- **Procedimiento Nº: PS/00418/2019**

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 30/10/2018, remitidas por la Agencia Vasca de Protección de Datos, tuvieron entrada en esta Agencia sendas reclamaciones formuladas por ***A.A.A., B.B.B., C.C.C.*** y ***D.D.D.*** (en adelante, los reclamantes) contra la entidad ZIURTAPEN ETA ZERBITZU EMPRESA-EMPRESA DE CERTIFICACION Y SERVICIOS IZENPE, S.A., con NIF ***A01337260*** (en adelante IZENPE o la reclamada), en relación con el proceso de recogida de datos biométricos de los ciudadanos vascos, particularmente de los usuarios del Servicio Vasco de Empleo LANBIDE, apoyada en comunicaciones expuestas en tablones de anuncios de las oficinas de esta entidad con el texto siguiente:

"Próximamente va a ser necesario la identificación digital de los/as usuarios/as de Lanbide. Por ello le invitamos a que una vez finalizada su atención pase por el puesto de recogida de datos biométricos".

Los reclamantes consideran que, si la recogida de datos se establece como obligatoria para formalizar determinados trámites, el consentimiento no sería libre. Entienden que se vulnera lo establecido en el Considerando 60 del Reglamento (UE) 2016/679, que obliga al responsable a facilitar al interesado cuanta información *"sea necesaria para garantizar un tratamiento leal y transparente"* y a *"informar a los interesados si están obligados a facilitar los datos y de las consecuencias en el caso de que no lo hicieran"*; y Considerando 43 del mismo Reglamento, según el cual *"para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de los datos en un caso concreto en el que exista un desequilibrio claro entre el interesado y el responsable del tratamiento, en particular cuando el responsable sea una autoridad pública"*.

Añaden que el dictamen 3/2012, sobre la evolución de las tecnologías biométricas, del Grupo de Trabajo del Artículo 29, ya advirtió que para poder considerar libremente otorgado el consentimiento tiene que haber una alternativa válida para la identificación.

Aportan copia del acuerdo de colaboración suscrito por LANBIDE e IZENPE para la puesta en marcha de medios de identificación electrónicos basados en la captación de datos biométricos, de 26 de octubre de 2017 (publicado el 26/03/2018), que regula el despliegue de medios de identificación electrónica de personas físicas, basado en la captación de datos biométricos. Según consta en el acuerdo, cuyo contenido consta reseñado en el Hecho Probado Tercero, LANBIDE actuará como entidad de registro de IZENPE para la expedición de medios de identificación digital y firma electrónica. Asimismo, se especifica que IZENPE (prestador de servicios de confianza) será responsable de los ficheros que tratan los datos y que LANBIDE actúa como encargado del tratamiento.

Con motivo de estas reclamaciones, que fueron inicialmente presentadas ante la Agencia Vasca de Protección de Datos, esta entidad, con fecha 06/07/2018, realizó inspección en una de las dependencias de LANBIDE. En el documento elaborado por esta actuación, que consta aportado por uno de los reclamantes, la inspección actuante señaló lo siguiente:

. Se verificó el proceso de recogida de huellas, que conlleva el tratamiento del DNI/NIE/Pasaporte; recogida de las huellas de los diez dedos de las manos y la imagen facial.
. Los representantes de la entidad manifestaron que se dispusieron diez puestos operativos para la experiencia piloto de recogida de huellas, habiendo recabado hasta la fecha 5900 datos biométricos de demandantes de empleo y de la renta de garantía de ingresos. La recogida tiene carácter voluntario.
La previsión es ampliar la recogida en las 43 oficinas de Lanbide a finales de 2018.
. LANBIDE no utiliza los datos biométricos para la identificación de los usuarios al no estar operativo el sistema. Dichos datos son almacenados por IZENPE
. Incorpora el folleto informativo expuesto en el tablón, cuyo detalle ya ha sido reseñado, la cláusula informativa que se entrega en las oficinas y el formulario para ejercicio del derecho de cancelación (el contenido de esta cláusula informativa consta reseñado en el Hecho Probado Quinto).

La Agencia Vasca de Protección de Datos inadmitió las reclamaciones mediante resolución de 29/10/2018, también aportada por uno de los reclamantes, en la que se acuerda, asimismo, el traslado de las mismas a esta Agencia. Considera la Agencia Vasca de Protección de Datos que LANBIDE actúa solo como una entidad de registro, siendo la entidad responsable de la recogida de datos IZENPE (sociedad pública constituida por el Gobierno vasco y las Diputaciones Forales), sobre la que dicha Agencia no dispone de competencias, al ser una sociedad mercantil no contemplada en la Ley vasca de protección de datos.

SEGUNDO: Las reclamaciones reseñadas fueron trasladadas a IZENPE que, con fecha 05/12/2018, informó al respecto lo siguiente:

1.- En el año 2002, la Administración General de la comunidad Autónoma de Euskadi y las Diputaciones Forales, a través de sus respectivas sociedades anónimas públicas informáticas, constituyeron la sociedad IZENPE para el desarrollo de la identificación electrónica.

Tiene la consideración de Prestador de Servicios de Confianza según el Reglamento (UE) Nº 910/2014, es decir, entidad prestadora de servicios de confianza: identificación electrónica, firma electrónica, etc.

IZENPE forma parte del sector público vasco y tiene la condición de medio propio personificado de Eusko Jaurlaritzaren Informatika Elkartea - Sociedad Informática del Gobierno Vasco, S.A. (Ejie), Lantik, S.A., Informatika Zerbitzuen Foru Elkartea - Sociedad Foral de Servicios Informáticos S.A. (IZFE) y del Centro de Cálculo de Álava, S.A. (CCASA) según lo determinado en Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europea y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

Según el estatuto de la sociedad, aportado por IZENPE con su respuesta, los encargos que le efectúen los poderes adjudicadores de los que IZENPE es medio propio: (i) tendrán

naturaleza instrumental y no contractual, por lo que a todos los efectos, tienen carácter interno, dependiente y subordinado; (ii) se articularán mediante encargos, que precisarán el objeto, plazos y demás condiciones del encargo; (iii) serán de ejecución obligatoria; (iv) se retribuirán mediante tarifas fijadas por el órgano encomendarte; y (v) llevarán aparejada la potestad para el órgano que confiere el encargo de dictar las instrucciones necesarias para su ejecución.

Constituye su objeto:
a) El fomento de las relaciones electrónicas sobre redes de telecomunicaciones, con las necesarias garantías de seguridad.
b) La prestación, en el ámbito de las instituciones que integran el sector público vasco, de servicios de seguridad, técnicos y organizativos, en las comunicaciones a través de técnicas y medios electrónicos, informáticos y telemáticos.
c) La emisión y gestión de medios y sistemas de identificación electrónicos para la identificación, autenticación, firma y/o sellado electrónico, a personas o entidades públicas o privadas.
d) Servicios de consultoría y cualquier otro relacionados con los párrafos anteriores.

2.- Desde 2016, en su calidad de medio propio de las Administraciones que participan en su capital, y por encargo de las mismas, y en el marco del Reglamento (UE) Nº 910/2014, IZENPE viene desarrollando el proyecto de emisión de medios de identificación con certificado centralizado (en la *nube)* para personas físicas denominados B@k y B@KQ. Busca dotar a la ciudadanía de un medio de identificación, siempre voluntario, de fácil uso en las relaciones telemáticas con las Administraciones vascas según los requisitos de cada procedimiento y/o servicio.

> . Se define B@K como un medio de identificación electrónica de nivel bajo, formado por un número de referencia coincidente con el DNI/NIE/Pasaporte del usuario y una contraseña; y un certificado no cualificado emitido en un repositorio centralizado que servirá para los actos de firma.
> . Se define B@K Q como un medio de identificación electrónica de nivel medio, formado por un número de referencia coincidente con el DNI/NIE/Pasaporte del usuario y una contraseña; un juego de coordenadas con 16 posiciones; y un certificado cualificado de firma electrónica emitido en un repositorio centralizado de IZENPE que servirá para los actos de firma.

Además, para dar respuesta a nuevas necesidades asociadas a los sistemas de identificación, IZENPE ha completado los medios B@K y B@KQ con otros factores de autenticación biométricos como la huella dactilar y/o fotografía.

IZENPE manifiesta que el encargo para la prestación de diversos servicios relativos a la identificación y firma electrónica se realiza a IZENPE, como medio propio, mediante Resolución (aporta copia) del Director de Servicios del Departamento de Gobernanza Pública y Autogobierno, que tiene atribuida en la efectiva implementación en las administraciones públicas de la Administración electrónica en los procedimientos administrativos y en la gestión de los asuntos públicos, así como la declaración y gestión de los servicios comunes de tramitación telemática de la Administración Pública de la Comunidad Autónoma de Euskadi.

En esta resolución se señala que el encargo constituye la actividad esencial de IZENPE, según sus estatutos, y son de obligado cumplimiento para esta sociedad.

Entre otros servicios electrónicos, el encargo tiene por objeto el Sistema integrado de claves eIDAS y comprende la creación, verificación y validación de claves de identificación y su preservación.

La supervisión de la correcta prestación del servicio corresponde a la Dirección de Atención a la Ciudadanía e Innovación y Mejora de la Administración.

En relación con estos encargos, IZENPE advierte que el correspondiente al año 2018 se encuentra pendiente de firma.

3. Por su parte, LANBIDE, creado por la Ley 3/2011, de 13 de octubre, es un organismo autónomo de carácter administrativo adscrito al Departamento de Empleo y Políticas Sociales del Gobierno Vasco, dotado de personalidad jurídica propia y plena capacidad de obrar para el cumplimiento de sus fines, que tiene encomendadas, entre otras funciones, la gestión de la intermediación y la ejecución de las políticas activas de empleo dentro del ámbito competencial de Euskadi, así como, la gestión de las prestaciones económicas de garantía de ingresos en los términos establecidos en Ley 18/2008, de 23 de diciembre, para la Garantía de Ingresos y para la Inclusión Social.

A finales del año 2017, atendiendo al volumen de solicitudes gestionadas por el organismo y al elevado número de personas que atienden en sus oficinas, el Gobierno Vasco y el Departamento de Empleo y Políticas Sociales en el marco del proceso de reforma y modernización de LANBIDE y con el propósito de prestar un mejor servicio a la ciudadanía, decidió implantar de forma experimental en la Comunidad Autónoma de Euskadi, un sistema de identificación y reconocimiento electrónico mediante factores biométricos (huella digital y rasgos faciales) para todos los trabajadores y usuarios del servicio, a fin de mejorar, simplificar y hacer más eficiente la gestión administrativa, dando respuesta así a las necesidades actuales de la sociedad.

Añade que el proyecto apuesta por habilitar un sistema digital, simple, rápido y seguro de identificación y autenticación de los interesados en el procedimiento administrativo ajustado a las previsiones legales de la LPACAP, y a los requerimientos del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, RGPD), quedando garantizados plenamente los derechos de la ciudadanía. Asimismo, el proyecto contribuye a consolidar la administración electrónica y avanzar en la digitalización del funcionamiento interno de la Administración.
El proceso de despliegue del sistema se inicia con el registro previo de los parámetros biométricos elegidos.

En este contexto, y para favorecer el despliegue e implantación de la huella digital como medio de identificación en LANBIDE, esta entidad e IZENPE suscribieron un acuerdo de colaboración, de 26/10/2017 (publicado el 26/03/2018), para la puesta en marcha de medios de identificación electrónicos basados en la captación de datos biométricos, que ha sido recientemente prorrogado y modificado para adecuarlo al nuevo marco regulador en materia de protección de datos establecido tras la entrada en vigor, el 25 de mayo de 2018, del RGPD, mediante la adenda suscrita el 15 de octubre de 2018, en la que se modifica la cláusula séptima, relativa a protección de datos. En su nueva redacción se especifica que LANBIDE no podrá utilizar los datos para fines propios, que los tratará de acuerdo con lo

determinado por IZENPE.

Tras la firma del Acuerdo de colaboración y en su condición de Entidad de Registro, LANBIDE pone a disposición de IZENPE sus espacios físicos, así como el personal encargado de las tareas de identificación y registro de usuarios, que es debidamente formado por esta última, llevando a cabo las siguientes actuaciones:
Verificación de su identidad.
Captura las huellas digitales.
Toma de una fotografía del rostro.
Recabar la firma de la solicitud de emisión de B@k y B@kQ.
Registrar/grabar los datos biométricos obtenidos (fotografía y huella dactilar) en el sistema de gestión de identidades de IZENPE.

A este respecto, manifiesta IZENPE que la participación en este proceso es totalmente voluntaria para los usuarios, que son debidamente informados sobre el tratamiento de datos y su finalidad conforme a lo establecido en el artículo 13 del RGPD, recabándose su consentimiento explícito (artículo 7 RGPD).

LANBIDE cuenta con una red de 43 oficinas distribuidas por todo el territorio de la Comunidad Autónoma de Euskadi. La planificación del proyecto para proporcionar medios de identificación electrónicos con factores biométricos a la ciudadanía contempla tres fases:
. En una primera fase se instaló un puesto de recogida de datos biométricos en una de las oficinas de LANBIDE, de forma experimental.
. En una segunda fase, correspondiente al estado actual y siguiendo con la modalidad experimental, el despliegue se ha ampliado a 10 puestos de registro, ubicados en sendas oficinas.
. En una tercera fase (a ejecutar en el segundo trimestre del 2019) se prevé extender el número de puestos de registro a la totalidad de las oficinas de LANBIDE y, además, se pretende que este medio de identificación pueda ser utilizado, por las personas que voluntariamente lo elijan, para el acceso a los servicios de esta entidad.

En primera instancia, el público destinatario para el uso de este sistema de identificación es el formado por el colectivo de personas usuarias del Servicio Vasco de Empleo: demandantes de empleo en general, participantes en acciones formativas y servicios de orientación, así como los solicitantes de prestaciones sociales de la Renta de Garantía de Ingresos (RGI) y de la Prestación Complementaria de Vivienda (PCV). Se trata de un colectivo cercano a las 300.000 personas.

El despliegue del proyecto ha ido acompañado de mensajes de comunicación que han sido expuestos en carteles informativos (aporta fotografía) en las oficinas de LANBIDE. La información expuesta, que no establecía la obligatoriedad de su uso para acceder a los servicios que presta el organismo, fue modificada el pasado mes de julio. El texto de este cartel es el siguiente:

“En esta oficina se ha instalado un puesto de recogida de datos biométricos para la identificación digital de las personas usuarias de LANBIDE.
Si usted está interesado/a le invitamos pasar por el puesto nº… para obtener la información que precise y, en su caso, realizar los trámites necesarios”.

La entidad IZENPE indica que, hasta noviembre 2018, aproximadamente 9.000 personas han

solicitado este medio de identificación con factores biométricos y que, en este tiempo, 3 personas han ejercido el derecho a la revocación del consentimiento otorgado.

4. Paralelamente, atendiendo a la regulación sobre esta materia establecida en el RGPD (que otorga a los datos biométricos el carácter de datos sensibles y cuya base legitimadora ha de estar establecida por Ley), el Gobierno Vasco ha promovido una reforma de la Ley 3/2011, de 13 de octubre, de creación de Lanbide-Servicio Vasco de Empleo, actualmente en proceso, que incorpora al texto legal la utilización de sistemas biométricos para la identificación de las personas usuarias de sus servicios y/o beneficiarios de sus prestaciones.

