo, de modo que ambos queden sometidos al cumplimiento de los términos y condiciones suscritos con sus respectivas entidades de crédito, así como y entre otros a las medidas de control aplicadas por dicha entidad y a las medidas de diligencia debida como paso previo a su registro.

Sociedad de Procedimientos de Pago, S.L. (en adelante SdPP), es responsable de los datos que constan en el Directorio del servicio Bizum, base de datos que incluye los datos necesarios de los usuarios del Servicio para poder prestarse conforme a la finalidad para la que ha sido definido, esto es, el envío de dinero de un usuario registrado a otro, o la solicitud de dinero de un usuario registrado a otro.

El servicio Bizum se presta y opera a través de las aplicaciones móviles bancarias de aquellas Entidades bancarias adheridas al Servicio, que son a su vez destinatarias de los datos del Directorio con la finalidad de poder identificar al emisor y el receptor con ocasión del envío o solicitud del dinero en cada caso habilitando así el correcto funcionamiento del Servicio. Las Entidades bancarias adheridas también podrán prestar el servicio Bizum, a su criterio, mediante sus sitios web o home banking puestos a disposición de sus clientes.

Todo usuario del servicio Bizum se ha de registrar en el mismo usando un identificador principal que será su teléfono móvil. Además, es condición indispensable para ser usuario de Bizum el ser titular de una cuenta bancaria (IBAN) en cualquiera de las Entidades adheridas al Servicio. Junto con estos datos, se recaban otros como el nombre y apellidos del usuario (detalle de los datos tratados en epígrafe 8 sobre el Registro de Actividades) necesarios para operar el servicio Bizum de forma correcta y de acuerdo con los Términos y Condiciones suscritos por los usuarios antes de registrarse. Una vez aceptados los Términos y Condiciones, así como la Política de Privacidad del Servicio, un usuario Bizum podrá acceder a la operativa de envío de cantidades o solicitud de cantidades a cualquier otro usuario registrado introduciendo únicamente el número de teléfono de dicho usuario o seleccionándolo desde su agenda de contactos. En este sentido respecto del deber de información, se ha establecido en los requisitos y exigencias mínimas y comunes entre las Entidades adheridas del Servicio y SdPP, que en el momento de registrarse el interesado en el servicio Bizum y previamente a otorgar su consentimiento para el uso de sus datos en los términos establecidos en la normativa vigente de protección de datos, con la finalidad de operar el Servicio de forma correcta, se le ofrezca información suficiente, clara y sencilla sobre los destinatarios de los datos, entre los que se encuentran SdPP, el conjunto de Entidades adheridas, así como los beneficiarios y ordenantes de las transferencias, esto es, el resto de usuarios miembros del servicio Bizum.

Adicionalmente, y respecto a la afirmación del reclamante incluida en el apartado "HECHOS QUE MOTIVAN LA RECLAMACIÓN" sobre "…y extraer sus datos

identificativos (nombre, iniciales y, en algunas ocasiones, alguno o los dos apellidos)" se informa de que durante el proceso de alta de los usuarios en Bizum y de acuerdo con lo definido en los Reglamentos del Servicio y su cuerpo normativo, las Entidades Adheridas asignarán a dichos usuarios un "nombre de usuario" o alias, que se corresponderá con su nombre y las iniciales de sus dos apellidos y que tendrá un fin identificativo del destinatario de una operación de transferencia inmediata. El hecho de que a través del uso del servicio Bizum, un usuario registrado pueda consultar previamente a ordenar o solicitar la transferencia inmediata, datos identificativos básicos del usuario con el que quiere operar se configura como una medida de seguridad y una mejora de la experiencia del usuario en cuanto a fiabilidad del Servicio ya que ofrece al interesado la oportunidad de verificar la identidad de la contraparte previamente a hacer cualquier disposición de capital, evitando fraudes y/o reclamaciones posteriores. En cualquier caso, este tratamiento de los datos es informado previamente al usuario del Servicio el cual acepta la comunicación de los datos, como se expuso anteriormente, entre otros, a los beneficiarios y ordenantes de las transferencias inmediatas para lo cual otorga su consentimiento de forma expresa, libre e informada para la contratación del Servicio Bizum, de acuerdo con la normativa vigente en materia de protección de datos. Por tanto, ni la consulta acerca de si un usuario es miembro del servicio Bizum, ni el conocer datos identificativos básicos de los usuarios con los que se quiere operar, constituyen violaciones de seguridad de los datos personales, sino medidas que aportan una experiencia de uso del Servicio segura y que evitan el fraude y los procesos de reclamaciones por cantidades enviadas o solicitadas a usuarios erróneos o fraudulentos.

