OTRAS DISPOSICIONES

DEPARTAMENTO DE GOBERNANZA PÚBLICA Y AUTOGOBIERNO

6006

RESOLUCIÓN 158/2018, de 27 de noviembre, del Director de la Secretaría del Gobierno y de Relaciones con el Parlamento, por la que se dispone la publicación de la Adenda de modificación y prórroga del Acuerdo de colaboración suscrito entre Lanbide-Servicio Vasco de Empleo y Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A. para el despliegue del proyecto piloto de medios de identificación electrónicos basados en la captación de datos biométricos.

Habiéndose suscrito por Lanbide-Servicio Vasco de Empleo el Convenio referenciado, y a los efectos de darle la publicidad debida,

RESUELVO:

Artículo único.– Publicar en el Boletín Oficial del País Vasco el texto de la Adenda de modificación y prórroga del Acuerdo de colaboración suscrito entre Lanbide-Servicio Vasco de Empleo y Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A. para el despliegue del proyecto piloto de medios de identificación electrónicos basados en la captación de datos biométricos, que figura como anexo a la presente.

En Vitoria-Gasteiz, a 27 de noviembre de 2018.

El Director de la Secretaría del Gobierno y de Relaciones con el Parlamento,
JUAN ANTONIO ARIETA-ARAUNABEÑA IBARZABAL.

ANEXO A LA RESOLUCIÓN 158/2018, DE 27 DE NOVIEMBRE, DEL DIRECTOR DE LA SECRETARÍA DEL GOBIERNO Y DE RELACIONES CON EL PARLAMENTO

ADENDA DE MODIFICACIÓN Y PRÓRROGA DEL ACUERDO DE COLABORACIÓN ENTRE LANBIDE-SERVICIO VASCO DE EMPLEO Y ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACIÓN Y SERVICIOS, IZENPE, S.A. PARA LA PUESTA EN MARCHA DE MEDIOS DE IDENTIFICACIÓN ELECTRÓNICOS BASADOS EN LA CAPTACIÓN DE DATOS BIOMÉTRICOS

En Vitoria-Gasteiz, a 15 de octubre de 2018.

REUNIDOS:

De una parte, Dña. Beatriz Artolazabal Albeniz, Consejera de Empleo y Políticas Sociales, en calidad de Presidenta del organismo autónomo Lanbide-Servicio Vasco de Empleo, en nombre y representación del mismo y en el ejercicio de las competencias atribuidas en virtud de lo dispuesto en el artículo 9 c) de la Ley 3/2011, de 13 de octubre, sobre Lanbide-Servicio Vasco de Empleo.

En adelante, Lanbide.

De otra, D.ª. Izaskun Urrestarazu Amondarain, en representación de Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A. en nombre y representación de la misma.

Sus facultades resultan de su condición de Directora, en virtud de escritura de poder otorgada el 21 de marzo de 2016, ante el Notario de Vitoria-Gasteiz, D. Alfredo Pérez Ávila bajo el número 773 de su protocolo, debidamente inscrita en el Registro Mercantil de Álava al Tomo 1541, Folio 79, Hoja VI-8926.

En adelante, Izenpe.

Ambas partes se reconocen la capacidad jurídica necesaria para suscribir el presente Acuerdo y en su virtud,

EXPONEN:

1.– Que con fecha 26 de octubre de 2017 Lanbide-Servicio Vasco de Empleo e Izenpe firmaron un Acuerdo de colaboración para la puesta en marcha de medios de identificación electrónicos basados en la captación de datos biométricos por el que Lanbide adquiría 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.

2.– Que conforme a lo establecido en la cláusula tercera del citado Acuerdo este tiene una duración de un año pudiéndose prorrogar por igual periodo de tiempo, y hasta un máximo de cuatro años adicionales, mediante acuerdo de las partes, que deberá ser formalizado antes de que finalice su plazo de vigencia.

3.– Que la cláusula undécima permite la modificación del acuerdo durante su vigencia, debiéndose incorporar al mismo, a modo de adenda, las modificaciones efectuadas.

La entrada en vigor, el 25 de mayo de 2018, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, Reglamento General de Protección de Datos (en adelante RGPD), requiere adaptar la redacción de la cláusula séptima a la nueva normativa.

4.– Que es voluntad de Lanbide e Izenpe formalizar la presente adenda de modificación y prórroga del acuerdo de 26 de octubre de 2017, por un nuevo periodo de un año, a fin de dar continuidad a la colaboración establecida.

En base a ello, ambas partes

ACUERDAN:

Primero.– Modificar la cláusula séptima relativa a protección de datos, que queda redactada 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, solo 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.

Si Lanbide considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, informará inmediatamente a Izenpe.

c) Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente acuerdo, incluso después de que finalice su objeto.

d) Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

e) Mantener a disposición de Izenpe la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

f) Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

g) Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, ante el encargado del tratamiento, este debe comunicarlo por correo electrónico a la dirección info@izenpe.com

La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.