Hasta que no se regule por Ley el uso de este sistema de identificación, únicamente está siendo probado de forma experimental, resultando necesario testar su funcionamiento y continuar con el desarrollo de la herramienta tecnológica que la sustenta.

A tal fin, mediante Resolución del Director General de LANBIDE de fecha 30 de noviembre de 2018, se acuerda *"Encargar a la empresa Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A., como medio propio personificado de la Administración General de la Comunidad Autónoma de Euskadi, la provisión de servicios para la implantación en Lanbide de un sistema que permita la identificación de personas basados en factores biométricos"*.

Según se indica en esta resolución, los servicios objeto del encargo se llevarán a cabo en varias fases y comprende la implantación de una solución informática para la solicitud de medios de identificación B@k y B@Kq con factores biométricos, proporcionando un sistema de gestión de registro de factores biométricos de identificación ciudadana basados en reconocimiento facial y huella dactilar consistente en el registro y consulta de datos de identificación.

El apartado sexto de esta resolución, dedicado a la protección de datos, señala que el régimen aplicable será el previsto en el RGPD, que IZENPE es responsable del tratamiento, el cual está identificado en su registro de tratamiento con el detalle siguiente:
. Tratamiento: gestión de medios de identificación basados en parámetros biométricos.
. Datos objeto de tratamiento: identificativos, categorías especiales de datos: datos biométricos.
. Período de conservación: 7/15 años, según el medio de identificación no cualificado/cualificado, desde la formalización de la solicitud.

El encargo comienza su vigencia el 01/01/2018 y se extiende hasta el 31/12/2019.

5. IZENPE formula una serie de consideraciones en relación con lo manifestado por los reclamantes, de las que cabe destacar las siguiente:

. El interés de IZENPE de completar los medios de identificación con factores biométricos deriva del impulso realizado por el Gobierno Vasco y el Departamento de Empleo y Políticas Sociales para implantar nuevas tecnologías de identificación de la ciudadanía, y concretamente del encargo vigente sobre la necesidad de llevar a cabo esta adecuación para satisfacer las necesidades de gestión de LANBIDE.

. Procede aclarar que es LANBIDE, y no IZENPE, quien establece la finalidad del uso de estos medios de identificación en la prestación de sus servicios.

. La emisión de los medios B@k y B@kQ es voluntaria y únicamente se expiden cuando previamente el solicitante ha cumplimentado y firmado la correspondiente solicitud de emisión.

. Se ha elaborado un documento del tipo *"preguntas frecuentes"* específico para el proyecto de Lanbide aclarando aspectos relativos a los derechos y riesgos asociados, así como sobre las circunstancias de la utilización de estos medios de identificación (se adjunta copia).

. IZENPE dispone del Informe de Evaluación de Impacto correspondiente al tratamiento de datos que conlleva este sistema de identificación con factores biométricos. Este informe concluye que dicho sistema no supone un riego significativo para la privacidad de los interesados. Con su escrito adjunta el Informe de evaluación de impacto de 10/07/2018 y una actualización de noviembre de 2018.

. IZENPE ha revisado y aclarado la información dada hasta la fecha sobre las características del medio, adecuándola a los requerimientos del RGPD, y se han adecuado al RGPD los formularios de solicitud de medios de identificación B@k y B@kQ con factores biométricos (el contenido de estas nuevas versiones consta reseñado en el Hecho Probado Quinto).

TERCERO: Las reclamaciones a las que se refieren las actuaciones fueron admitidas a trámite mediante resoluciones de fecha 09/01/2019.

CUARTO: A la vista de los hechos denunciados en la reclamación y de los documentos aportados por los reclamantes e IZENPE, 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 los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, 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).

En el marco de estas actuaciones previas, por la inspección actuante se solicitó información a IZENPE que, con fecha 18/02/2019, presentó la respuesta siguiente:

1. La emisión de los medios de identificación electrónica se realiza según lo determinado en el documento denominado *"Política del certificado de ciudadano"*, publicado en www.izenpe.eus y notificado al Ministerio de Industria, Turismo y Comercio (aporta copia de este documento).

Se trata de un documento que detalla y completa lo definido de forma genérica en la Declaración de Prácticas de Certificación de IZENPE, www.izenpe.eus/dpc y que describe los medios electrónicos de identificación expedidos por esta sociedad a la ciudadanía, en lo que aquí procede los medios B@k y B@kQ y define su ciclo de vida (verificación de la identidad del solicitante, procedimiento de solicitud, emisión y entrega, así como la revocación y renovación).

Todos los estados del ciclo de vida de un medio de identificación, excepto la revocación de un medio por causas técnicas, requieren que el solicitante cumplimente y firme el correspondiente formulario de solicitud. A través del formulario de solicitud se informa sobre las características del medio electrónico solicitado, condiciones de uso y legislación aplicable

en materia de datos de carácter personal; y se recaban del interesado los datos personales necesarios para la expedición del medio de identificación y su consentimiento libre, mediante la firma del mismo.

2. El número de usuarios de los que se han tomado datos biométricos antes de la modificación de los formularios de solicitud es 10.378 registros, de los cuales 3.624 son anteriores a la fecha de entrada en vigor del RGPD. Tras la modificación de los formularios de solicitud se han realizado 320 registros hasta el día 15/02/2019. El total de registros a dicha fecha asciende, por tanto, a 10.738 usuarios.
IZENPE advierte que los formularios iniciales se utilizaron desde el 26/10/2017 y que éstos fueron modificados con fecha 04/12/2018, si bien, debido a una incidencia de tipo técnico, los nuevos modelos no se han usado hasta el 5 de febrero de 2019 (ambos formularios se aportaron con su escrito de 05/12/2018).

Aporta copia de estos formularios. El nuevo modelo de solicitud que, según indica IZENPE, se elaboró en diciembre de 2018, coincide con el reseñado en el Antecedente Segundo.

El formulario que manifiestan haber utilizado inicialmente y que aportan con este escrito de 18/02/2019 contiene la información siguiente:

Se informa que la identificación electrónica, B@k está formada por un número de referencia coincidente con el DNI/NIE del usuario y una contraseña asignados por IIZENPE; un certificado no cualificado emitido en un repositorio centralizado que servirá para los actos de firma; y datos biométricos (huella dactilar y fotografía). El medio B@kQ está formado, además, por un juego de coordenadas con 16 posiciones y un certificado cualificado de firma electrónica emitido en un repositorio centralizado seguro de IZENPE, la “nube”, que servirá para los actos de firma.

El detalle de los datos recabados y la información básica de protección de datos coincide con la reseñada en el Hecho Probado Quinto.

Por otra parte, el formulario aportado dispone de un espacio habilitado para la firma del solicitante y, a continuación, se añade un apartado sobre *“Emisión y Activación”* con el texto siguiente: *“Tras la identificación y firma del formulario de solicitud, el solicitante podrá iniciar la emisión de B@k. El proceso comienza con el envío de un SMS con la contraseña (que por seguridad debe cambiar). Por último, Izenpe generará un certificado no cualificado de firma electrónica emitido en un repositorio centralizado seguro”*.

En el caso de B@kQ se incluye otro apartado más, sobre la identificación del solicitante (de manera presencial, a distancia utilizando medios de identificación electrónica distintos del certificado, certificado de firma electrónica cualificada u otros medios) y la documentación de identificación aportada o que autoriza a consultar, según el interesado sea ciudadano español, ciudadano miembro de la UE/EEE o extracomunitario.

3. El único tratamiento que se realiza sobre dichos datos, al igual que con los obtenidos con posterioridad a la modificación, es el derivado de la *“gestión de medios de identificación basados en parámetros biométricos”*, cuya finalidad es el registro de solicitudes y la emisión de estos medios de identificación, y en su caso la revocación, en calidad de prestador de servicios de confianza.

En el futuro, las administraciones de la Comunidad Autónoma podrán utilizar los sistemas como medios de identificación en la gestión de la identificación de los ciudadanos.

4. En respuesta a la consulta que le fue realizada sobre si han establecido un procedimiento para revisar los consentimientos obtenidos antes de la modificación de los formularios de solicitud, manifiestan que todas las solicitudes han requerido que el interesado cumplimentara el formulario y consintiera en el tratamiento de sus datos mediante la firma del mismo, y que ha ofrecido la información referente a las características del medio y sus condiciones de uso, por lo que no han considerado necesario obtener nuevos consentimientos.

QUINTO: Con fecha 04/11/2019, tuvo entrada en esta Agencia un nuevo escrito de la entidad IZENPE, en el que manifiesta que ha llevado a cabo un análisis exhaustivo de la normativa aplicable a su actividad, y, en relación con el tratamiento de datos biométricos, señala lo siguiente:
. El *"Convenio de Colaboración"* suscrito con LANBIDE se formuló de acuerdo con la normativa de protección de datos anterior a la plena aplicabilidad del RGPD.
. Que una vez aprobada la Ley 9/2017, de 8 de noviembre, de contratos del sector público, IZENPE pasó a tener la consideración de medio propio personificado de una serie de Administraciones territoriales vascas, concretamente de la Administración General de Euskadi, de la cual depende LANBIDE, según consta en la modificación de los estatutos de la mercantil que aporta.
. Una vez modificados los estatutos, LANBIDE dictó resolución de 30/11/2018, anterior a la entrada en vigor de la LOPDGDD, en la que se recogía la condición de medio propio personificado de IZENPE, si bien, se sigue aplicando a esa relación el esquema basado en la LOPD de 1999.
. Como consecuencia de lo anterior, el estudio realizado recomienda la reformulación de los roles como responsable y encargado del tratamiento de datos, teniendo en cuenta la condición de IZENPE como medio propio de sus administraciones matrices.

Añade que en el momento en que se llevó a cabo el tratamiento no estaba en vigor la LOPDGDD y la exigencia de que el tratamiento de datos biométricos requiriera un reconocimiento expreso en una norma con rango de ley, cuando dicho tratamiento fuera realizado por las Administraciones Públicas.

Asimismo, advierte que, como conclusión del mencionado análisis, y considerando que a partir de la entrada en vigor de la LOPDGDD cualquier tratamiento de datos por parte de los poderes públicos (más aún aquel que tenga por objeto la recogida de datos biométricos, ya sea directamente o en su condición de medio propio personificado; esto es, a través de encargos) que se fundamente en razones de interés público o en el ejercicio de potestades públicas requiere su cobertura o previsión por una norma con rango de ley; y dado que, en la actualidad, no existe en el ordenamiento jurídico vasco una norma con rango de Ley que prevea expresamente la posibilidad de llevar a cabo el tratamiento analizado fundado en razones de interés público o en el ejercicio de poderes públicos, como medida de prudencia, IZENPE ha trasladado a LANBIDE la decisión de suspender provisionalmente el tratamiento del registro de datos biométricos para la emisión de medios de identificación a la ciudadanía mientras no exista tal cobertura legal. Por lo tanto, desde el 26 de octubre de 2019 este tratamiento de datos no se está realizando.

La puesta en marcha de este sistema de identificación es una posibilidad que se prevé expresamente en la proposición de Ley para la Garantía de Ingresos y para la inclusión,

actualmente en trámite, que presumiblemente dará cobertura legal a LANBIDE, en los términos establecidos por el artículo 8.2 de la LOPDGDD, para llevar a cabo la identificación de la ciudadanía por medio de sistemas biométricos, lo cual podría acabar con las dudas razonables que se presentan en el actual tratamiento de datos personales.

En base a ello, y teniendo en cuenta que IZENPE no puede ser sancionada por un tratamiento de datos realizado en su condición de medio propio personificado que actúa mediante encargos, solicita el archivo de las actuaciones. Estima, además, que procede dicho archivo considerando que cuando se inició el tratamiento de datos biométricos no estaba definido legalmente que el consentimiento del afectado no fuera base legítima suficiente para tal tratamiento.

SEXTO: Con fecha 18/12/2019**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la entidad IZENPE, de conformidad con lo previsto en el artículo 58.2 del RGPD, por la presunta infracción del artículo 4 de la LOPD y artículo 5 del RGPD, determinando que la sanción que pudiera corresponder sería de apercibimiento, sin perjuicio de lo que resulte de la instrucción.

Asimismo, a los efectos previstos en el artículo 49 de la LOPD y artículo 58.2.d) del RGPD, en dicho acuerdo de inicio se advertía a la entidad citada que las infracciones imputadas, de confirmarse, podrán conllevar la adopción de las medidas necesarias para adecuar a la normativa de protección de datos personales las operaciones de tratamiento que realiza, la información ofrecida a sus clientes y el procedimiento mediante el que los mismos prestan su consentimiento para la recogida y tratamiento de sus datos personales, con el alcance expresado en los Fundamentos de Derecho del repetido acuerdo y sin perjuicio de lo que resulte de la instrucción.

SÉPTIMO: Notificado el citado acuerdo de inicio, IZENPE presentó escrito de alegaciones en el que solicita que se dicte resolución por la que se acuerde el archivo del procedimiento, de acuerdo con las consideraciones siguientes:

I.- Desde el punto de vista formal, señala que no le consta ninguna actuación de investigación específica, más allá de dar traslado a esa parte para que formulara alegaciones en relación con las actuaciones previas que han determinado la apertura del procedimiento; que tampoco le consta ninguna notificación de la AEPD que indique la fecha en la que se procedió a iniciar el período de actuaciones previas de investigación, por lo cual resulta complejo determinar el cumplimiento de las exigencias de doce meses establecidas en el artículo 67.2 de la LOPDGDD; ni tiene constancia formal de las reclamaciones que fueron admitidas a trámite, los términos exactos en que se formularon y si las mismas reproducen lo expuesto ante la Agencia Vasca de Protección de Datos.

En este apartado, IZENPE solicita copia de las reclamaciones y de las actuaciones previas de investigación, reservándose el derecho a formular alegaciones complementarias.