Los datos personales involucrados en la petición de información en virtud del requerimiento N/Ref: E/08452/2020 son:

- Nombre e iniciales de apellidos de los usuarios registrados en el servicio Bizum - Nombre y apellidos de los usuarios registrados en el servicio Bizum

- Teléfono móvil de los usuarios registrados en el servicio Bizum

Respecto a la afirmación del reclamante "El reclamante sostiene que esta operación se podría automatizar con un script, que permitiría recopilar los datos de identidad de los aproximadamente 9 millones de usuarios de los que dispone el servicio." algunas consideraciones:

- El acceso a los datos identificativos básicos y pseudoanonimizados (véase un nombre con dos iniciales que a nuestro juicio no identifica directamente a una persona física inequívocamente) por parte de los usuarios registrados en el servicio Bizum, es un acceso lícito para cumplir con las finalidades expuestas anteriormente (prevención del fraude, experiencia de uso segura) que es en todo caso informado y aceptado por cada uno de los usuarios registrados respecto de sus datos en el momento de darse de alta en el Servicio.

- Cualquier acceso ilícito a esos datos para finalidades que contravengan las previstas en los Términos y Condiciones y en la Política de Privacidad del Servicio y/o en la normativa vigente en materia de protección de datos será responsabilidad de quien o quienes operen esos accesos y utilicen los datos para finalidades ilícitas.

- Además, y como se explicará en el epígrafe séptimo del presente documento, resulta altamente improbable el ejecutar un script como el apuntado por el reclamante, sin que los sistemas de control del tráfico y fraude de la infraestructura del Servicio y/o de las Entidades adheridas lo detectaran, bloqueando así al o a los usuarios sospechosos de la iniciación de operaciones masivas con fines fraudulentos.

Cabe, por último mencionar, que en el momento de definir el servicio Bizum y su funcionamiento, habiendo tenido en cuenta los conceptos y obligaciones de privacidad desde el diseño, así como la normativa vigente en cada momento de protección de datos, se ha valorado positivamente la funcionalidad de ofrecer el nombre y las dos iniciales de los apellidos de la contraparte, al cliente final del Servicio garantizando una experiencia de uso segura, obteniendo previamente su consentimiento informado para el alta en el Servicio sobre el uso de sus datos y sus destinatarios, versus la baja probabilidad y existencia de incentivos para que alguien pueda construir un mecanismo informático capaz de obtener la asociación completa de los nombres y teléfonos del total de los usuarios que forman parte del servicio Bizum.

El servicio Bizum, respecto de los datos identificativos teléfono móvil, nombre y apellidos de cada usuario registrado realiza básicamente dos tratamientos:

i) Almacenamiento en el Directorio de usuarios del Servicio cuyo responsable es SdPP.

ii) *Transmisión entre Entidades adheridas con las que los usuarios se dan de alta para poder procesar las solicitudes y envíos de transferencias inmediatas.*

Los datos que conforman el Directorio de usuarios registrados en el Servicio se almacenan en bases de datos a las que se les aplican medidas de seguridad de cifrado y se comunican entre las partes que operan el Servicio (SdPP, las Entidades Adheridas y los terceros delegados con funciones de procesador o infraestructura) utilizando líneas de comunicación privadas y cifrando los canales y los datos con sistemas seguros que garantizan la confidencialidad, integridad y disponibilidad de los datos personales. Además, el acceso a los datos está restringido a las Entidades adheridas al Servicio y a aquellos terceros en los que hayan podido delegar competencias (p.e. los procesadores) siendo este acceso a través de un canal privado y mediante el uso de claves y firmas criptográficas específicas que aseguran que quien accede es quien dice ser y está autorizado para ello.

