

- **Expediente N.º: EXP202500496**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

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

HECHOS

PRIMERO: Con fecha 9 de diciembre de 2024, se presentó reclamación ante la Agencia Española de Protección de Datos contra **OCTOPUS ENERGY ESPAÑA, S.L.** con NIF **B40563082** (en adelante, OCTOPUS o la parte reclamada). Los motivos en que basa la reclamación son los siguientes:

La parte reclamante manifiesta que, en fecha 17 de junio de 2024, su empresa suministradora NATURGY, le comunica la baja como su comercializadora. Señala que tras comunicarse con NATURGY le informan que la baja la ha solicitado un tercero, sin su consentimiento, siendo la nueva empresa OCTOPUS.

Junto a la notificación se aporta la siguiente documentación:

- Copia de la denuncia policial de 18 de junio de 2024 y ampliación de 14 de noviembre de 2024, en la que además manifiesta haber recibido dos correos no deseados de 13 de junio a nombre de **A.A.A.** de Lima (Perú).
- Copia del correo de NATURGY de 2 de octubre de 2024 confirmando la baja de los servicios de mantenimiento de gas a 1 de octubre de 2024 e informando de que el suministro de electricidad fue dado de alta por otra comercializadora el 14 de junio de 2024.
- Copia de la captura de pantalla de sus suministros en la web de su suministradora.
- Reclamación dirigida a OCTOPUS de 19 de octubre de 2024 por la suplantación de su identidad y correos electrónicos intercambiados con el delegado de protección de datos de la parte reclamada, desde 9 de octubre a 15 de noviembre de 2024 en los que se le informa de que la contratación se hizo por la web desde la dirección de email *****EMAIL.1**, la IP *****IP.1** y cuenta bancaria terminada en ****XX**. La parte reclamante manifiesta que investigó que dicha IP está localizada en Lima (Perú).
- Carta de Experian de 5 de agosto de 2025 comunicando la inclusión en el fichero de morosidad Badexcug por cuenta de la parte reclamada el 3 de agosto de 2025 por una deuda de 246 €.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación a OCTOPUS, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las

acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue recogido en fecha 22 de enero de 2025 como consta en el acuse de recibo que obra en el expediente.

Con fecha 18 de febrero de 2025 se recibe en esta Agencia escrito de respuesta de OCTOPUS indicando que la contratación se produjo antes de la implementación de mejoras en el proceso de contratación para evitar fraudes. En concreto, señala lo siguiente:

- *“En (...) a través de la página web de OCTOPUS (<https://octopusenergy.es/>) (...) para el domicilio el (...). Seguidamente, el día 17 de junio de 2024, la anterior suministradora energética con la que originalmente el reclamante tenía contratado el servicio le comunicó que le daba de baja del servicio. Ante esta información el reclamante se puso en contacto con ellos para pedir explicaciones.*
- *La Compañía bajo la dirección y liderazgo del equipo ejecutivo, ha implementado recientemente, en concreto en noviembre de 2024, dentro de las herramientas para la detección del fraude existentes en el mercado, un sistema para bloquear las posibles altas falsas en el proceso de onboarding digital que ofrece OCTOPUS a través de su página web a fin de mitigar el número de contrataciones fraudulentas e implementar controles de seguridad adecuados, y todo parece indicar su correcto funcionamiento siendo esta reclamación en base a un supuesto anterior a la implantación de este nuevo sistema.*
- (...)”

TERCERO: Con fecha 19 de febrero de 2025, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

1) Se solicita información a la parte reclamada y se obtiene respuesta donde manifiesta lo siguiente (el subrayado es de esta Agencia):

“Primera. - Respecto a la copia de RAT de la actividad afectada por la reclamación.

(...) En relación con el tratamiento objeto de la presente reclamación, en el RAT se recogen de forma estructurada y detallada los elementos exigidos por la normativa, incluyendo, a modo enunciativo pero no limitativo, la finalidad del tratamiento, las categorías de datos tratados, los destinatarios previstos y los plazos de conservación.

Se adjunta como **documento 1** el RAT respecto de la gestión de la contratación online.