II.- Considera oportuno concretar el espacio temporal sobre el que se proyectan las reclamaciones formuladas y su marco normativo, para delimitar correctamente las responsabilidades y definir el papel de IZENPE, en su condición de responsable del tratamiento o, en su caso, encargado del tratamiento, y definir si su actuación es formal e instrumental o se trata de una actuación sustantiva resultado del ejercicio de la propia competencia. Con este propósito, realiza la siguiente secuencia temporal de los hechos:

a) El Acuerdo de colaboración Lanbide/Izenpe, de 26 de octubre de 2017 (publicado en marzo de 2018), cuyo objeto único era la configuración de LANBIDE como entidad de registro, se dicta siendo directamente aplicable la LOPD y la Ley Parlamento Vasco 2/2004, de ficheros de carácter personal y creación AVPD. En ese acuerdo, de conformidad con el artículo 12 de la entonces vigente LOPD, IZENPE adquiere la condición de responsable de ficheros, que no debe confundirse con la condición de responsable del tratamiento, según el RGPD.

b) Tras la entrada en vigor, el 08/03/2018, de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (en adelante, LCSP), se produjo la adaptación de los Estatutos de IZENPE y su consideración como medio propio personificado de la Administración General de la Comunidad Autónoma y de sus organismos públicos (como es el caso de LANBIDE), de conformidad con lo establecido en el artículo 32 de la citada Ley. No obstante, hasta entonces, la sociedad mercantil ya tenía la condición de medio propio y servicio técnico, desde la modificación de sus Estatutos Sociales en el año 2010. Y, por consiguiente, actuaba materialmente a través de encomiendas que le formalizaban las entidades matrices, entre ellas LANBIDE.

c) Cuando se dicta el Acta de Inspección de la AVPD, el 6 de julio de 2018, como consecuencia de las denuncias cursadas en relación con las pruebas biométricas realizadas, estaba vigente la LCSP y ya era plenamente aplicable el RGPD, que estaba dando sus primeros pasos con muchas incógnitas sobre su alcance; pero se trata de hechos anteriores a la exigencia de norma con rango de ley para disponer de una base legítima de tratamiento por misiones realizadas en interés público o en el ejercicio de poderes públicos (artículo 8 de la LOPDGDD). En ese Acta se constata lo siguiente: 1) se da por bueno el Acuerdo de colaboración y el reparto de roles allí recogido; 2) no se define qué entidad cumple el papel de responsable del tratamiento y cuál la de encargado según el RGPD; 3) se parte del criterio del consentimiento como base legítima del tratamiento (artículo 6 RGPD); y 4) se concluye que ha podido haber una infracción de la normativa en materia de protección de datos formalizada a través del RGPD.
Además, destaca IZENPE, cuando se puso en marcha el sistema de identificación (octubre de 2017) aún no estaba plenamente efectivo el RGPD, por lo que las pruebas biométricas no tenían la consideración de datos de carácter especial. Esto ocurrió a raíz de la plena aplicabilidad del RGPD.

d) El 26 de octubre de 2018 se aprueba la prórroga y modificación del Acuerdo de colaboración suscrito el año anterior. Sigue estando vigente la LOPD en todo aquello que no hubiese quedado desplazada por el RGPD, que era completamente aplicable. También se había aprobado el Real Decreto-Ley 5/2018, cuya disposición transitoria se refería a los contratos de encargados y a su aplicabilidad hasta 2022.

e) La Resolución R18-071 de la AVPD inadmite las denuncias, conforme a lo dispuesto en la Ley 2/2004 del Parlamento Vasco, que no atribuye competencias a esa entidad para incoar un expediente sancionador a una sociedad mercantil de titularidad pública.

f) Con fecha 30/11/2018, en el marco del RGPD y de la LCSP, mediante Resolución de la Dirección General de LANBIDE se formaliza el encargo a IZENPE *de "la prestación de servicios de identificación basados en factores biométricos"*, en su condición de medio propio personificado del Gobierno Vasco y, concretamente, de LANBIDE. Esta Resolución sigue impregnada, en parte, del reiterado acuerdo de colaboración, puesto que se caracteriza a

IZENPE como responsable del tratamiento, pero su cláusula tercera explicita que la supervisión de la correcta prestación del encargo es de LANBIDE, y se indica en la cláusula segunda que corresponde a este organismo autónomo la definición de los fines del tratamiento.
Considera IZENPE que el medio propio personificado al que se realiza el encargo (aún tratándose de una entidad de registro) no puede ser en ningún caso responsable del tratamiento, dado que esa entidad instrumental no dispone de la competencia material que le obligue a ello.

g) A partir de esa fecha, IZENPE, teniendo en cuenta el expediente seguido en la AEPD, entonces en fase de actuaciones previas, y las dudas que había abierto la configuración jurídica del modelo de actuaciones hasta entonces existente, optó por plantear la no renovación de la prórroga, paralizar el tratamiento hasta que existiera una base legítima mediante una Ley de cobertura (que está en tramitación en el Parlamento Vasco) y dar traslado a la AEPD de tales extremos mediante escrito de 04/11/2019, al efecto de que no se llevara a cabo la incoación del expediente sancionador, atendiendo a su consideración de entidad instrumental como medio propio personificado que no definía los fines ni el objetivo del tratamiento. Dada esta condición, IZENPE no podía disponer de forma efectiva (no formal) de poder alguno de supervisión sobre la entidad de la que era receptora de la encomienda o encargo, pues –como se viene reiterando- aquélla no era titular de la competencia material alguna sobre los citados fines u objetivos del tratamiento.

III.- La naturaleza jurídica de IZENPE: sus consecuencias en el presente supuesto.

IZENPE es una empresa que presta servicios de confianza en materia de identificación electrónica, de acuerdo con lo establecido en el Reglamento (UE) 910/2014 (Reglamento eIDAS) y la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, y tiene la consideración de medio propio personificado, con carácter instrumental, dependencia indirecta y naturaleza vicarial en relación con las entidades o Administraciones Públicas para las que actúa. Según los Estatutos de IZENPE, los encargos que reciba de los poderes adjudicadores de los que es medio propio tendrán naturaleza instrumental y no contractual, tienen carácter interno, dependiente y subordinado; se articulan mediante encargos de ejecución obligatoria, según las instrucciones del órgano que confiere dicho encargo.

IV.- El carácter de IZENPE como entidad prestadora de servicios de confianza, en el campo de las transacciones electrónicas de ámbito europeo o transnacional. según el Reglamento eIDAS y su aplicación al presente caso. De lo establecido en este Reglamento, IZENPE destaca lo siguiente:

a) Esta normativa ha de aplicarse de forma que se cumplan los principios relativos a la protección de datos personales. El citado Reglamento eIDAS y el RGPD son dos conjuntos normativos conexos, pero que no son intercambiables, puesto que ambos establecen sus respectivos supuestos singulares de responsabilidad, confidencialidad y mecanismos de seguridad en función del círculo de atribuciones que en cada caso se lleven a cabo.
b) Así, en el marco del Reglamento eIDAS, los prestadores de servicios de confianza deben responder de los perjuicios ocasionados a cualquier persona física o jurídica, y no solo física, como ocurre en el ámbito del RGPD.
c) El objetivo del reiterado Reglamento eIDAS no es otro que *“proporcionar un marco coherente con vistas a garantizar un elevado nivel de seguridad y de certidumbre jurídica de los servicios de confianza”*. Y, a tal efecto, se crea la etiqueta de confianza UE y se garantiza

el reconocimiento mutuo de firmas electrónicas. Asimismo, se regulan los certificados cualificados, la firma electrónica avanzada, el sello electrónico cualificado y avanzado, etc.
d) El artículo 24 del Reglamento eIDAS prevé expresamente en su apartado 2 que *"Los prestadores cualificados que prestan servicios de confianza cualificados: (…) j) Garantizarán un tratamiento lícito de los datos personales de conformidad con la Directiva 95/46/CE"*. Sin embargo, al ser la sociedad mercantil un medio propio personificado de una entidad que es titular material de la competencia y que define los fines y objetivos (por qué y para qué) del tratamiento de datos y su aplicación concreta (gestión y control de determinadas prestaciones sociales), ese reenvío a la normativa de protección de datos debe aplicarse a la delimitación de las figuras de responsable y encargado del tratamiento, claves en la resolución del presente caso.

De lo expuesto, IZENPE extrae las conclusiones siguientes:
a) El Reglamento eIDAS no refleja, al ser anterior, la diferenciación de roles entre responsable y encargado del tratamiento tal y como ha sido ulteriormente precisada por el RGPD, por lo que la interpretación de sus previsiones normativas debe ser adecuada a esa nueva reconfiguración del papel de ambas figuras.
b) Cabe, diferenciar las responsabilidades derivadas de un incumplimiento de las obligaciones contenidas en el Reglamento eIDAS, de aquellas otras responsabilidades que se produzcan como consecuencia de los tratamientos de datos de carácter personal, que no se regirán por ese conjunto normativo sino por el RGPD.
c) Se deben diferenciar aquellos casos en que la actuación de la entidad prestadora de servicios de confianza es de carácter general (emisión de sistemas de identificación que tienen por destinatarios servicios de carácter general o trámites antes cualquier entidad o administración pública), de aquellas otras actuaciones singulares o específicas que buscan la emisión de un sistema de identificación vinculado al ejercicio de competencias materiales concretas atribuidas a una determinada entidad. En el primer caso, la entidad prestadora del servicio de confianza tendrá la consideración de responsable del tratamiento; y no en el segundo caso, en el que se establece un mecanismo de control y gestión vinculado a las competencias de la entidad matriz y no de la entidad instrumental.
d) El Reglamento de 2014 se dicta con un marco normativo europeo distinto del que actualmente rige la normativa de protección de datos: el RGPD. Y, por tanto, es el RGPD el que define los roles de responsable del tratamiento y de encargado del tratamiento.

V.- Por otra parte, argumenta que, como medio propio de una Administración Pública o entidad de Derecho Público, le es aplicable el régimen sancionador establecido para la entidad que formula el encargo, es decir, el previsto en el artículo 77 LOPDGDD. Sigue la doctrina, apoyada por las Juntas Consultivas, según la cual cuando actúa una entidad mercantil como medio propio personificado de una Administración Pública, en la práctica está actuando materialmente la propia Administración. Y añade que, si la no imposición de sanciones económicas a una Administración Pública se justifica por el principio de Hacienda Pública, para que tales sanciones no reviertan en el presupuesto público, el mismo argumento se puede extraer cuando actúa una entidad mercantil en el contexto indicado.

VI.- La afectación al principio de proporcionalidad en las medidas de captación de datos biométricos en su modalidad de huellas dactilares. La aplicación excepcional de la captación. Su finalidad. El principio de proporcionalidad en sentido estricto. Aplicación de la normativa de 1999 bajo los presupuestos de las previsiones del RGPD.

La recogida de datos biométricos puede ser lícita cuando hay consentimiento del interesado y

el juicio de proporcionalidad es pertinente y no excesivo.

Desde la óptica del juicio de proporcionalidad, la prueba biométrica era idónea, por cuanto atendía a un fin legítimo, y se llevó a cabo la información requerida en el RGPD (con dificultades de interpretación debido a su reciente aplicabilidad); desde la misma óptica, se entiende cumplimentado el juicio de necesidad, ya que la medida de intervención es indispensable, no existiendo otras con menor injerencia que alcancen el mismo resultado o fin legítimo de simplificación de la gestión, control del fraude y control del gasto; y en cuanto al juicio de proporcionalidad estricto, en el que entran en juego los intereses en conflicto, se han producido más beneficios que cargas con la aplicación del tratamiento, tanto desde el punto de vista normativo (las ventajas para la Administración titular de la competencia y los usuarios es evidente, en la agilización del trámite) y empírico, si bien el problema radica probablemente en la dimensión de la muestra realizada (recogida de las huellas dactilares de los diez dedos de ambas manos), la cual se debe valorar atendiendo a la dimensión empírica del problema expuesto.

También en este apartado reitera IZENPE que el tratamiento de los datos biométricos se inició con el marco normativo anterior al RGPD, cumpliéndose entonces las exigencias establecidas con la única duda del alcance de la captación de las minucias de las huellas sobre los dedos de ambas manos. Así, puede suscitarse si el tratamiento era pertinente y no excesivo, pero para ello debe tenerse en cuenta que se hizo con carácter contingente y como prueba piloto. Este contexto limita o atenúa la responsabilidad, ya que cuando se inició el tratamiento no suponía incidir en datos sensibles y, por tanto, la desproporción de uso no tenían las consecuencias que se derivan de la aplicación del RGPD, también en lo que afecta a los principios de su artículo 5. A esto se añaden las dudas sobre el alcance de innumerables previsiones del nuevo marco normativo europeo, que se mantienen en lo que se refiere al reparto de roles entre responsable y encargado del tratamiento, especialmente en un caso como el presente en el que entran en juego distintos círculos aplicativos de normas en distintos ámbitos materiales y en diferentes momentos.

Plantea cómo puede imputarse una infracción grave ante una normativa que aún no ofrecía una claridad interpretativa, más aún con ausencia de jurisprudencia, y sin considerar que la entidad actuó con la confianza legítima de que su intervención era correcta, en su condición de medio propio personificado que atendía las encomiendas y encargos realizados. IZENPE no puede asumir la condición de responsable último y exclusivo del diseño del tratamiento, pues no le competía ejercer tales funciones ni tenía las atribuciones para definir el alcance y objetivos de ese tratamiento.

Asimismo, cabe recordar que el sistema de identificación basado en factores biométricos en el ámbito de gestión de LANBIDE únicamente contempló la fase piloto, cuyo objetivo era la evaluación y experimentación de las tecnologías biométricas que fueran a formar parte del proyecto final, que no ha llegado a ponerse en marcha. La toma de las minucias de las diez huellas dactilares tenía como objetivo la evaluación del comportamiento del sistema desde las perspectivas tecnológicas, de experiencia de usuario y desde el ámbito de la protección de datos personales. Se pretendía adoptar la solución óptima, reduciendo la tasa de error y el tiempo de respuesta, asociada a la minimización de la toma de datos biométricos. En este sentido, el proyecto piloto contemplaba la identificación basada en las minucias de una sola huella dactilar.

En todo caso, el proyecto se encuentra suspendido desde octubre de 2019 a la espera de la

aprobación de la ley correspondiente que legitime la implantación del sistema de identificación.

IZENPE aporta un *"Informe técnico"* relativo a la información que se ofrecía a los interesados, en el que reproduce el texto sobre la activación del sistema de identificación incluido en los formularios de solicitud de medios de identificación, que requiere la finalización del proceso por parte del usuario para su utilización, y destaca que estos medios conllevan la emisión de un certificado de firma electrónica en un repositorio centralizado seguro albergado en IZENPE.

OCTAVO: Con fecha 02/07/2020 se formuló propuesta de resolución en el sentido siguiente:

1. Que por la Directora de la Agencia Española de Protección de Datos se sancione a la entidad IZENPE, por una infracción de los artículos 4.1 de la LOPD y 5 del RGPD, tipificada en los artículos 44.3 c) de la LOPD y 83.5 a) del RGPD, respectivamente, con sanción de apercibimiento.

2. Que por la Directora de la Agencia Española de Protección de Datos se requiera a la entidad IZENPE, para que en el plazo que se determine, adecúe a la normativa de protección de datos personales las operaciones de tratamiento que realiza, con el alcance expresado en el Fundamento de Derecho VIII. En concreto, se propone que IZENPE cese en la utilización ilícita de los datos de carácter personal relativos a las huellas dactilares de los interesados, por lo que deberá mantener el registro de una sola huella dactilar, a su elección, y proceder a la eliminación del resto de huellas (las correspondientes a nueve dedos de las manos).