Adicionalmente a las medidas de seguridad técnicas previamente descritas, cabe mencionar otras medidas implantadas en el servicio Bizum con el objetivo de minimizar sus riesgos operativos, pero también con el objetivo de evitar posibles violaciones de la seguridad con afectación a datos personales. De este modo, el Servicio cuenta con limitaciones que permiten realizar un número determinado de solicitudes de cantidades, así como incluir un número máximo de destinatarios en un mismo envío con lo que se evita un uso masivo del Servicio y se es capaz de detectar un comportamiento anómalo del mismo desde la compañía que lo opera."

Aportan copia del registro de actividades de tratamientos.

1. Con fecha 22 de febrero de 2021, en el marco de las actuaciones de inspección de referencia se solicitó ampliación de información y documentación especto a las políticas de seguridad al responsable del tratamiento. Del escrito de respuesta se desprende lo siguiente:

   Respecto al análisis y gestión de riesgos de seguridad:

   Manifiestan que de acuerdo con la normativa vigente, SdPP, en su condición de responsable del tratamiento de los datos del servicio Bizum, a través de Redsys, quien actúa en calidad de encargado del tratamiento, habiendo sido asimismo designado por SdPP como proveedor de la infraestructura técnica del servicio puesta a disposición de las entidades adheridas al mismo, dispone de una estructura claramente establecida para la gestión de los riesgos derivados del tratamiento y la prestación del servicio Bizum.

   Aportan copia de la metodología e informe de análisis de riesgos de fecha 1 de julio de 2020. El diseño de la metodología ha tenido en cuenta, entre otras, las siguientes características:

   Alinear las necesidades del análisis de riesgos de Seguridad de la Información, sujeto a la norma ISO/IEC 27001 con las del análisis de riesgos operacionales para la continuidad de negocio, sujeto a la norma ISO/IEC 22301 e ISO/IEC 20000 unificarlas en un único análisis de riesgos.

   Incluir el detalle de los activos, amenazas y controles/medidas de seguridad que apliquen a cada proceso de negocio y al mismo tiempo hacer manejable la evaluación de riesgo.

   Constituir un apoyo sólido sobre el que sustentar futuros procesos de evaluación, auditoría, certificación.

   Ninguno de los riesgos analizados alcanza niveles altos o muy altos, disponiendo de niveles de riesgos moderados. El nivel de riesgo residual del servicio es bajo.
   Tras la adopción del plan de tratamiento de riesgos el valor del riesgo es bajo.

   Respecto a las políticas de seguridad y auditorias de seguridad de los sistemas:

   Aportan relación de las políticas de seguridad específicas conforme a las cuales el servicio Bizum opera.

   Aportan copia del índice del contenido de las auditorias y manifiestan que el servicio Bizum se encuentra dentro del alcance.

2. Con fecha 22 de febrero de 2021, solicitó información respecto a las medidas de seguridad específicas implantadas con el fin de evitar para evitar un uso masivo fraudulento del servicio BIZUM y capaz de detectar un comportamiento anómalo del mismo desde la compañía que lo opera. En el escrito de respuesta se hace una descripción de las siguientes medidas:

- Barreras externas a la Infraestructura Bizum que debería superar un atacante inicialmente para poder llevar a cabo el acceso a los datos:

o El posible o posible atacantes tendrían que ser usuarios/clientes registrados e identificados de al menos una de las Entidades bancarias adheridas a Bizum (o haber suplantado a dichos usuarios habiendo superado primeramente todas las medidas de seguridad establecidas por las entidades para ello en sus propios canales de acceso al servicio Bizum (App, sitios web, home bankings...)

o XXXXXXXX.

o XXXXXXXX.

o XXXXXXXX.