El tratamiento relativo a la gestión de la contratación online se lleva a cabo con la finalidad de gestionar el servicio de suministro eléctrico, incluyendo altas, bajas y cambios de comercializadora. Este proceso comprende distintas fases, desde la recogida inicial de los datos hasta su validación y la formalización del contrato, desarrollándose siempre conforme a los principios de licitud, lealtad, transparencia y minimización de datos. La información contenida en el RAT permite verificar de manera objetiva cómo se ejecuta dicho tratamiento y acreditar su adecuación a la normativa de protección de datos. Dado que la finalidad del tratamiento es precisamente la gestión de la contratación del suministro, el RAT recoge de forma estructurada todos los elementos exigidos por la normativa aplicable respecto a este tratamiento en particular.

Segunda. - Respecto a la fecha de inicio de este tratamiento.

En fecha 12/06/2024 a través de la página web de OCTOPUS (<https://octopusenergy.es/>) se formalizaron un contrato de suministro de energía eléctrica y otro de gas para el (...) en nombre de A.A.A..

Tras la contratación del servicio a través de la página web, en cumplimiento de la normativa, OCTOPUS envió correo electrónico facilitado en el momento de la contratación, copia de los contratos de suministro eléctrico y de gas firmados mediante firma digital del supuesto contratante en la que figura nombre, DNI del firmante y fecha y hora de la firma, así como las condiciones generales y particulares del contrato, garantizando la trazabilidad y validez del consentimiento prestado.

Se adjunta a continuación captura de la firma digital utilizada en la formalización del contrato de **A.A.A.**.”

Se comprueba que la captura de pantalla contiene respecto del cliente, el nombre completo y DNI del titular, y un pie de firma: *Firmado digitalmente por* nombre del titular y *Fecha: 12-06-2024, 16:15:22*.

“Seguidamente, el día 17 de junio de 2024, la anterior suministradora energética con la que originalmente el reclamante tenía contratado el servicio le comunicó que le daba de baja del servicio. Ante esta información el reclamante se puso en contacto con ellos con el fin de obtener aclaraciones sobre lo sucedido. Tras diversos intercambios de comunicaciones para clarificar la situación con el reclamante, en el mes de octubre el **A.A.A.** solicitó a nuestra Compañía el desistimiento en distintas fechas para cada servicio de luz y gas confirmándose de forma inmediata su petición por OCTOPUS pese que estuvo manteniendo el servicio de luz y gas más de 4 meses desde el alta de la contratación finalmente fraudulenta.

En cuanto se tuvo conocimiento de la voluntad de A.A.A. de desistir del servicio contratado, se procedió de forma inmediata a gestionar dicha solicitud (...).

Tercero.- Respecto a la acreditación de todos los documentos vinculados a la contratación reclamada, así como todos los datos personales recogidos.

(...) la entidad OCTOPUS, en su condición de responsable del tratamiento, manifiesta lo siguiente:

Documentación vinculada a la contratación:

- a. Condiciones generales y particulares aceptadas por el cliente.
- b. Confirmación de la contratación y comunicación de bienvenida.
- c. Facturas emitidas.

La citada documentación se adjunta al presente escrito como **documento 2, 3, 4** respectivamente”.

Se comprueba que el documento 2 contiene los datos identificativos de la parte reclamante, junto con las “Condiciones particulares del contrato, fecha de contrato: 12-06-2024 y Condiciones generales de contratación de servicios de luz y gas OCTOPUS ESPAÑA ENERGY ESPAÑA S.L.U v2024-01, Firmado digitalmente por: **A.A.A.** Fecha: 12-06-2024, 16:15:24”, y los CUPS de gas y luz, respectivamente, en las pgs.12 y 19.

Se comprueba que el documento 3 contiene copia de un correo con el contrato enviado el día reclamado 12/6/2024 a la dirección electrónica *****EMAIL.1**, a la dirección IP *****IP.2** para los dos CUPS de electricidad y gas.

Se comprueba que el documento 4 contiene 6 facturas de fechas de emisión de 19/7/2024 a 12/11/2024, una de gas y cinco de electricidad.

“Respecto a la tipología de datos personales del reclamante tratados en el marco de la citada contratación; se han recabado y tratado exclusivamente los datos personales necesarios para la formalización, gestión y ejecución del contrato, de conformidad con el principio de minimización de datos (art. 5.1.c RGPD). En concreto los siguientes:

- a. Datos identificativos: nombre y apellidos, DNI/NIE, dirección postal y CUPS.
- b. Datos de contacto: número de teléfono, correo electrónico.
- c. Datos contractuales: fecha de contratación, tipo de servicio/producto contratado, condiciones económicas, historial de modificaciones contractuales.
- d. Datos de facturación y pago: datos bancarios (IBAN), información de transacciones realizadas.
- e. Datos de navegación o interacción digital: cuando la contratación se ha efectuado por medios electrónicos (por ejemplo, direcciones IP, logs de acceso, aceptaciones en plataforma, etc.).