NOVENO: Notificada a la entidad IZENPE la citada propuesta de resolución, con fecha 16/07/2020, se recibió en esta Agencia escrito de alegaciones en el que reproduce, básicamente, sus alegaciones anteriores, en base a las cuales solicita el archivo de las actuaciones:

I. Después de señalar que la fase de admisión a trámite establecida en el artículo 65.4 de la LOPDGDD era prescindible en este caso, dado que las reclamaciones se presentaron ante la AVPD, que se declaró incompetente, se refiere IZENPE a la duración de las actuaciones previas de investigación, que el artículo 67 de la LOPDGDD fija en doce meses. Entiende IZENPE que cabe diferenciar entre la dimensión formal y material del caso para concluir que, aunque formalmente se cumplió dicho plazo, el mismo solo puede emplearse cuando la complejidad de la investigación aconseje extenderla hasta sus límites máximos, sin que pueda hacerse un uso discrecional, como en este caso, en el que la apertura del procedimiento se fundamenta sustancialmente en las actuaciones que llevó a cabo la Agencia Vasca, sin que la AEPD llevase a cabo ninguna actuación material de investigación efectiva, habiéndose limitado a solicitar información o documentación adicional. En su conjunto, considerando todas las fases indicadas, las actuaciones de investigación alcanzan casi veinte meses, y en base a ello concluye que la AEPD dilató artificialmente el período de investigación, incumpliendo materialmente el plazo máximo establecido.

Un caso como este, en el que intervienen dos autoridades de control, no está previsto en el citado artículo 67, pero se aproxima materialmente a la relación entre la autoridad de control de un Estado miembro y la AEPD, cuando esta última recibe un expediente admitido por aquella. En este caso, el plazo de doce meses debería iniciarse con el traslado de las actuaciones.

En cuanto a las consecuencias de esta caducidad cita la STS de 13 de mayo de 2019 (RC 2415/2016), que sigue la estela de otro pronunciamiento precedente (STS de 6 de mayo de 2015, RC 3438/2012), en la que se recoge una nueva doctrina en virtud de la cual el período de actuaciones previas debe proyectarse sobre la realización efectiva de actividades de investigación sin proceder artificialmente a su prolongación, pues ello pudiera implicar incurrir en un fraude de ley.

Esta extensión temporal ha perjudicado a IZENPE, que ha ido acumulando a los hechos probados intervenciones posteriores en materia de protección de datos y ampliando el foco cuantitativo de posibles infracciones. En el propio escrito de propuesta de resolución se indica que son 3.624 los registros de formularios anteriores a la fecha de entrada en vigor (rectius, de efectividad o plena aplicabilidad) del RGPD, siendo a fecha de 15/02/2019 10.738 usuarios el número de registro.

II. Destaca el interés de la entidad IZENPE en definir la posición que adopta en el nuevo marco normativo, como entidad mercantil con carácter de medio propio personificado de un conjunto de administraciones públicas territoriales y de las entidades instrumentales que dependen de aquellas, dado que son constantes los encargos de tratamientos de datos, y plantea una serie de cuestiones preliminares:

a) Tener en cuenta las diferentes normativas que convergen es importante para deslindar las presuntas responsabilidades, considerando de manera especial el cambio que ha supuesto el RGPD en algunos aspectos como son la posición del responsable y encargado del tratamiento y el régimen sancionador aplicable a empresas públicas que tienen la condición de medio propio personificado después de la aprobación de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP), que acentúa la posición de dependencia funcional de estos medios, de modo que no puede atribuírseles una responsabilidad más gravosa en materia de protección de datos personales que a la empresa matriz, que es la que tiene la competencia material y la que define los fines.

No basta para ello, como hizo la AVPD y luego ratifica la AEPD, con la mera traslación formal de unos Acuerdos de colaboración que se suscribieron en 2017 y se fueron prorrogando posteriormente, pues estos acuerdos se redactaron de conformidad con la LOPD y la normativa reglamentaria que la desarrollaba (al hablar de responsable de ficheros). Una vez entrada en vigor la LCSP la única vía para formalizar esas relaciones entre LANBIDE e IZENPE eran los encargos a medio propio personificado, algo que -por circunstancias ajenas a esta mercantil- no se formalizó hasta el 30 de noviembre de 2018 y, además, manteniendo, también de forma errónea, los roles de responsable del tratamiento y de encargado del tratamiento de forma cruzada (esto es, asignando el papel de responsable de tratamiento a quien debía ser encargado y viceversa, como consecuencia de la traslación automática de la figura del responsable del fichero a la de responsable de tratamiento, que no son en absoluto coincidentes ni tienen por qué tener esa correspondencia).

b) Según el artículo 2 de la Ley 2/2004, de ficheros de datos de carácter personal de titularidad pública y creación de la Agencia Vasca de Protección de Datos, esta autoridad de control no tiene competencia para depurar las responsabilidades que se derivaran de un tratamiento llevado a cabo por una sociedad mercantil de carácter público, aunque las acciones o participaciones correspondan en su totalidad a poderes públicos vascos, por lo que se encontrarían sometidos al control y fiscalización de la AEPD.

Esta situación cambia con la LOPDGDD, cuyo artículo 57 establece que las autoridades autonómicas de protección de datos podrán ejercer las potestades establecidas en los artículos 57 y 58 del RGPD cuando, de acuerdo con la normativa autonómica, se refieran a *"tratamientos de los que sean responsables las entidades integrantes del sector público de la correspondiente Comunidad Autónoma (…) incluidas en su ámbito territorial (…)"*. En estos momentos al no haberse modificado la Ley 2/2004, la competencia seguiría siendo transitoriamente de la AEPD, pero la finalidad fundamental de esa atribución genérica no puede ser otra que ampliar el foco de supervisión, como es el caso, a todas aquellas empresas públicas que son dependientes, vinculadas o están adscritas (a efectos de control económico-financiero) a una Administración matriz y que actúan como medio propio personificado de ésta o de las Administraciones que conformen el accionariado y el Consejo de Administración de tales mercantiles. El vínculo de dependencia se estrecha y atrae para sí la competencia de la autoridad de control autonómica a una esfera institucional que hasta ahora no le competía.

Ello tiene también estrechas conexiones con el alcance del régimen excepcional en materia de sanciones a las administraciones públicas y entidades dependientes que se prevé en el artículo 77 LOPDGDD, cuya lógica institucional está ayuna de fundamento salvo que se justifique que el medio propio personificado siempre que actúe de acuerdo con el encargo recibido no puede ser sancionado autónomamente y lo debe ser la Administración matriz.

III. Considera necesario precisar conceptual y normativamente algunos argumentos y expresiones que se recogen en la propuesta de resolución:

a) No es cierta la indicación: *"IZENPE ha declarado que se decidió implantar el sistema en LANBIDE de forma experimental para todos los trabajadores y usuarios del servicio (colectivo cercano a 300.000 personas), a fin de mejorar, simplificar y hacer más eficiente la gestión administrativa, dando respuesta así a las necesidades de la sociedad"*.

No se puede utilizar la expresión impersonal *"se decidió"*, puesto que el titular de la competencia material era y es LANBIDE, actuando entonces IZENPE como medio propio y servicio técnico y, a partir de la entrada en vigor de la LCSP 9/2017, como medio propio personificado. LANBIDE es la interesada en los propósitos indicados anteriormente.

b) Sobre los hechos probados concluidos a partir de los documentos formalizados, según los cuales *"IZENPE se declara responsable del tratamiento (también del fichero) y LANBIDE interviene como encargado para la mera recogida y validación de los datos y su posterior envío a IZENPE"*, señala esta entidad que la Agencia no ha realizado ningún esfuerzo interpretativo para advertir (*"una suerte de levantamiento del velo"*, dice IZENPE) que esa mercantil no podía responsabilizarse del tratamiento de acuerdo con el RGPD. Además, considerarlo como encargada del tratamiento no afecta ni modifica a posteriori los derechos de los interesados, como señala la propuesta de resolución, que en nada se ven afectados por el cambio de roles.

c) Considera errónea la interpretación de la figura del responsable del tratamiento contenida en el RGPD la afirmación realizada en la propuesta que dice así: *"Conviene, asimismo, tener presente la definición de responsable del tratamiento expresada en el artículo 4 del RGPD, que considera como tal no solo al que define los fines, sino también al que habilita los medios para el tratamiento, como hace IZENPE en este caso"*. Este artículo exige que el responsable

“determine los fines y medios del tratamiento”, no solo los medios, o se correría el riesgo de diluir los perfiles diferenciadores de responsable y encargado. Aquella lectura sería particularmente grave en relación con los medios propios personificados.

Cita el Considerando 74 del RGPD y añade que no puede ser responsable del tratamiento quién en ningún caso define los fines, aunque ponga medios para que esos fines se cumplan, pues en ese caso se haría responsable de medidas que escapan a su ámbito de actuación material, al margen de que responda como encargado por las funciones asignadas.

En ningún caso puede considerarse a IZENPE como responsable del tratamiento, por mucho que se recogiera equivocadamente tal condición en los documentos que se aportaron por la AVPD al expediente sancionador. A partir de la plena aplicabilidad del RGPD, IZENPE no podía tener tal condición pues es materialmente imposible que la mercantil defina los fines del tratamiento cuando no es titular de la competencia sustantiva a la que sirve tal tratamiento: *“mejorar, simplificar y hacer más eficiente la gestión administrativa”* de un ámbito material como son las políticas activas de empleo y la renta de garantía de ingresos en las que no tiene, ni por asomo, posibilidad alguna de intervenir, ya que no está dentro de su objeto social ni es propio de su naturaleza como medio propio personificado.

d) El planteamiento anterior no se tuvo en cuenta por la AVPD cuando resolvió inadmitir las reclamaciones.

Derivar de un documento formal que LANBIDE, entidad que fijaba los fines y se beneficiaba de los resultados del tratamiento, solo es una entidad de registro es una conclusión apresurada, ya que la normativa de protección de datos personales no se puede interpretar exclusivamente a partir de la regulación material en ese ámbito, sino a través del conjunto del ordenamiento jurídico vigente, por lo que debe precisarse, por un lado, la competencia material de la entidad que define los fines y medios del tratamiento, que es LANBIDE; y, por otro, que IZENPE tiene la consideración de medio propio personificado de las Administraciones Públicas o entidades dependientes que le realizan *“encargos”* y está, por consiguiente, sometida a un *“control análogo”* al que la entidad matriz (LANBIDE) ejerce sobre sus propios servicios administrativos, por lo que carece absoluta y totalmente de autonomía (también de competencia) para definir los fines del tratamiento y los medios que ponga en acción lo son siempre al servicio de tales fines.

e) sobre la reformulación de los roles ya anunciada, aclara IZENPE que su propósito es dejar constancia de lo siguiente:

. Que hasta 25 de mayo de 2018, reconoció en el Acuerdo de colaboración que tenía la condición de responsable de fichero, aunque ya entonces era medio propio y servicio técnico o medio propio personificado de LANBIDE en este caso. Las responsabilidades que se pudieran
derivar de las actuaciones realizadas en tal período eran en la condición de tal, pero nunca de responsable del tratamiento.
. Que a partir del 25 de mayo de 2018, IZENPE no podía tener la consideración de responsable del tratamiento, conforme a lo expuesto (no le corresponde la competencia material que determina los fines y su actúa en su condición de medio propio personificado de la entidad titular de la competencia).
. Que, tal *“reformulación”* de roles no afecta a los derechos de los reclamantes que formularon en su día la oportuna reclamación, pues ya sea LANBIDE o ya sea IZENPE, en sus roles

formales o materiales (sean de encargado o responsable y viceversa), responderían de las irregularidades hipotéticas del tratamiento realizado.
. Es necesario deslindar las figuras de responsable y encargado del tratamiento en la resolución de este procedimiento, que tendrá importantes repercusiones generales y sentará doctrina al respecto, dejando claro que la definición de los fines se vinculan necesariamente con las competencias materiales que desarrolla una entidad y no sólo con los medios que facilita para poner en marcha o aplicar un determinado tratamiento; y sin olvidar que IZENPE es un medio propio personificado controlada por entidad matriz de forma análoga al control que ejerce sobre las entidades que dependen de ella (jerarquía impropia).
. Que las autoridades de control ejercen ámbitos competenciales diferenciados en función de las administraciones y entidades del sector público de que se traten, si bien esta situación puede verse alterada en un futuro por lo establecido en el artículo 57.1 LOPDGDD.
. IZENPE tiene naturaleza de medio propio personificado y sus recursos financieros dependen exclusivamente de las Haciendas Públicas de las distintas entidades a las que prestan esos servicios mediados, por lo que carece de sentido que se le impongan multas administrativas (es una empresa pública de carácter instrumental, sometida a *"control análogo"* al existente a otro servicio administrativo y financiada exclusivamente por *"encargos"* que determinan qué se debe hacer, cómo y con qué finalidad).
En razón de lo expuesto, solicita:

a) que se proceda, por motivos formales, al archivo de las actuaciones, debiéndose estimar la caducidad del procedimiento, lo que no impide, en principio, que la AEPD lo pueda reactivar en los términos establecidos en la LPACAP; en particular la extensión artificial de las actuaciones previas de investigación, que se han prolongado más allá del plazo necesario.

b) Subsidiariamente, proceder, por motivos materiales, al archivo de las actuaciones en los términos planteados en sus escritos de alegaciones.

En el caso de que no se admitieran ninguna de las dos peticiones anteriores, se solicita:

a) Que la resolución acoja exclusivamente las responsabilidades de IZENPE como responsable del fichero del tratamiento hasta el 25 de mayo de 2018, reconociendo igualmente que, durante ese período, tenía la condición de medio propio y servicio técnico o, en su caso, de medio propio personificado de LANBIDE, y que su actuación era instrumental y no material, al carecer de las competencias sustantivas cuya eficiencia se pretendían mejorar.
b) Que, a partir del 25 de mayo de 2018, IZENPE no podía tener materialmente la condición de responsable de un tratamiento de datos, considerando que no definía los fines del tratamiento.
c) Que, las sanciones que, en su caso, se le puedan aplicar lo deberían ser como encargado del tratamiento y nunca como responsable del tratamiento, pues esta consideración fue equivocadamente atribuida por una traslación mecánica de la figura del responsable de fichero a la de responsable del tratamiento, cuando esta última se ha redefinido completamente tras la plena aplicabilidad del RGPD. Tal consideración es, asimismo, muy importante para la mercantil dada su condición de medio propio personificado de diferentes Administraciones Públicas y entidades al servicio de aquellas.
d) Que, todo lo anterior no afectaría a los derechos de los reclamantes en ningún caso. Sin perjuicio de que la reclamación inicial de tales reclamantes se dirigió ante LANBIDE, que ejercía la competencia efectiva y llevó a cabo la encomienda (formulada como *"acuerdo de colaboración"*), de conformidad con el TRLCSP de 2011, o el *"encargo"*, de acuerdo con la LCSP de 2017.

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

1.- En el año 2002, la Administración General de la Comunidad Autónoma de Euskadi y las Diputaciones Forales, a través de sus respectivas sociedades anónimas públicas informáticas, constituyeron la sociedad Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A. (IZENPE) para el desarrollo de la identificación electrónica, como sistema propio de identificación y firma electrónica.

Según consta en sus Estatutos Sociales, que se declaran reproducidos a efectos probatorios, IZENPE tiene entre su objeto social la emisión y gestión de medios y sistemas de identificación electrónicos para la identificación, autenticación, firma y/o sellado electrónicos, a personas o entidades públicas o privadas.