- Barreras establecidas en la propia infraestructura del servicio Bizum:

o XXXXXXXX.

o Las peticiones de acceso al servicio se canalizarían desde las entidades a la infraestructura de Bizum, donde se encuentran las siguientes barreras limitativas:

♣ XXXXXXXX.

♣ XXXXXXXX.

1. Con fecha 18 de diciembre de 2020, el subinspector actuante realizó las siguientes comprobaciones:

- Se realiza un alta de usuario en el servicio BIZUM a través de la app móvil de la entidad ING BANK N.V., Sucursal en España (en adelante, ING) con la que tiene suscrito un contrato de cuenta bancaria. Se verifica que para realizar el alta es necesario aceptar los términos y condiciones del servicio, además de confirmar el número de teléfono móvil y la cuenta bancaria a través del cual se usa el servicio.

- Se realiza un envío de dinero a un número de teléfono móvil no registrado en BIZUM, comprobando que aparece la siguiente notificación: "*No está registrado en BIZUM. Le enviaremos una invitación para que se registre. Si en 48 horas no se registró se cancelará el envío*"

Así mismo se comprueba que en la línea móvil se recibe un SMS con el siguiente contenido: *"Hola.* ***A.A.A.*** *CL te ha hecho un BIZUM de 1 EUR. Date de alta en tu banco antes de 2 días y recíbelo al instante. +info bizum.es."*

- Se accede a la opción de envío de dinero a número de teléfono móvil registrado en BIZUM, se selecciona de la agenda un número de teléfono registrado en BIZUM, se selecciona siguiente y se comprueba que antes de confirmar la operación aparece en el nombre e iniciales de los apellidos del beneficiario.

Se confirma la operación y aparece la siguiente notificación: "*El dinero llegará a su destino inmediatamente"*

Se comprueba que en la cuenta bancaría se anota el apunte con los siguientes datos: *"Transferencia Bizum emitida*", el importe, el concepto y la fecha.

- Se repite la operación anterior comprobando que antes de confirmar la operación es posible volver a la selección del número de teléfono destinatario, se selecciona un nuevo número y nuevamente aparece nombre e iniciales de los apellidos del nuevo destinatario o en su caso el literal: "*No está registrado en BIZUM. Le enviaremos una invitación para que se registre. Si en 48 horas no se registró se cancelará el envío".* Se ha reiterado esta comprobación hasta 10 veces en la misma sesión con números distintos.

- Se comprueba que los *"Términos y condiciones del servicio"* tienen el siguiente contenido:

"El presente documento contiene los términos y condiciones aplicables al Servicio Bizum (en adelante, el Servicio) asociado a tu/s cuentas bancaria en ING BANK N.V., Sucursal en España (en adelante, ING).

1) *DESCRIPCIÓN DEL SERVICIO*

Se trata de un servicio que te permite, en cualquier momento, realizar las siguientes operaciones a través de la aplicación de banca móvil de ING:

a) *Enviar dinero de tu cuenta bancaria en ING a la cuenta de un particular que también esté dado de alta en el Servicio Bizum, que lo recibirá inmediatamente.*

   En caso de que la persona a la que quiere enviar dinero no tenga contratado el Servicio de Bizum, podrás invitarle a que contrate el Servicio Bizum

b) Solicitar dinero a un particular para que lo envíe a tu cuenta.

c) *Recibir dinero en su cuenta de ING asociada al servicio de Bizum de un particular que también esté dado de alta en el Servicio Bizum*

   Al ser un servicio asociado a tu cuenta bancaria en ING, las operaciones quedan reflejadas en los movimientos de la misma.