Corresponde a Izenpe facilitar a través de los formularios de solicitud del certificado el derecho de información en el momento de la recogida de los datos.

h) Notificación de violaciones de la seguridad de los datos.

El Encargado del Tratamiento notificará al Responsable del Tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de 24 horas, y a través de la dirección info@izenpe.com o del número de teléfono 902 542 542, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si se dispone de ella se facilitará, como mínimo, la información siguiente:

– Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

– El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

– Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

– Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

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

Corresponde al Encargado del Tratamiento comunicar las violaciones de la seguridad de los datos a la Autoridad de Protección de Datos.

La comunicación contendrá, como mínimo, la información siguiente:

– Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

– Nombre y datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

– Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

– Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

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

i) Dar apoyo a Izenpe en la realización de las consultas previas a la autoridad de control, cuando proceda.

j) Poner disposición de Izenpe toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.

k) Implantar las medidas de seguridad siguientes:

– Validación inicial de identidad.

– Verificar la identidad del suscriptor, y comprobar que las solicitudes de certificado sean precisas, autorizadas y completas de acuerdo con la evidencia recopilada o la atestación de identidad.

– Conservar toda la información y documentación relativa a los certificados, cuya emisión, renovación, o revocación gestiona.

– Comunicar a Izenpe, con la debida diligencia, las solicitudes de revocación de los certificados de forma rápida y fiable.

– Permitir a Izenpe el acceso a los archivos y la auditoría de sus procedimientos en la realización de sus funciones y en el mantenimiento de la información necesaria para las mismas.

– Informar a Izenpe de las solicitudes de emisión, revocación, y cualquier otro aspecto que afecte a los certificados emitidos por la misma.

– Cumplir en el desempeño de sus funciones de gestión de emisión, renovación, y revocación de los certificados los procedimientos establecidos por Izenpe y la legislación vigente en esta materia.

– Cumplimiento de la normativa y estándares de seguridad (RGPD, ISO, ETSI.

– Procesamiento de las solicitudes de certificado.

– Los datos de registro se intercambiarán de forma segura y solo con proveedores de servicios de registro reconocidos, cuya identidad esté autenticada.

– Controles de personal.

– Asegurar de que los operadores respalden la fiabilidad de las operaciones.

– Se empleará personal que posean los conocimientos, la fiabilidad, la experiencia y las calificaciones necesarias y que hayan recibido formación sobre las normas de seguridad y protección de datos personales según corresponda para los servicios ofrecidos.

– Seguridad de operaciones.

– Se utilizarán sistemas y productos confiables que estén protegidos contra modificaciones y aseguren la seguridad técnica y la confiabilidad de los procesos soportados por ellos.

– La integridad de los sistemas e información debe estar protegida contra virus, software malicioso y no autorizado.

– Los medios utilizados dentro de los sistemas deben manejarse de forma segura para proteger los medios de daños, robos, accesos no autorizados y obsolescencia.

– Se deberá especificar y aplicar procedimientos para garantizar que:

1.– Los parches de seguridad se aplican dentro de un tiempo razonable después de que estén disponibles.

2.– Los parches de seguridad no se aplican si introducen vulnerabilidades o inestabilidades adicionales que superan los beneficios de su aplicación.

3.– Se documentan las razones para no aplicar ningún parche de seguridad.

– Seguridad de red.

– Se protegerá la red y sistemas de ataques.

– Se tomarán medidas técnicas y organizativas apropiadas contra el tratamiento no autorizado o ilegal de datos personales y contra la pérdida accidental o destrucción de datos personales.

En todo caso, deberá implantar mecanismos para:

– Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

– Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

– Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.

– Seudonimizar y cifrar los datos personales, en su caso.

l) Destino de los datos.

Destruir los datos, una vez cumplida la prestación.

Una vez destruidos, Izenpe deberá certificar su destrucción por escrito, entregando el certificado al Responsable del Tratamiento.

No obstante, Izenpe puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

Segundo.– Prorrogar por un año la duración del Acuerdo de colaboración entre Lanbide-Servicio Vasco de Empleo e Izenpe, para la puesta en marcha de medios de identificación electrónicos basados en la captación de datos biométricos, por medio del cual Lanbide actúa como Entidad de Registro de Izenpe para la expedición de medios de identificación digital y firma electrónica B@K y B@K Q.

La presente prórroga surtirá efecto desde el 26 de octubre de 2018 y tendrá una duración de 1 año desde la misma. Para una nueva prórroga y/o finalización de la presente, se hará conforme a la cláusula tercera del citado Acuerdo de colaboración.

Y en prueba de conformidad, y para que conste a los efectos oportunos, se firma esta Adenda de prórroga en el lugar y fecha arriba indicados.

La Presidenta de Lanbide-Servicio Vasco de Empleo,
BEATRIZ ARTOLAZABAL ALBENIZ.

Por Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios Izenpe, S.A.,
IZASKUN URRESTARAZU AMONDARAIN.