Tiene la consideración de prestador de servicios de confianza (identificación electrónica, firma electrónica, etc.) según el Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE; y tiene, asimismo, la condición de medio propio personificado de las entidades que participan en su capital, según lo determinado en Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europea y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

2. IZENPE ha declarado que, desde 2016, en su calidad de medio propio de las Administraciones que participan en su capital, por encargo de las mismas, y en el ámbito del Reglamento eIDAS, viene desarrollando el proyecto de emisión de medios de identificación con certificado centralizado (en la *nube)* para personas físicas, con el que se pretende dotar a la ciudadanía de un medio de identificación, siempre voluntario, de fácil uso en las relaciones telemáticas con las Administraciones vascas según los requisitos de cada procedimiento y/o servicio.

Ha desarrollado dos sistemas (B&K y B&K Q) que permiten la identificación y firma electrónica, formados por un número de referencia, contraseña, juego de coordenadas y certificado de firma electrónica.

. Se define B@K como un medio de identificación electrónica de nivel bajo, formado por un número de referencia coincidente con el DNI/NIE/Pasaporte del usuario y una contraseña; y un certificado no cualificado emitido en un repositorio centralizado que servirá para los actos de firma.
. Se define B@K Q como un medio de identificación electrónica de nivel medio, formado por un número de referencia coincidente con el DNI/NIE/Pasaporte del usuario y una contraseña; un juego de coordenadas con 16 posiciones; y un certificado cualificado de firma electrónica emitido en un repositorio centralizado de IZENPE que servirá para los

actos de firma.

IZENPE ha manifestado ante esta Agencia que el encargo para la prestación de diversos servicios relativos a la identificación y firma electrónica se realizó mediante Resolución de 14/11/2017 (que se declara reproducida a efectos probatorios), del Director de Servicios del Departamento de Gobernanza Pública y Autogobierno, en cuya estructura se integra la Dirección de Atención a la Ciudadanía e Innovación y Mejora de la Administración, que tiene atribuida *"la efectiva implementación en las administraciones públicas de la Administración electrónica en los procedimientos administrativos y en la gestión de los asuntos públicos"*, así como, *"la declaración y gestión de los servicios comunes de tramitación telemática de la Administración Pública de la Comunidad Autónoma de Euskadi"*.

Los servicios electrónicos que deberá prestar IZENPE permitirán a la Administración General de la Comunidad Autónoma de Euskadi relacionarse con la ciudadanía, las empresas privadas y con el resto de Administraciones Públicas. Entre otros servicios electrónicos, el encargo tiene por objeto el sistema integrado de claves eIDAS y comprende la creación, verificación y validación de claves de identificación y su preservación.

3. Lanbide-Servicio Vasco de Empleo, organismo autónomo de carácter administrativo adscrito al Departamento de Empleo y Políticas Sociales, y la entidad IZENPE suscribieron un acuerdo de colaboración, de 26/10/2017 (publicado el 26/03/2018), que se declara reproducida a efectos probatorios, para la puesta en marcha de medios de identificación electrónicos de personas físicas (trabajadores y usuarios de Lanbide -demandantes de empleo en general, participantes en acciones formativas y servicios de orientación, así como los solicitantes de prestaciones sociales de la Renta de Garantía de Ingresos y de la Prestación Complementaria de Vivienda; se trata de un colectivo cercano a las 300.000 personas) basados en la captación de datos biométricos. Se pretende incorporar elementos de identificación más seguros, tales como factores biométricos, entre ellos los rasgos faciales y huellas digitales. Según su parte expositiva, el acuerdo se enmarca en la Ley 39/2015, para profundizar en la implantación de la Administración electrónica, y el Reglamento (UE) 910/2014.

Mediante Resolución 156/2018, de 26 de noviembre, del Director de la Secretaría del Gobierno y de Relaciones con el Parlamento, se dispuso la publicación de dicho acuerdo de colaboración bajo el rótulo *"Acuerdo de colaboración para el despliegue del proyecto piloto de medios de identificación electrónicos basados en la captación de datos biométricos"*.

En el acuerdo se expone que LANBIDE tiene instaurada la clave operativa como medio para acreditar la identidad y tiene intención de facilitar un sistema interoperable que permita a las personas usuarias de sus servicios relacionarse con cualquier administración con las garantías legales y de seguridad; y que se pretende incorporar nuevos factores de identificación a los dos sistemas desarrollados por IZENPE (B&K y B&K Q), tales como los factores biométricos, entre los que cita los rasgos faciales y huellas digitales.

En su clausulado se indica lo siguiente:

. Izenpe es un prestador de servicios de confianza. En virtud de este acuerdo, Lanbide adquiere la condición de entidad de registro de Izenpe para la expedición de medios de identificación digital y firma electrónica B&K y B&K Q. en relación con las personas físicas usuarias que soliciten medios de identificación expedidos por IZENPE.

LANBIDE llevará a cabo las acciones siguientes: verificar la identidad; captura de las huellas digitales; fotografía del rostro; firma de la solicitud de emisión de B&K y B&K Q; registrar los datos biométricos obtenidos (huellas y foto) en el en el sistema de gestión de identidades (fichero de identidades) de Izenpe fichero de identidades de IZENPE; remitir a Izenpe la solicitud de emisión de B@k y B@k Q firmada tanto por el solicitante como por el operador de Lanbide.
. Validez un año.
. IZENPE imparte la formación y facilita el software.
. Protección de datos: IZENPE es el responsable de los ficheros declarados ante la AEPD, que tratan los datos de los distintos servicios acordados y Lanbide intervine como encargado del tratamiento, conforme al artículo 12 LOPD.

Con fecha 15/10/2018, las entidades IZENPE y LANBIDE suscribieron una Adenda del Acuerdo de colaboración de 26/10/2017, que se declara reproducida a efectos probatorios, para la prórroga del mismo por un año a contar desde el 26/10/2018 y para adaptar al RGPD la redacción de la cláusula séptima, relativa a la protección de datos, que queda como sigue:

"1.- Izenpe respecto de los datos que proporciona el solicitante de los medios de identificación, tiene la condición de Responsable del Tratamiento e identifica este servicio en el ámbito del siguiente tratamiento:
Tratamiento: Gestión de medios de identificación basados en factores biométricos.
Datos objeto tratamiento: Identificativos. Categorías especiales de datos: datos biométricos.
Periodo conservación: 7/15 años, según el medio de identificación no cualificado/cualificado, desde la formalización de la solicitud.
2.- Cuando Lanbide actúe como Entidad de Registro adquirirá la condición de Encargado de Tratamiento de los datos de carácter personal que el solicitante proporciona.
Este tratamiento consistirá en la recogida y validación de los datos y su posterior envío a Izenpe. Para la ejecución de esta prestación, Izenpe proporcionará a Lanbide acceso a las aplicaciones necesarias.
3.- Lanbide así como su personal, adquiere las siguientes obligaciones:
a) Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto del presente acuerdo.
En ningún caso podrá utilizar los datos para fines propios.
b) Tratar los datos de acuerdo con lo determinado por Izenpe.
(…)".

4.- Con motivo de las reclamaciones que han dado lugar a las presentes actuaciones, que fueron inicialmente presentadas ante la Agencia Vasca de Protección de Datos, los servicios de inspección de la misma realizaron una inspección en una de las oficinas de LANBIDE. En el Acta de Inspección elaborada, de fecha 06/07/2018, que se declara reproducida a efectos probatorios, consta lo siguiente:

<<… se solicita información sobre el proceso de recogida de huellas, ofreciéndose el personal de Lanbide a realizar una simulación del proceso completo, que conlleva el tratamiento del DNI/NIE/Pasaporte, la recogida de la huella de los diez dedos de las manos y la imagen facial…
A preguntas de los inspectores actuantes, se informa que actualmente existen 43 oficinas de Lanbide, con 600 puestos y diez puestos operativos para la experiencia piloto de recogida de huellas dactilares, habiéndose recabado hasta la fecha alrededor de 5.900 datos biométricos. Las Personas que acuden a la oficina son demandantes de empleo y de la renta de garantía

de ingresos y la recogida de sus datos biométricos tiene carácter voluntario. Cuando la persona acude a la oficina para realizar algún trámite, una vez que ha terminado, se le informa de la futura necesidad de identificación digital de usuarios, tras lo cual, se le remite al punto de recogida…

El personal de Lanbide informa a los inspectores que los datos de huella y faciales de los usuarios son recogidos por Lanbide por cuenta de la empresa de certificación y servicios Izenpe, S.A., que es quien almacena los datos. La previsión es ampliar la recogida mediante lectores de huella en las 43 oficinas de Lanbide hacia finales de 2018. En la actualidad, Lanbide no utiliza los datos biométricos con fines de identificación de los usuarios de sus servicios al no estar operativo aún el sistema.

El personal de Lanbide, a petición de los inspectores, entrega a éstos el folleto informativo sobre la recogida de datos biométricos, la cláusula informativa que se entrega en las oficinas y el modelo de ejercicio del derecho de cancelación>>.

(Posteriormente, en su respuesta a la AEPD de 05/12/2018, IZENPE manifestó que, hasta noviembre 2018, aproximadamente 9.000 personas solicitaron este medio de identificación con factores biométricos. Y en su escrito de 18/02/2019, declaró que hasta el 15/02/2019 el número de usuarios de los que se habían tomado datos biométricos ascendía a 10.738 usuarios, de los cuales 3.624 son anteriores a la fecha de entrada en vigor del RGPD).
5. Durante la inspección realizada por la Agencia Vasca de Protección de Datos en fecha 06/07/2018, se comprobó que en los tablones de anuncios de la oficina de Lanbide figuraban expuestos carteles informativos con el texto siguiente:

"Próximamente va a ser necesario la identificación digital de los/as usuarios/as de Lanbide. Por ello le invitamos a que una vez finalizada su atención pase por el puesto de recogida de datos biométricos…".

(IZENPE ha declarado ante esta Agencia que el texto del cartel informativo fue sustituido en julio de 2018 por el siguiente: *"En esta oficina se ha instalado un puesto de recogida de datos biométricos para la identificación digital de las personas usuarias de LANBIDE.*
Si usted está interesado/a le invitamos pasar por el puesto nº… para obtener la información que precise y, en su caso, realizar los trámites necesarios").

. Asimismo, durante dicha inspección se recabó el documento utilizado para facilitar a los interesados información en materia de protección de datos personales y recabar su consentimiento para la recogida de sus datos. El contenido de este documento es el siguiente:

"Izenpe le informa que a través de los datos biométricos (huellas dactilares y fotografía) que van a registrarse, podrá disponer de un medio de identificación electrónica que le permitirá relacionarse con las administraciones vascas.
Además, y según el nivel de seguridad requerido en virtud del trámite administrativo, dichos datos biométricos podrán completar el uso de los medios de identificación electrónica B@K y/o B@K Q.
Este medio de identificación está compuesto por huellas dactilares, fotografía facial del solicitante y los siguientes datos personales:
El solicitante deberá cumplimentar los siguientes datos_todos los datos son de cumplimentación obligatoria_.

Apellidos
Nombre
Número de DNI/Pasaporte
Fecha de nacimiento
Correo electrónico
Teléfono móvil de contacto

Cláusula informativa (Información básica sobre protección de datos)
Responsable: Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A.
Finalidad: Prestación y gestión de servicios asociados a los medios de identificación electrónica
Derechos: acceso, rectificación y cancelación a través, c/… o info@izenpe.com.

Información adicional
Http://www.izenpe.eus/contenidos/información/doc_comun/es_def/adjuntos/DOC_P_PDS_v1.0.pdf

Fecha y firma del solicitante".

(En el ejemplar de este formulario inicial aportado por IZENPE con su escrito de 18/02/2019 se informa que la identificación electrónica, B@k está formada por un número de referencia coincidente con el DNI/NIE del usuario y una contraseña asignados por IIZENPE; un certificado no cualificado emitido en un repositorio centralizado que servirá para los actos de firma; y datos biométricos (huella dactilar y fotografía). El medio B@kQ está formado, además, por un juego de coordenadas con 16 posiciones y un certificado cualificado de firma electrónica emitido en un repositorio centralizado seguro de IZENPE, la "nube", que servirá para los actos de firma).

. Los formularios anteriores de solicitud de medio de identificación fueron posteriormente modificados. Las nuevas versiones contienen la información básica y un enlace a la web para la información adicional. En el primer apartado de esta solicitud se explica que el medio de identificación está formado por un número de referencia u certificado no cualificado o un juego de coordenadas (según el tipo de medio) y se añade que "además, puede ser complementado por otros factores de autenticación biométricos como la huella dactilar y/o fotografía" (única referencia a los datos biométricos que aparece en estos documentos de solicitud).

En estos nuevos formularios de solicitudes de B&K y B&K Q se informa a los interesados que se trata de medios de identificación electrónica que le permitirán relacionarse con las administraciones vascas y se detalla que dichos medios de identificación están formados por un número de referencia (coincidente con el DNI/NIE/pasaporte del usuario y una contraseña), un certificado no cualificado emitido en un repositorio centralizado que servirá para los actos de firma (B@K) o un juego de coordenadas con 16 posiciones y un certificado cualificado de firma electrónica emitido en un repositorio centralizado de IZENPE que servirá para los usos de firma (B@K Q). En ambos casos, además, el medio de identificación puede ser complementado por otros factores de autenticación biométricos como la huella dactilar y/o fotografía (única referencia a los datos biométricos que aparece en estos documentos de solicitud).

Se añade que cuando el titular de B@k o B@K Q utilice el medio de que se trate para su

identificación ante un servicio electrónico, Izenpe, en el caso de que la autenticación sea correcta, ofrecerá al organismo responsable del servicio el resultado de la misma.

Con la firma de las solicitudes correspondientes, el firmante declara que ha leído y acepta los Términos y Condiciones de uso de este medio de identificación publicadas en www.izenpe.eus/condicionesuso.

En los citados formularios se recaban datos personales relativos a nombre, apellidos, DNI o pasaporte, fecha de nacimiento, correo electrónico y teléfono móvil de contacto.

En el dorso de estas solicitudes se ofrece *"Información básica sobre protección de datos"*, con el contenido siguiente:
"Responsable: IZENPE
Finalidad: Expedición y gestión del ciclo de vida del medio de identificación solicitado.
Legitimación: consentimiento del interesado
Destinatarios: no se prevé ceder o comunicar datos a terceros, salvo previsión legal, ni efectuar transferencias internacionales.
Derechos: Derecho a obtener confirmación sobre los tratamientos que de sus datos que se llevan a cabo por Izenpe.
Puede ejercer sus derechos de acceso, rectificación, supresión y portabilidad de sus datos, de limitación y oposición a su tratamiento, a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos, así como a retirar su consentimiento en cualquier momento y a presentar una reclamación ante la Agencia Española de Protección de Datos.
Podrá ejercitar estos derechos mediante petición a la dirección postal C/ Beato Tomás de Zumárraga nº. 71, 1ª planta. 01008 Vitoria-Gasteiz o de manera electrónica datos@izenpe.eus tal y como se indica en la información adicional.
Información adicional: disponible en www.izenpe.eus/datos".

Con la firma de la solicitud (incluye un espacio para la firma), según se indica en la misma, el interesado consiente a IZENPE el tratamiento de los datos de carácter personal referentes al medio de identificación solicitado.