1) *ALTA EN EL SERVICIO*

   Al darte de alta en el Servicio, aceptas los presentes términos y condiciones del Servicio.

   Para darte de alta en el Servicio, debes: (i) confirmar tu número de teléfono móvil que debe ser el mismo que tengas registrado en ING como teléfono de contacto, y que se utiliza como identificador a efectos de la prestación del Servicio; y (ii)

seleccionar la cuenta bancaria en ING a la que debe asociarse el Servicio y que, sirve como cuenta de abono de las operaciones del Servicio.

Puedes modificar tu cuenta asociada en cualquier momento, y puedes seleccionar tu cuenta bancaria en la que quieres que se cargue cada operación de envío, antes de iniciarla. No obstante, en caso de que modifiques tu número de teléfono móvil de contacto, ten en cuenta: (i) que para poder operar de nuevo a través del Servicio, será necesario que vuelvas a darte de alta confirmando tu nuevo número de teléfono móvil, (ii)que las operaciones pendientes asociadas al número anterior se cancelarán de manera automática y, (iii) que los particulares, para enviarte o solicitarte dinero, deben tener el número correcto.

El número de teléfono móvil asociado al Servicio únicamente puede estar registrado como identificador a efectos de la prestación del Servicio en una entidad adherida.

2) *FUNCIONAMIENTO DEL SERVICIO*

Para operar a través del Servicio debes seguir las indicaciones que aparecen en ******URL.1****, en la aplicación de banca móvil de* ***I****NG, en la web del proveedor del Servicio:* ******URL.2****.*

3.1. Envío/Solicitud de dinero a través del Servicio

Puedes enviar/solicitar dinero a un particular siempre que estés dado de alta correctamente en el Servicio, desde la aplicación de banca móvil de ING.

En caso de envío de dinero a un particular que no esté dado de alta en el Servicio, la operación quedará pendiente de ejecución durante el plazo máximo de dos (2) días hasta ese particular se dé de alta en el Servicio. Si no lo hace en dicho plazo, la operación no se realiza. Adicionalmente, en el caso de que el particular al que quieres enviar/solicitar dinero no esté dado de alta en el Servicio, puedes invitarle a que se dé de alta, informándole a través del servicio de mensajería, de forma gratuita.

3) *LÍMITES DEL SERVICIO*

Importe mínimo de cada operación: 0,50 euros.

Importe máximo de cada operación: 500 euros.

Importe máximo enviado a un mismo particular por día: 2.000 euros.

Número máximo de solicitudes enviadas/transferencias recibidas por un mismo particular por mes: 150.

4) *OTRAS FUNCIONALIDADES*

Podrás consultar a través del Servicio en la aplicación de banca móvil de ING, las transferencias emitidas y recibidas, así como las que estén pendientes de

autorización. Además, los datos relativos a estas transferencias quedarán reflejados en los movimientos de tu/s cuenta/s bancarias en ING asociadas al Servicio y que podrás consultar en la web de ING y en la aplicación de banca móvil de ING.

5) *DURACIÓN DEL SERVICIO*

El Servicio se presta con carácter indefinido.

Cancelación/desactivación por tu parte:

En cualquier momento, puedes cancelar el Servicio, dándote de baja en el mismo.

Además, dispones de un plazo de catorce (14) días, a contar desde el día siguiente a la fecha de alta en el Servicio, para renunciar a la aplicación de los presentes términos y condiciones, contactando por teléfono con el Servicio de Atención al Cliente de ING.

Cancelación/bloqueo por parte de ING:

ING puede cancelar el Servicio en cualquier momento, y sin motivo alguno, comunicándotelo con, al menos, dos (2) meses de antelación salvo que la normativa aplicable establezca un plazo superior a la fecha en que el Servicio deba considerarse cancelado.