Cuarta. - Respecto a la acreditación de la base legitimadora de dicho tratamiento.

(...) los contratos de suministro fueron formalizados electrónicamente a través de la página web de OCTOPUS, y constaban firmados digitalmente a nombre de **A.A.A.**. Esta circunstancia llevó a la Compañía, en un primer momento, a considerar que la contratación se había realizado de forma legítima, conforme al procedimiento habitual y a lo previsto en la normativa vigente.

En este sentido, y hasta que se tuvo conocimiento de que el **A.A.A.** no había autorizado dicha contratación y manifestó su voluntad de desistir, el tratamiento de sus datos personales se basaba en lo dispuesto en el artículo 6.1.b del Reglamento General de Protección de Datos (RGPD), al ser necesario para la ejecución de un contrato en el que el interesado figuraba, en apariencia, como parte contratante. Esta base legal, junto con la información recogida en el contrato de prestación de servicios y la Política de Privacidad de nuestra web, sustentaba inicialmente dicho tratamiento.

No obstante, tan pronto como el reclamante trasladó a nuestra empresa su voluntad de desistir de los contratos y manifestó que su identidad había sido presuntamente suplantada, de forma inmediata se procedió a dar de baja ambos contratos como se ha expuesto anteriormente.

Quinta.- Respecto a los controles realizados para verificar la identidad de la persona que realiza la contratación.

(...) los procesos de contratación en OCTOPUS se realizan exclusivamente a través de su página web, siendo el propio consumidor quien, de forma voluntaria, cumplimenta los formularios habilitados, acepta los términos y condiciones, y consiente expresamente la política de privacidad. Todo ello está disponible de manera clara, transparente y accesible antes de formalizar la contratación. Por tanto, dichos procesos se ajustan estrictamente a la normativa aplicable en materia de contratación a distancia y a la legislación del sector eléctrico. (...) la contratación que ha motivado la presente reclamación —realizada el 17 de junio de 2024 a nombre de **A.A.A.**— tuvo lugar con anterioridad a la implantación de un nuevo sistema avanzado de detección de fraudes en los procesos de contratación online, el cual fue introducido en octubre de 2024 como parte del compromiso de OCTOPUS con la mejora continua en materia de ciberseguridad y prevención del fraude.

Desde la implantación de este sistema, la Compañía ha destinado recursos significativos, tanto técnicos como humanos, para reforzar la seguridad de sus procesos internos y minimizar el riesgo de suplantaciones de identidad o contrataciones fraudulentas y la capacitación del personal clave en la identificación de patrones sospechosos. El contrato de **A.A.A.** fue formalizado conforme a los procedimientos digitales estándar vigentes en la fecha del alta (junio de 2024), los cuales, en ese momento, cumplían con las garantías exigidas por la normativa de contratación a distancia dado que el contrato fue firmado digitalmente, enviado al correo electrónico facilitado en el proceso de alta y confirmado mediante la aceptación explícita de los términos y condiciones, los cuales se presentaban de forma clara y accesible.

Pese a que el **A.A.A.** comunicó su disconformidad con la contratación transcurridos cuatro meses desde la formalización, en el momento en que la compañía tuvo conocimiento del posible caso de suplantación, se actuó de inmediato para cancelar la contratación no autorizada y realizar las investigaciones internas pertinentes. Esta respuesta rápida y diligente refleja el compromiso de OCTOPUS con la protección de los derechos de los consumidores, incluso en casos en los que, a priori, no se aprecia una actuación anómala por parte del sistema.