. En su escrito de 18/02/2019, IZENPE ha declarado lo siguiente:
El número de usuarios de los que se han tomado datos biométricos antes de la modificación de los formularios de solicitud es 10.378 registros, y 320 registros más tras su modificación.
IZENPE advierte que los formularios iniciales se utilizaron desde el 26/10/2017 y que éstos fueron modificados con fecha 04/12/2018, si bien, debido a una incidencia de tipo técnico, los nuevos modelos no se han usado hasta el 5 de febrero de 2019.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada Autoridad de Control, y según lo establecido en los artículos 47, 48, 64.2 y 68.1 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para iniciar y resolver este procedimiento.

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

Con carácter previo, procede analizar la excepción planteada por IZENPE en su escrito de alegaciones a la apertura del procedimiento, relativa a la posible caducidad de las actuaciones previas de investigación. Esta entidad manifestó que no consta ninguna actuación de investigación específica, al margen del traslado de las reclamaciones, de modo que no es posible determinar el cumplimiento de las exigencias de doce meses establecidas en el artículo 67.2 de la LOPDGDD. Añade que tampoco tuvo conocimiento de la admisión a trámite de las reclamaciones.

Los trámites realizados por esta Agencia a los que se refiere IZENPE en su alegación anterior tienen que ver con el proceso de admisión a trámite de las reclamaciones recibidas, que incluyó para cuatro de las cinco reclamaciones recibidas su traslado al responsable, previo al acuerdo de admisión de la reclamación.

De conformidad con lo establecido en el artículo 55 del RGPD, la Agencia Española de Protección de Datos es competente para desempeñar las funciones que se le asignan en su artículo 57, entre ellas, la de hacer aplicar el Reglamento y promover la sensibilización de los responsables y los encargados del tratamiento acerca de las obligaciones que les incumben, así como tratar las reclamaciones presentadas por un interesado e investigar el motivo de las mismas.

Correlativamente, el artículo 31 del RGPD establece la obligación de los responsables y encargados del tratamiento de cooperar con la autoridad de control que lo solicite en el desempeño de sus funciones. Para el caso de que éstos hayan designado un delegado de protección de datos, el artículo 39 del RGPD atribuye a éste la función de cooperar con dicha autoridad.

Del mismo modo, el ordenamiento jurídico interno, en el artículo 65.4 la LOPDGDD, ha previsto un mecanismo previo a la admisión a trámite de las reclamaciones que se formulen ante la Agencia Española de Protección de Datos, que consiste en dar traslado de las mismas a los delegados de protección de datos designados por los responsables o encargados del tratamiento, a los efectos previstos en el artículo 37 de la citada norma, o a éstos cuando no los hubieren designado, para que procedan al análisis de dichas reclamaciones y a darles respuesta en el plazo de un mes. Se trata de un trámite potestativo, de modo que este traslado se lleva a cabo si la Agencia así lo estima, tal y como se decidió en este caso.

Así, de conformidad con esta normativa, con carácter previo a la admisión a trámite de las reclamaciones que han dado lugar al presente procedimiento, se dio traslado de las mismas a IZENPE para que procediese a su análisis, diera respuesta a esta Agencia y comunicara a los reclamantes la decisión adoptada al respecto.

El resultado de dicho traslado no permitió entender satisfechas las pretensiones de los reclamantes. En consecuencia, a los efectos previstos en su artículo 64.2 de la LOPDGDD,

mediante sendos acuerdos de fecha 09/01/2019, la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite las reclamaciones presentadas.

Sobre esta cuestión, IZENPE ha manifestado en sus alegaciones a la propuesta de resolución que el trámite de traslado era prescindible en este caso, dado que las reclamaciones se presentaron ante la AVPD, que se declaró incompetente. Sin embargo, ninguna consecuencia jurídica tiene este hecho ni las actuaciones desarrolladas por la AVPD previas a la remisión de las reclamaciones a la AEPD, respecto de la formalización o no del trámite citado, o la oportunidad que supone para el responsable de dar respuesta a las reclamaciones y la posibilidad que ello conlleva para evitar que las mismas sigan el curso previsto en el Título VIII de la LOPDGDD.

Acordada esta admisión a trámite, que fue notificada a los reclamantes, y no a IZENPE, conforme a lo establecido en el artículo 65.5 de la LOPDGDD, se iniciaron actuaciones previas de investigación señaladas con el número E/00995/2019. En el marco de estas actuaciones, con fecha 04/02/2019, los servicios de inspección de esta Agencia cursaron a IZENPE una solicitud de información, en la que consta dicho número de referencia y se indica expresamente que dicho requerimiento se realiza *"En el marco de las actuaciones practicadas por la Subdirección General de Inspección de Datos con objeto de aclarar los términos de unos hechos susceptibles de posible infracción a la normativa vigente de Protección de Datos y de los cuales ha tenido conocimiento esta Agencia Española de Protección de Datos"* y en uso de las facultades conferidas por el artículo 58.1 del RGPD y el artículo 67 *"Actuaciones previas de investigación"* de la LOPDGDD.

Siendo así, resulta que las actuaciones previas de investigación desarrolladas eran conocidas por IZENPE.

Por otra parte, cabe señalar que en el momento en que tuvo lugar la notificación de la apertura del presente procedimiento, en fecha 19/12/2019, no había transcurrido el plazo de duración previsto en el artículo 67.2 de la LOPDGDD, contado desde la fecha del acuerdo de admisión a trámite.

IZENPE no comparte la conclusión anterior. En sus alegaciones a la propuesta de resolución manifiesta que el plazo de doce meses sólo puede emplearse cuando la complejidad de la investigación aconseje extenderla hasta sus límites máximos; y añade que el acuerdo de apertura se basa en las actuaciones desarrolladas por la AVPD, sin que la AEPD llevase a cabo ninguna actuación material de investigación efectiva, habiéndose limitado a solicitar información o documentación adicional (cita la STS de 13/05/2019 -RC 2415/2016-, que sigue otro pronunciamiento precedente -STS de 06/05/2015, RC 3438/2012-, señalando que recoge una nueva doctrina en virtud de la cual el período de actuaciones previas debe proyectarse sobre la realización efectiva de actividades de investigación sin proceder artificialmente a su prolongación.

Entiende que la remisión de las reclamaciones a la AEPD por otra autoridad de control supone que el cómputo del plazo de doce meses se inicie con ese traslado de las actuaciones y concluye que la AEPD dilató artificialmente el período de investigación hasta casi veinte meses, perjudicando a IZENPE, que ha ido acumulando a los hechos probados intervenciones posteriores en materia de protección de datos y ampliando el foco cuantitativo de posibles infracciones (por ejemplo, en número de usuarios registrados).

Sin embargo, la norma establece claramente las distintas actuaciones que pueden

seguirse una vez recibida una reclamación y los procedimientos a que puede dar lugar, estableciendo positivamente el período de duración y el cómputo de ese período para cada actuación. En lo que ahora interesa, la decisión sobre la admisión o inadmisión a trámite debe notificarse a la reclamante en el plazo de tres meses desde que la reclamación tuvo entrada en la Agencia; una vez admitida a trámite la reclamación, podrán llevarse a cabo actuaciones previas de investigación, con una duración no superior a doce meses, contados desde la fecha del acuerdo de admisión a trámite. El cómputo del tiempo empleado para evaluar la admisibilidad de la reclamación queda excluido del cómputo del plazo disponible para el desarrollo de las actuaciones de investigación.

No distingue la norma ninguna regla especial para reclamaciones presentadas ante las autoridades autonómicas de protección de datos que sean finalmente remitidas a esta Agencia para su examen; ni tampoco la duración de las actuaciones previas se somete a condición alguna en cuanto a su desarrollo, ya sea formal o material.

Por otra parte, es necesario precisar que las Sentencias del TS que cita IZENPE no se refieren específicamente a esta última cuestión, ni concluye lo expresado por IZENPE sobre la exigencia de vincular el período de actuaciones previas de investigación a la realización efectiva de actividades de investigación. Esta Sentencia analiza una posible infracción de los artículos 20.6 del Real Decreto 1398/93, de 4 de agosto, por el que se aprueba el Reglamento del Procedimiento para el Ejercicio de la Potestad Sancionadora y 42.3.a de la Ley 30/1992, en cuanto al cómputo del plazo para apreciar la caducidad del expediente sancionador. El recurrente alegó que el cómputo de ese plazo debe iniciarse en la fecha de formulación de la denuncia previa y el Tribunal declaró que el plazo de que dispone la Administración para resolver se inicia con el acuerdo de iniciación del expediente, quedando por ello excluido de dicho cómputo el periodo de tiempo transcurrido desde la fecha de la noticia del hecho infractor y, en su caso, el empleado en las actuaciones previas. Añade la Sentencia citada lo siguiente:

“El recurrente sostiene que con esa interpretación se está concediendo a la Administración un plazo ilimitado para iniciar el procedimiento. Sin embargo, esta Sala tiene declarado que ese periodo anterior al acuerdo de iniciación <<... ha de ser forzosamente breve y no encubrir una forma artificiosa de realizar actos de instrucción y enmascarar y reducir la duración del propio expediente posterior >> (sentencia de 6 de mayo de 2015, recurso de casación 3438/2012, F.J. 2º, donde se cita, a su vez, un pronunciamiento anterior en esa misma línea de razonamiento)”.

Se cuestiona, por tanto, el encubrimiento de actos de instrucción con anterioridad al inicio del procedimiento con el fin de sustraerlos del cómputo del plazo de caducidad, pero esta Sentencia no contiene ningún pronunciamiento sobre lo alegado por IZENPE en relación con las actuaciones previas de investigación.

Ningún perjuicio se traduce para IZENPE del seguimiento de los trámites previstos en la normativa reseñada.

III

La LPACAP dedica el Capítulo II del Título I a la *“Identificación y firma de los interesados en el procedimiento administrativo”*, artículos 9 a 12.

El artículo 9 de la citada Ley establece que *"las Administraciones Públicas están obligadas a verificar la identidad de los interesados en el procedimiento administrativo, mediante la comprobación de su nombre y apellidos o denominación o razón social, según corresponda, que consten en el Documento Nacional de Identidad o documento identificativo equivalente"*. Este precepto, en su apartado 2, se refiere a los sistemas que podrán utilizar los interesados para identificarse ante las Administraciones Públicas:

"2. Los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de los sistemas siguientes:
a) Sistemas basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la "Lista de confianza de prestadores de servicios de certificación".
b) Sistemas basados en certificados electrónicos cualificados de sello electrónico expedidos por prestadores incluidos en la "Lista de confianza de prestadores de servicios de certificación".
c) Sistemas de clave concertada y cualquier otro sistema, que las Administraciones consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad, previa autorización por parte de la Secretaría General de Administración Digital del Ministerio de Política Territorial y Función Pública, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior. La autorización habrá de ser emitida en el plazo máximo de tres meses. Sin perjuicio de la obligación de la Administración General del Estado de resolver en plazo, la falta de resolución de la solicitud de autorización se entenderá que tiene efectos desestimatorios.

Las Administraciones Públicas deberán garantizar que la utilización de uno de los sistemas previstos en las letras a) y b) sea posible para todo procedimiento, aun cuando se admita para ese mismo procedimiento alguno de los previstos en la letra c)".

Por otra parte, el Reglamento (UE) 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, en su Capítulo I, dedicado a las *"Disposiciones Generales"*, establece lo siguiente:

"Artículo 2. Ámbito de aplicación
1. El presente Reglamento se aplica a los sistemas de identificación electrónica notificados por los Estados miembros y a los prestadores de servicios de confianza establecidos en la Unión.
2. El presente Reglamento no se aplica a la prestación de servicios de confianza utilizados exclusivamente dentro de sistemas cerrados resultantes del Derecho nacional o de acuerdos entre un conjunto definido de participantes.
3. El presente Reglamento no afecta al Derecho nacional o de la Unión relacionado con la celebración y validez de los contratos u otras obligaciones legales o de procedimiento relativos a la forma".

"Artículo 5. Tratamiento y protección de los datos
1. El tratamiento de los datos personales será conforme a lo dispuesto en la Directiva 95/46/CE".

A este respecto, el Considerando 11 del citado Reglamento expone lo siguiente:

"El presente Reglamento debe aplicarse de forma que se cumplan plenamente los principios relativos a la protección de los datos personales establecidos en la Directiva 95/46/CE del Parlamento Europeo y del Consejo. A tal efecto, visto el principio de reconocimiento mutuo que establece el presente Reglamento, la autenticación a efectos de un servicio en línea debe implicar exclusivamente el tratamiento de los datos identificativos que sean adecuados, pertinentes y no excesivos para la concesión del acceso al servicio en línea de que se trate. Por otra parte, los prestadores de servicios de confianza y el organismo de supervisión deben respetar asimismo los requisitos de confidencialidad y seguridad del tratamiento previstos en la Directiva 95/46/CE".

Y el artículo 24 de este Reglamento, incluido en el Capítulo III, referido a los Servicios de Confianza, establece lo siguiente:

"Artículo 24 Requisitos de los prestadores cualificados de servicios de confianza

1. Al expedir un certificado cualificado para un servicio de confianza, un prestador cualificado de servicios de confianza verificará, por los medios apropiados y de acuerdo con el Derecho nacional, la identidad y, si procede, cualquier atributo específico de la persona física o jurídica a la que se expide un certificado cualificado.

La información a que se refiere el párrafo primero será verificada por el prestador de servicios de confianza bien directamente o bien por medio de un tercero de conformidad con el Derecho nacional:

a) en presencia de la persona física o de un representante autorizado de la persona jurídica, o

b) a distancia, utilizando medios de identificación electrónica, para los cuales se haya garantizado la presencia de la persona física o de un representante autorizado de la persona jurídica previamente a la expedición del certificado cualificado, y que cumplan los requisitos establecidos con el artículo 8 con respecto a los niveles de seguridad «sustancial» o «alto», o

c) por medio de un certificado de una firma electrónica cualificada o de un sello electrónico cualificado expedido de conformidad con la letra a) o b), o

d) utilizando otros métodos de identificación reconocidos a escala nacional que aporten una seguridad equivalente en términos de fiabilidad a la presencia física. La seguridad equivalente será confirmada por un organismo de evaluación de la conformidad.

2. Los prestadores cualificados de servicios de confianza que prestan servicios de confianza cualificados:

(…)

f) utilizarán sistemas fiables para almacenar los datos que se les faciliten de forma verificable, de modo que:

i) estén a disposición del público para su recuperación solo cuando se haya obtenido el

consentimiento de la persona a la que corresponden los datos,
ii) solo personas autorizadas puedan hacer anotaciones y modificaciones en los datos almacenados,
iii) pueda comprobarse la autenticidad de los datos;

g) tomarán medidas adecuadas contra la falsificación y el robo de datos;

h) registrarán y mantendrán accesible durante un período de tiempo apropiado, incluso cuando hayan cesado las actividades del prestador cualificado de servicios de confianza, toda la información pertinente referente a los datos expedidos y recibidos por el prestador cualificado de servicios de confianza, en particular al objeto de que sirvan de prueba en los procedimientos legales y para garantizar la continuidad del servicio. Esta actividad de registro podrá realizarse por medios electrónicos;

(…)

j) garantizarán un tratamiento lícito de los datos personales de conformidad con la Directiva 95/46/CE;

k) en caso de los prestadores cualificados de servicios de confianza que expidan certificados cualificados, establecerán y mantendrán actualizada una base de datos de certificados".