Asimismo, al ser un servicio asociado a tu cuenta bancaria en ING, en caso de cancelación de la misma, el Servicio queda igualmente cancelado.

Además, ING puede bloquear el Servicio por razones objetivamente justificadas relacionadas con la seguridad adoptada para el correcto funcionamiento del Servicio, la sospecha de una actividad fraudulenta o un mal uso del mismo y/o si su uso pudiera suponer un aumento significativo del riesgo de hacer frente a tus obligaciones de pago.

6) *MODIFICACIÓN DEL SERVICIO*

ING podrá modificar los presentes términos y condiciones, así como incluir otros nuevos en cualquier momento, comunicándotelo con, al menos, dos (2) meses de antelación - salvo que la normativa aplicable establezca un plazo superior a la fecha de aplicación de los mismos. Puedes oponerte a su aplicación antes de que termine dicho plazo sin ningún coste para ti. Tu oposición supondrá la cancelación inmediata del Servicio. No obstante, en caso de que las modificaciones o nuevos términos y condiciones sean más favorables para ti, podrán aplicarse de inmediato y sin previo aviso. En todo caso, los términos y condiciones del Servicio estarán disponibles en todo momento ******URL.1****.*

7) *SUJECCIÓN AL CONTRATO DE PRESTACIÓN DE SERVICIOS DE ING*

ING presta el Servicio dentro de la operativa prevista en el Contrato de Prestación de Servicios que tienes suscrito con esta entidad. Por tanto, resulta aplicable, en

todo caso, lo dispuesto en este contrato, en especial, lo relativo a tus obligaciones de diligencia y responsabilidad en caso de uso fraudulento, adopción de medidas de seguridad, custodia de claves y elementos de seguridad que permitan el uso del Servicio, y notificación en caso de sustracción o pérdida de los mismos.

8) *TRATAMIENTO DE DATOS PERSONALES*

ING tratará tus datos personales que nos has facilitado en el registro para permitir el uso del Servicio. Para ello, es imprescindible que estos datos (nombre y apellidos, DNI, número de teléfono, dirección postal y de correo electrónico e IBAN) se comuniquen a la Sociedad de Procedimientos de Pago, S.L. (Bizum), con domicilio en C/ ******DIRECCIÓN.1*** *y a las sociedades que figuran en* ******URL.3****.*

Asimismo, te informamos de que los datos de la operación realizada podrán ser comunicados a los beneficiarios y a los ordenantes. No obstante, lo anterior, el dato relativo al IBAN del ordenante y del beneficiario de la operación, en ningún caso, será facilitado a ninguna de ambas partes de forma completa, a fin de que este dato no sea conocido íntegramente por la otra parte interviniente en la operación.

Dado que el Servicio te permite acceder y seleccionar de tu agenda de contactos del teléfono el número al que quieres enviar o solicitar dinero es necesario, para poder operar, que tus contactos puedan ver si tienes el Servicio activado porque en tu contacto se incluirá el logotipo de Bizum y por otro lado, tu podrás saber si tus contactos lo tienen contratado de la misma forma. Asimismo, ING necesariamente tendrá que tener acceso a tu agenda de contactos para poder prestarte el Servicio pero, en ningún caso, esta información será usada por ING para otras finalidades distintas de las indicadas en este documento.

Por otro lado, ING te informa de que si envías dinero a una ONG será necesario que comunique a dicha ONG tu nombre, apellidos y NIF con el fin de que ésta pueda cumplir con la normativa fiscal sobre la Renta de las Personas Físicas en vigor remitiendo, a dichos efectos, una declaración informativa sobre los donativos recibidos durante un año natural, en los términos previstos en la citada norma.

Podrás ejercer tus derechos de protección de datos enviando tu solicitud junto con la fotocopia de tu DNI a ******EMAIL.1****. Asimismo, podrás contactar con nuestro Delegado de Protección de Datos en la dirección* ******EMAIL.2****.*

Por último, ING te informa que esta cláusula se complementa con la cláusula "Protección de Datos para clientes y potenciales de ING" de tu contrato con nosotros.