De acuerdo con el citado Reglamento (UE) 910/2014, los prestadores de servicio de confianza están sometidos a la supervisión de un órgano designado por el Estado miembro, y este organismo de supervisión está obligado a *"cooperar con las autoridades de protección de datos, por ejemplo informándoles de los resultados de las auditorías de los prestadores cualificados de servicios de confianza, en caso de resultar infringidas las normas sobre protección de datos de carácter personal. El suministro de información debe incluir, en particular, los incidentes en materia de seguridad y las violaciones de los datos de carácter personal"*.

Corresponde a los prestadores de servicios de confianza la rendición de cuentas en relación con sus operaciones y servicios.

Se establece, asimismo, el reconocimiento mutuo de los medios de identificación electrónica entre Estados miembros a efectos de la autenticación transfronteriza. En este sentido, los sistemas que se notifiquen a la Comisión serán interoperables.

De acuerdo con lo expuesto, el prestador de servicios de confianza viene obligado a registrar y almacenar los datos, así como al mantenimiento de la base de datos, correspondiéndole garantizar el tratamiento lícito de los datos personales.

IV

En el presente caso, IZENPE realiza tratamientos de datos personales identificativos y de contactos de usuarios del servicio vasco LANBIDE, a los que añade la toma de una fotografía, que también tiene la consideración de dato personal, al igual que las huellas dactilares que se incorporan como factor de identificación.

La recogida de estos datos se lleva a cabo con la finalidad de establecer un sistema de medios de identificación electrónicos en el marco de las normas reseñadas en el fundamento de anterior, y tiene lugar en un período anterior y posterior al 25/05/2018, fecha a partir de la que resulta aplicable el RGPD.

A los tratamientos de datos anteriores a esa fecha les resulta de aplicación los principios y normas establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), y entre ellos, los principios de pertinencia y proporcionalidad, establecido en el artículo 4.1 de dicha Ley Orgánica.

“Artículo 4. Calidad de los datos

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido”.

Este artículo 4 de la LOPD, con la denominación *“Calidad de datos”*, es el primer precepto del título II dedicado a los *“Principios de calidad de datos”,* que derivan del derecho fundamental a la protección de datos. El apartado 1 del artículo 4 de la LOPD comienza estableciendo que los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, de acuerdo con una serie de criterios, que se resumen en el principio de proporcionalidad, cuyo cumplimiento se exige al responsable del tratamiento.

Dicho artículo relaciona el principio de proporcionalidad en el tratamiento de los datos de carácter personal y la limitación de los fines, que impide el tratamiento de aquellos que no sean necesarios o proporcionales a la finalidad que justifica el tratamiento, resultando contrario a la LOPD el tratamiento de los datos excesivos. En consecuencia, el tratamiento del dato ha de ser pertinente y no excesivo en relación con el fin perseguido. Únicamente pueden ser sometidos a tratamiento aquellos datos que sean estrictamente necesarios para la finalidad perseguida. Por otra parte, el cumplimiento del principio de proporcionalidad no sólo debe producirse en el ámbito de la recogida de los datos, sino que ha de respetarse, asimismo, en el posterior tratamiento que se realice de los mismos.

Este criterio, se encuentra recogido también en el artículo 6 de la Directiva 95/46/CE y aparece reflejado en el Convenio 108, del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, cuyo artículo 5.c) indica que *"los datos de carácter personal que sean objeto de un tratamiento automatizado... serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado”.*

Son los mismos principios recogidos en el Considerando 28 de la citada Directiva: *“(28) Considerando que todo tratamiento de datos personales debe efectuarse de forma lícita y leal con respecto al interesado; que debe referirse, en particular, a datos adecuados, pertinentes y no excesivos en relación con los objetivos perseguidos; que estos objetivos han de ser explícitos y legítimos, y deben estar determinados en el momento de obtener los datos; que los objetivos de los tratamientos posteriores a la obtención no pueden ser incompatibles con los objetivos originalmente especificados”*.

En definitiva, el momento en el que han de determinarse las finalidades es el de la recogida de los datos, cualquier tipo de recogida, careciendo de validez la recogida de datos con finalidades que no hayan sido fijadas o determinadas de modo preciso, o tan vagas o genéricas que admitiera cualquier propósito. Se trata de que el particular pueda identificar las finalidades de forma clara y precisa, sin que le genere ninguna duda o dificultad para su compresión.

Además, la determinación de las finalidades es necesaria para valorar si el tratamiento del dato personal es *"pertinente"* al fin perseguido e implica que no deberán recabarse datos personales que no sean necesarios para el propósito al que serán destinados.

Por otra parte, el deber de información y principio del consentimiento están regulados en los artículos 4.1, 5 y 6 de la LOPD:

"Artículo 5. Derecho de información en la recogida de datos.

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

(…)

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior...".

"Artículo 6. Consentimiento del afectado

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.
2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.
3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.
4. En los casos en los que no sea necesario el consentimiento del afectado para el

tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado".

Asimismo, el Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre, establece en su artículo 10 los supuestos que legitiman el tratamiento de los datos. El apartado 1 de este artículo dispone que *"Los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello"*.

La vulneración de estos preceptos es constitutiva de infracción leve en el artículo 44.2.c) (deber de informar) de la LOPD, o grave en los artículos 44.3.b) (principio del consentimiento) y c) (principio de proporcionalidad) de la misma norma, pudiendo ser sancionadas con multa de 900 a 40.000 euros en el caso de infracciones leves, y de 40.001 a 300.000 euros para las graves.

El artículo 45.6 de la LOPD admite, excepcionalmente, la posibilidad de no acordar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que los hechos fuesen constitutivos de infracción leve o grave y que el infractor no hubiese sido sancionado o apercibido con anterioridad.

Interesa destacar, asimismo, lo dispuesto en el artículo 49 de la citada Ley Orgánica, que otorga al órgano sancionador la potestad de requerir a los responsables, en supuestos constitutivos de infracción grave o muy grave, la cesación en la utilización ilícita de los datos de carácter personal.

V

En términos similares a la Directiva 95/46/CE y la LOPD, el artículo 5 del RGPD se refiere a los principios relativos al tratamiento de datos, estableciendo que los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (*"minimización de datos"*); y tratados de manera lícita, leal y transparente en relación con el interesado (*"licitud, lealtad y transparencia"*).

El artículo 13 del citado texto legal detalla la *"información que deberá facilitarse cuando los datos personales se obtengan del interesado"*, en el momento mismo en que tiene lugar esa recogida de datos, de la que se destaca la siguiente:

. La identidad y los datos de contacto del responsable y, en su caso, de su representante;
. Los datos de contacto del delegado de protección de datos, en su caso;
. Los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
. Cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;
. El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
. La existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos

personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
. Cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;
. El derecho a presentar una reclamación ante una autoridad de control;
. Si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;

En relación con el principio de transparencia citado, el artículo 11.1 y 2 de la LOPDGDD admite que se facilite al afectado la información básica que se indica en el mismo (identidad del responsable, finalidad y ejercicio de derechos) y se indique una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

Por otra parte, los artículos 6 y 7 del mismo RGPD se refieren, respectivamente, a la *"Licitud del tratamiento"* y las *"Condiciones para el consentimiento".*

"Artículo 6 Licitud del tratamiento
1.El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:
a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.
Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

2.Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.

3.La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:
a) el Derecho de la Unión, o
b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.
La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al

responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido...".

"Artículo 7 Condiciones para el consentimiento
1.Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.
2.Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.
3.El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.
4.Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato".

Los supuestos en los que el tratamiento se refiera a categorías especiales de datos personales están regulados en el artículo 9 del RGPD en los términos siguientes:

"1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexuales de una persona física.

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;
(…)".

El incumplimiento de los preceptos citados es constitutivo de infracción tipificada en el artículo 83.5 del RGPD, que bajo la rúbrica "*Condiciones generales para la imposición de multas administrativas"* dispone lo siguiente:

"Las infracciones de las disposiciones siguientes se sancionarán, 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;
b) los derechos de los interesados a tenor de los artículos 12 a 22 (…)".

A este respecto, la LOPDGDD, en su artículo 71 establece 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 efectos del plazo de prescripción, el artículo 72 de la LOPDGDD indica:

"Artículo 72. Infracciones consideradas muy graves.
1. 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.
(…)
e) El tratamiento de datos personales de las categorías a las que se refiere el artículo 9 del Reglamento (UE) 2016/679, sin que concurra alguna de las circunstancias previstas en dicho precepto y en el artículo 9 de esta ley orgánica".

Para el caso de que concurra una infracción de los preceptos del RGPD, entre los poderes correctivos de los que dispone la Agencia Española de Protección de Datos, como autoridad de control, el artículo 58.2 de dicho Reglamento contempla los siguientes:

"2 Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:
(…)
b) sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;"
(...)
d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;
(…)
i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;".

En relación con la posibilidad de sancionar con apercibimiento que contempla el citado artículo 58.2 b), se considera lo expresado en el Considerando 148 del RGPD:

"En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. Debe no obstante prestarse especial atención a la naturaleza,

gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de conducta y a cualquier otra circunstancia agravante o atenuante."

VI

La entidad IZENPE, constituida como medio propio personificado por la Administración General de la Comunidad Autónoma de Euskadi y las Diputaciones Forales, recibió el encargo de las mismas para la emisión de medios de identificación electrónica que permitan a los ciudadanos y empresas privadas relacionarse telemáticamente con la administración vasca. Para la ejecución de este encargo, IZENPE dispuso dos sistemas (B&K y B&K Q) que permiten la identificación y firma electrónica, formados por un número de referencia, contraseña, juego de coordenadas y certificado de firma electrónica.

Para el desarrollo del proyecto citado, según ha declarado la propia IZENPE, con fecha 26/10/2017 suscribió un convenio de colaboración con LANBIDE, en virtud del cual esta última actúa como entidad de registro de IZENPE para la expedición de medios de identificación digital y firma electrónica, para facilitar un sistema interoperable a personas físicas usuarias de dicho servicio de empleo. IZENPE ha declarado que el Departamento de Empleo y Políticas Sociales decidió implantar el sistema en LANBIDE de forma experimental para todos los trabajadores y usuarios del servicio (colectivo cercano a 300.000 personas), a fin de mejorar, simplificar y hacer más eficiente la gestión administrativa, dando respuesta así a las necesidades actuales de la sociedad.

Dicho acuerdo de colaboración fue prorrogado y modificado para adecuarlo al nuevo marco regulador en materia de protección de datos establecido tras la entrada en vigor, el 25 de mayo de 2018, del RGPD, mediante la adenda suscrita el 15 de octubre de 2018, en la que se modifica la cláusula séptima relativa a protección de datos. En su nueva redacción se especifica que LANBIDE no podrá utilizar los datos para fines propios, que los tratará de acuerdo con lo determinado por IZENPE

Para la ejecución del acuerdo, LANBIDE pone a disposición de IZENPE sus espacios físicos y el personal encargado de las tareas de identificación y registro de usuarios, contemplándose tres fases: un solo puesto de recogida de datos inicialmente, una ampliación posterior a 10 puestos y una tercera fase (a ejecutar en el segundo trimestre del 2019), en la que se prevé extender el número de puestos de registro a la totalidad de las oficinas de LANBIDE (43 oficinas). En esta fase se pretendía que este medio de identificación pudiera ser utilizado, por las personas que voluntariamente lo eligiesen, para el acceso a los servicios de esta entidad, si bien IZENPE ha indicado que, hasta tanto no se regule por Ley el uso del sistema (actualmente en tramitación), únicamente será probado de forma experimental.

Según consta en la parte expositiva, el acuerdo se enmarca en la Ley 39/2015, para profundizar en la implantación de la Administración electrónica, y el Reglamento (UE) 910/2014. En virtud de este acuerdo, IZENPE actúa en su condición de prestador de servicios de confianza y Lanbide adquiere la condición de entidad de registro de IZENPE para la expedición de medios de identificación digital y firma electrónica B&K y B&K Q. en relación con las personas físicas usuarias que soliciten medios de identificación expedidos por

IZENPE. Como tal, IZENPE es responsable de la base de datos que permitirá la interoperabilidad del sistema, de su almacenamiento y gestión.

Se pretendía la implantación de un sistema interoperable que permitiera al ciudadano relacionarse con las Administraciones Públicas. Se trata, según lo define la propia IZENPE en sus alegaciones, de un caso en el que la actuación de la entidad prestadora de servicios de confianza es de carácter general y no una actuación singular que busca la emisión de un sistema de identificación vinculado al ejercicio de competencias de LANBIDE.

Desde el punto de vista de la protección de datos personales, IZENPE se declara responsable del tratamiento (también del fichero) y LANBIDE intervine como encargado para la mera recogida y validación de los datos y su posterior envío a IZENPE. Así consta en los documentos formalizados y en la información facilitada a los interesados.

Modificar esta posición a posteriori afectaría de modo significativo a los derechos de los interesados. IZENPE ha alegado que la *"reformulación"* de los roles de responsable y encargado del tratamiento no afecta a los derechos de los reclamantes. Sin embargo, nos referimos aquí a los perjuicios que ello representa para los titulares de los datos personales en general, que recibieron una información clara y específica sobre la identidad del responsable (IZENPE) y la forma en la que podrán ejercer sus derechos ante dicho responsable.

Con este propósito de alterar la condición bajo la que intervienen estas entidades no puede hacerse valer la Resolución del Director General de LANBIDE de fecha 30 de noviembre de 2018, por la que se acuerda *"Encargar a la empresa Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A., como medio propio personificado de la Administración General de la Comunidad Autónoma de Euskadi, la provisión de servicios para la implantación en Lanbide de un sistema que permita la identificación de personas basados en factores biométricos"*, señalando que en la misma se dispone que corresponde a LANBIDE la definición de los fines del tratamiento y a la que se atribuye una vigencia retroactiva con efectos de 01/01/2018.

Cabe señalar, por un lado, que esta Resolución no forma parte del objeto del procedimiento, iniciado para analizar el alcance de la recogida de datos llevada a cabo por LANBIDE en virtud de los acuerdos antes citados; y, por otro lado, que también esta Resolución declara a IZENPE como responsable del tratamiento, identificado en su registro de tratamiento como *"gestión de medios de identificación basados en parámetros biométricos"*.

Asimismo, considerando las repetidas manifestaciones realizadas por IZENPE sobre la condición de responsable del tratamiento que se atribuye a la entidad que determina las finalidades del tratamiento de los datos, conviene tener presente la definición de "responsable del tratamiento" expresada en el artículo 4 del RGPD, que considera como tal no solo al que define los fines, sino también al que habilita los medios para el tratamiento, circunstancia esta que no se menciona por aquella entidad. En este caso, es IZENPE y no LANBIDE quien dispone los fines y los medios para el tratamiento, en virtud de su condición de prestador de servicios de confianza, a la que se hizo referencia anteriormente.

Tampoco puede negarse la actuación de IZENPE como responsable del tratamiento de los datos acudiendo a su naturaleza de medio propio personificado, instrumental, en relación

con las entidades o Administraciones Públicas para las que actúa, desde el punto de vista de la normativa de contratos del sector público (artículo 32 de la LCSP).