9) *NORMATIVA APLICABLE Y JURISDICCIÓN*

Los presentes términos y condiciones se rigen por la legislación española y la jurisdicción de los tribunales españoles competentes."

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 "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, se reclama la existencia potencial de una quiebra de seguridad de datos personales, fundamentada en el hecho, de que a través de la app de BIZUM, se puede conocer si el titular de un número de teléfono móvil está inscrito en el servicio, y extraer sus datos identificativos (nombre, iniciales y, en algunas ocasiones, alguno o los dos apellidos). Pudiendo automatizarse esta operación con un script, dando lugar a una brecha de confidencialidad.

La reclamada aporta copia de la metodología e informe de análisis de riesgos de fecha 1 de julio de 2020, resultando que ninguno de los riesgos analizados alcanza niveles altos, siendo los niveles de riesgos moderados y respecto al nivel de riesgo residual del servicio, es calificado como bajo. Asimismo, aportan relación de las políticas de seguridad específicas, conforme a las cuales el servicio Bizum opera y copia del índice del contenido de las auditorias, manifestando que el servicio Bizum se encuentra dentro del alcance.

Por lo que respecta a las medidas adoptadas para evitar un uso masivo fraudulento del servicio y detectar un comportamiento anómalo, se detallan barreras "externas", entre ellas las propias establecidas por las entidades financieras adheridas al sistema, tales como la obligación de ser usuario registrados, la necesidad de "hackear" la aplicación móvil bancaria para poder inocular un script, así como vulnerar las alertas cuando se dan peticiones masivas, y por supuesto el coste de tiempo que sería necesario para ejecutar el ataque. Adicionalmente Bizum posee sus propias medidas, entre ellas, el caudal máximo de conexiones concurrentes asignada a cada entidad, el uso de un sistema de inteligencia artificial que realiza predicciones de uso y si se da una desviación significativa, se generaría una alerta, que provocaría la comprobación manual de la misma. Por tanto de la documentación analizada, se desprende que el reclamado dispone de medidas de seguridad razonables en función de los posibles riesgos estimados. A este respecto, indicar que el 4 de mayo se recibe notificación de una brecha de confidencialidad, detectada los días 28 y 29 de abril a través de los controles anteriores y el que para su resolución el día 29 de abril, ha implicado el bloqueo de siete usuarios y la monitorización de sus actividades .

En lo que afecta al acceso a los datos, la reclamada afirma que éste, está restringido a las Entidades adheridas al Servicio y aquellos terceros en los que hayan podido dele-

gar competencias (p.e. los procesadores), siendo este acceso a través de un canal privado y mediante el uso de claves y firmas criptográficas específicas, que aseguran que quien accede es quien dice ser y está autorizado para ello.

Asimismo se ha confirmado por la inspección, accediendo a la página web de una entidad adherida en la que se informa de los datos que son recabados y que es imprescindible la comunicación tanto a la reclamada como a las sociedades que figuran en ******URL.3***. Se indica además que los datos podrán ser comunicados a los beneficiarios y a los ordenantes, así como otra información que será visible para los usuarios, cumpliendo con lo establecido en el art 13 del RGPD, referente a la información que ha de facilitarse al interesado. Asimismo, se constata la licitud del tratamiento conforme a lo establecido en el art 6.1.b) del RGPD, al ser éste necesario para la ejecución del servicio objeto del contrato. En consecuencia, consta la licitud de los tratamientos realizados por el reclamado, así como la existencia de medidas técnicas y organizativas razonables para evitar la incidencia denunciada.

III

Por lo tanto, se ha acreditado que la actuación del reclamado 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 al reclamante ***A.A.A.*** y al reclamado **SOCIEDAD DE PROCEDIMIENTOS DE PAGO, S.L.,** con CIF B87599478.

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