Precisamente esa condición de responsable del tratamiento de IZENPE, y su naturaleza de entidad mercantil, determinó la resolución dictada por la Agencia Vasca de Protección de Datos por la que inadmitió las reclamaciones de referencia y ordenó su remisión a esta Agencia Española de Protección de Datos.

En sus alegaciones a la propuesta de resolución, IZENPE prescinde de todos los argumentos anteriores para defender que no puede ser considerada responsable del tratamiento en ningún caso, especialmente a partir de la plena aplicación del RGPD. Basa este planteamiento en su condición de entidad mercantil con carácter de medio propio personificado, que la sitúa en una posición de dependencia funcional de las Administraciones Públicas que le realizan *"encargos"*, de lo que deriva la imposibilidad material de definir los fines del tratamiento, al no ser titular de la competencia sustantiva a la que sirve el tratamiento.

Considera que los documentos formalizados no determinan su condición de responsable, por cuanto se dispuso erróneamente el reparto de roles de responsable y encargado del tratamiento, llegando a reprochar a esta Agencia no haber realizado ningún esfuerzo interpretativo de tales documentos para advertir (*"una suerte de levantamiento del velo"*, dice IZENPE) que esa mercantil no podía responsabilizarse del tratamiento de acuerdo con el RGPD. Más que un *"esfuerzo interpretativo"*, lo que IZENPE está exigiendo a esta Agencia es una modificación de los términos convenidos y la obtención de conclusiones contrarias a la relación dispuesta por la propia entidad IZENPE.

Y no solo pretende que esta Agencia renuncie a extraer conclusiones de las relaciones formalizadas por IZENPE en este caso, sino también del resto de circunstancias concurrentes, con el propósito de que la resolución que se dicte se base únicamente en un análisis conceptual de su condición de medio propio personificado, como entidad instrumental que actúa por encargo de las Administraciones Públicas de las que depende.

El planteamiento realizado por IZENPE no tiene en cuenta lo establecido en el citado artículo 32 de la LCSP, según el cual IZENPE también puede actuar como poder adjudicador, tal y como ocurre en este caso (*"3. El apartado 2 del presente artículo también se aplicará en los casos en que la persona jurídica controlada, siendo un poder adjudicador, realice un encargo al poder adjudicador que la controla o a otra persona jurídica controlada, directa o indirectamente, por el mismo poder adjudicador, siempre que no exista participación directa de capital privado en la persona jurídica a la que se realice el encargo"*).

IZENPE, en las mencionadas alegaciones, omite algo esencial para la valoración del presente caso, como es su condición de prestador de servicios de confianza según el Reglamento (UE) 910/2014 (eIDAS), que está en el mismo origen de su creación (IZENPE se constituye por la Administración de la Comunidad Autónoma de Euskadi y las Diputaciones Forales para el desarrollo de la identificación electrónica, y constituye su objeto la emisión y gestión de medios y sistemas de identificación electrónicos para la identificación, autenticación, firma y/o sellado electrónico, a personas o entidades públicas o privadas).

Como tal, desde 2016 viene desarrollando el proyecto de emisión de medios de identificación con certificado centralizado (en la nube) para personas físicas denominados

B@k y B@KQ, con el que se busca dotar a la ciudadanía de un medio de identificación en las relaciones telemáticas con las Administraciones vascas. Ambos certificados se emiten en un repositorio común. Cuando el titular utilice el medio de que se trate para su identificación ante un servicio electrónico, IZENPE, en el caso de que la autenticación sea correcta, ofrecerá al organismo responsable del servicio el resultado de la misma.

Se trata de un sistema integrado de claves eIDAS, interoperable, y comprende la creación, verificación y validación de claves de identificación, así como su preservación. Según se explica en el documento denominado *"Política del certificado de ciudadano"*, publicado en www.izenpe.eus y notificado al Ministerio de Industria, Turismo y Comercio, IZENPE es responsable de verificar la identidad del solicitante, el procedimiento de solicitud, emisión y entrega del medio de identificación electrónica, así como de su revocación y renovación.

IZENPE es responsable de la recogida de datos, de su almacenamiento y del tratamiento de datos que requiere el proceso de identificación.

El acuerdo de colaboración suscrito por IZENPE y LANBIDE se formaliza para la puesta en marcha en esta última de esos medios de identificación electrónica, en el marco de la Ley 39/2015 y el Reglamento (UE) 910/2014.

VII

El proyecto puesto en marcha por IZENPE contempla la recogida de datos identificativos y de contacto de los interesados (apellidos, nombre, número de DNI/Pasaporte, fecha de nacimiento, correo electrónico y teléfono móvil). Además, para dar respuesta a nuevas necesidades asociadas a los sistemas de identificación, los medios se completan con otros factores de autenticación biométricos como la huella dactilar y/o fotografía. Según pudo comprobar la Agencia Vasca de Protección de Datos en inspección realizada con fecha 06/07/2018, el proceso seguido por LANBIDE incluía la recogida de las huellas de los diez dedos de las manos y la imagen facial.

Así, LANBIDE lleva a cabo las siguientes actuaciones, conforme al sistema de registro habilitado para la recogida de información:

. Verificación de la identidad del interesado mediante un sistema de validación del documento de identificación presentado.
. Recabar la firma de la solicitud de emisión de B@k y B@kQ: se generará un documento personalizado diferente en función de si la persona tiene DNI/NIE y si dispone ya de B@KQ o B@K (serán 3 posibles) y se imprime el documento a firmar por el ciudadano autorizando la recogida de sus datos biométricos (fotografía facial y minucias dactilares) por parte de IZENPE para su relación con las administraciones públicas.
. Recogida de fotografía facial identificativa.
. Escaneo de huellas digitales (el número de las mismas será parametrizable).
. Registrar/grabar los datos biométricos obtenidos (fotografía y huella dactilar) en el sistema de gestión de identidades de IZENPE.

Se dispuso un formulario de solicitud de medios de identificación con factores biométricos, que fue posteriormente revisado para adecuar la información que facilita, adecuándola al RGPD. En ambos formularios se informa a los interesados que se trata de

medios de identificación electrónica que le permitirá relacionarse con las administraciones vascas y se detalla que dichos medios de identificación están formados por un número de referencia (coincidente con el DNI/NIE/pasaporte del usuario y una contraseña), un certificado no cualificado emitido en un repositorio centralizado que servirá para los actos de firma (B@K) o un juego de coordenadas con 16 posiciones y un certificado cualificado de firma electrónica emitido en un repositorio centralizado de IZENPE que servirá para los usos de firma (B@K Q). En ambos casos, además, el medio de identificación puede ser complementado por otros factores de autenticación biométricos como la huella dactilar y/o fotografía (única referencia a los datos biométricos que aparece en estos documentos de solicitud).

Con la firma de las solicitudes correspondientes, el firmante declara que ha leído y acepta los Términos y Condiciones de uso de este medio de identificación publicadas en www.izenpe.eus/condicionesuso, y consiente a IZENPE el tratamiento de los datos de carácter personal referentes al medio de identificación solicitado.

En el dorso de estas solicitudes se ofrece *"Información básica sobre protección de datos"*, con los detalles correspondientes a la identidad del responsable, finalidad, legitimación (consentimiento del interesado), destinatarios y derechos, advirtiendo, además, sobre la posibilidad de obtener más información disponible en la web *"www.izenpe.eus/datos"* Se accede a esta información y se comprueba que, en el apartado relativo a los derechos del interesado, se informa sobre la posibilidad de "retirar el consentimiento").

Según la información facilitada por IZENPE, el número de usuarios de los que se han tomado datos biométricos antes de la modificación de los formularios de solicitud es 10.378 registros, de los cuales 3.624 son anteriores a la fecha de entrada en vigor del RGPD. Tras la modificación de los formularios de solicitud se han realizado 320 registros hasta el día 15/02/2019. El total de registros a dicha fecha asciende, por tanto, a 10.738 usuarios.

De acuerdo con lo expuesto, se entiende que IZENPE es la entidad responsable de la recogida de datos y el tratamiento posterior que pudiera conllevar el uso de los medios de identificación a los que se refieren las actuaciones. A este respecto, dicha entidad ha declarado que es LANBIDE la que define la finalidad del uso de estos medios y que el último estudio realizado recomienda la reformulación de los roles como responsable y encargado del tratamiento de datos, teniendo en cuenta la condición de IZENPE como medio propio de sus administraciones matrices. Sin embargo, no aclara cómo se formalizará esta nueva reformulación, ni si la misma resulta contraria a la información que se facilita a los interesados sobre la condición de responsable de IZENPE.

Por otra parte, consta que la base legitimadora del tratamiento de datos personales es el consentimiento del interesado, prestado mediante la firma expresa que se recaba mediante los formularios de solicitud de los medios de identificación, en los que, además, se incluye la información básica en materia de protección de datos personales. Se trata de un consentimiento válido, obtenido una vez cumplidas las exigencias de transparencia establecidas en la normativa aplicable.

No obstante, entiende esta Agencia, en relación con los datos biométricos recabados, que la recogida de la huella dactilar de los diez dedos de las manos incumple el principio de *"pertinencia y proporcionalidad"* o *"minimización de datos"*, regulado en los artículos 4 de la LOPD y 5 del RGPD, por cuanto los medidos de identificación que pretenden implantarse no requieren, para ser efectivos, la recogida de las huellas dactilares de todos los dedos de

ambas manos, lo que tampoco se justifica en razón a la finalidad pretendida.

Por tanto, el tratamiento de datos personales consistente en la recogida de las huellas de los diez dedos de las manos no es proporcional a la finalidad que justifica el tratamiento, resultando contrario a la LOPD y al RGPD. Se trata de una recogida de datos excesivos, por cuanto no son estrictamente necesarios para la finalidad perseguida. Conforme al principio de minimización, deberá evitarse el tratamiento de datos innecesarios y desproporcionados en relación con las finalidades pretendidas (limitación de la finalidad). Y es el responsable del tratamiento, IZENPE en este caso, el obligado a cumplir estos principios relativos al tratamiento.

Es cierto que en la información aportada se hace referencia a la recogida de *"minucias dactilares"* y a que el número de las huellas escaneadas será parametrizable. Pero no se aportan detalles suficientes al respecto, ni se indica el alcance que esto representa en relación con la recogida de las huellas de todos los dedos de las manos que venía realizándose, según pudo verificar la Agencia Vasca de Protección de Datos.

Dicho incumplimiento de los artículos 4.1 de la LOPD y 5 del RGPD se encuentran tipificados como infracción grave en el artículo 44.3 c) de la LOPD (*"Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en el artículo 4 de la presente Ley y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave"*); y en el artículo 83.5 a) del RGPD (*"Las infracciones de las disposiciones siguientes… a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9"*), respectivamente.

En cuanto a las medidas que corresponde imponer por este incumplimiento, de acuerdo con lo establecido en los artículos 45.6 de la LOPD y 58.2 b) del RGPD, se considera procedente sancionar la citada infracción con apercibimiento.

Se tiene en cuenta, por un lado, que IZENPE no ha sido sancionada con anterioridad y, por otro, que parte de la recogida de datos personales llevada a cabo tiene carácter experimental, que se ha declarada que LANBIDE no utiliza los datos biométricos para la identificación de los usuarios al no estar operativo el sistema y, principalmente, que IZENPE está llevando a cabo una reformulación del proyecto y ha resuelto suspender provisionalmente el tratamiento del registro de datos biométricos para la emisión de medios de identificación a la ciudadanía mientras no exista cobertura legal, en referencia a una norma actualmente en tramitación, que presumiblemente dará cobertura legal para llevar a cabo la identificación de la ciudadanía por medio de sistemas biométricos, en los términos establecidos por el artículo 8.2 de la LOPDGDD. A este respecto, ha manifestado a esta Agencia que desde el 26 de octubre de 2019 este tratamiento de datos no se está realizando.

IZENPE, no obstante, deberá aclarar el alcance de la información que se ofrecía a los interesados sobre la activación del sistema de identificación. Así, en los formularios de recogida de datos, a continuación del espacio habilitado para la firma del solicitante, se añade un apartado sobre *"Emisión y Activación"* con el texto siguiente: *"Tras la identificación y firma del formulario de solicitud, el solicitante podrá iniciar la emisión de B@k. El proceso comienza con el envío de un SMS con la contraseña (que por seguridad debe cambiar). Por último, Izenpe generará un certificado no cualificado de firma electrónica emitido en un repositorio centralizado seguro"*.

Finalmente, en respuesta a lo planteado por IZENPE en su escrito de alegaciones a la propuesta de resolución, es preciso puntualizar que no procede incluir en el presente acto los pronunciamientos que solicita, con vistas al futuro, sobre el régimen sancionador aplicable a empresas públicas que son medio propio personificado, que dicha entidad vincula a la competencia que pueda atribuirse a la AVPD y la AEPD de conformidad con lo establecido en el artículo 57.1 de la LOPDGDD.

VIII

Conforme a lo dispuesto en el artículo 49 de la LOPD, que otorga al órgano sancionador la potestad de requerir a los responsables, en supuestos constitutivos de infracción grave o muy grave, la cesación en la utilización ilícita de los datos de carácter personal; y el artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá *"ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado…"*; procede requerir a la entidad IZENPE para que, en el plazo de un mes, adecúe a la normativa de protección de datos personales las operaciones de tratamiento que realiza, con el alcance expresado en los Fundamentos de Derecho. En concreto, procede que IZENPE cese en la utilización ilícita de los datos de carácter personal relativos a las huellas dactilares de los diez dedos de las manos, ajustando este tratamiento de datos de forma que se conserve el registro de un número de huellas dactilares compatible con el principio de minimización de datos, siempre que se justifique debidamente ese número.

Se advierte que no atender los requerimientos de este organismo puede ser considerado como una infracción administrativa grave al *"no cooperar con la Autoridad de control"* ante los requerimientos efectuados, pudiendo ser valorada tal conducta a la hora de la apertura de un procedimiento administrativo sancionador con multa pecuniaria.

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

la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a EMPRESA DE CERTIFICACION Y SERVICIOS IZENPE, S.A., con NIF ***A01337260***, una sanción de apercibimiento, por una infracción de los artículos 4.1 de la LOPD y 5 del RGPD, tipificada en los artículos 44.3 c) de la LOPD y 83.5 a) del RGPD, respectivamente.

SEGUNDO: REQUERIR a la entidad EMPRESA DE CERTIFICACION Y SERVICIOS IZENPE, S.A., para que en el plazo un mes, contado desde la notificación del presente acto, adecúe a la normativa de protección de datos personales las operaciones de tratamiento que realiza, con el alcance expresado en el Fundamento de Derecho VIII. En concreto, se requiere que IZENPE cese en la utilización ilícita de los datos de carácter personal relativos a las huellas dactilares de los diez dedos de las manos, ajustando este tratamiento de datos de forma que se conserve el registro de un número de huellas dactilares compatible con el principio de minimización de datos, siempre que se justifique debidamente ese número.

TERCERO: NOTIFICAR la presente resolución a la entidad EMPRESA DE CERTIFICACION

Y SERVICIOS IZENPE, S.A.

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 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 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.

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://sedeagpd.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.

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