El sistema de contratación digital vigente en junio de 2024 era coherente con los estándares del sector y proporcionaba un equilibrio adecuado entre la experiencia del usuario y la seguridad del proceso bajo un procedimiento legítimo y conforme a derecho. No obstante, y como parte de su compromiso con la mejora continua, en noviembre de 2024, OCTOPUS reforzó dicho sistema incorporando tecnologías adicionales de detección de fraude, tales como:

- a. Llevar a cabo una evaluación y supervisión interna del proceso de contratación para revisar el número de altas fraudulentas que se producen a partir de la implantación de las medidas correctoras y evaluar su eficacia. Desde la fecha de la reclamación se han reducido considerablemente, al haberse bloqueado más de 20.000 contrataciones fraudulentas, tal y como se puede apreciar en la captura de pantalla del sistema ***HERRAMIENTA.1, adjunto como Documento 5 (...).
- b. Control interno para identificar accesos sospechosos desde ubicaciones no habituales fuera de España.
- c. Establecimiento de alertas automáticas en los sistemas internos para notificar intentos repetidos de alta desde un mismo dispositivo.
- d. Remisión de comunicado interno al personal de la Compañía recordando la existencia de procedimientos en cumplimiento de la normativa de protección de datos y direcciones de contacto del DPD y legal Counsel
- e. Establecimiento de un plan de formación interno en 2025 que ya se ha llevado a cabo por el DPD a los distintos departamentos de la empresa.

Respecto a los controles realizados por la Compañía debemos señalar que OCTOPUS lucha de forma proactiva contra el slamming, práctica muy habitual que afecta al sector de las eléctricas, y supone el cambio de distribuidora energética, sin consentimiento expreso del cliente. En cuanto el slamming se hace efectivo, se ejerce el derecho de desistimiento o se produce un nuevo movimiento de slamming en favor de la empresa comercializadora original. Este problema perjudica de igual forma al consumidor y a la empresa receptora del switching, por este motivo OCTOPUS está implantando una serie de medidas con el objetivo de erradicar este problema;

(...)

(...) la Política de la Compañía se basa en captar y fidelizar a clientes que realmente desean estar con Octopus y darles el mejor servicio a los clientes.

Sexta.- Respecto a acreditar el análisis de riesgos para los derechos y libertades realizado antes de la reclamación indicando si se consideró el riesgo vinculado a la suplantación de la identidad en la contratación, detallando y acreditando las medidas implantadas a raíz de este análisis.

OCTOPUS (...) habitualmente realiza un análisis inicial de riesgos asociado al tratamiento con el objetivo de enfocar adecuadamente los esfuerzos en una gestión proporcional de los riesgos. (...)

El análisis de riesgos realizado sobre el tratamiento objeto de la presente reclamación dio como resultado un nivel de riesgo bajo, teniendo en cuenta las características específicas del tratamiento y el hecho de que no se identificaron amenazas significativas para los derechos y libertades de los interesados en el proceso de la contratación online de los suministros de OCTOPUS. Esta valoración se basa en la tipología de datos tratados, la información suministrada a los interesados, los posibles escenarios de impacto y las medidas de mitigación y garantías organizativas aplicadas.

En atención al requerimiento efectuado por la AEPD se informa que el análisis de riesgos del tratamiento objeto de la reclamación figura en la pestaña ARI y ARR del **documento 1** adjunto al presente escrito relativo al RAT.

Séptima.- Respecto a la acreditación del nuevo análisis de riesgo realizado y la implantación de las nuevas medidas para mejorar los tratamientos y reducir los riesgos junto con su fecha de implantación,

(...) tras detectar intentos de contrataciones fraudulentas durante el ejercicio 2024, la entidad ha implantado, de forma proactiva y en coherencia con su política de mejora continua, herramientas de prevención del fraude que permiten detectar posibles suplantaciones de identidad en los procesos de contratación, minimizando así el riesgo de que estas situaciones lleguen a materializarse y cumpliendo siempre la normativa y prácticas del sector energético.

Estas herramientas, que han sido evaluadas como idóneas, incorporan mecanismos técnicos de verificación de identidad, así como controles adicionales en los procesos de contratación digital, con el objetivo de mitigar el riesgo de fraude. Las medidas se implantaron en octubre de 2024, por lo que no se encontraban operativas en el momento en que se produjo el alta de A.A.A. Actualmente, dichas herramientas están plenamente integradas y en funcionamiento, lo que ha contribuido a una reducción significativa de los intentos de contratación fraudulenta. (...)

Octava.- Respecto a la justificación del motivo de la inclusión en fichero de morosidad de los datos de la parte reclamante estando reconocido que la deuda no es cierta.

Tras la recepción de la reclamación y la correspondiente revisión interna de los procesos operativos vinculados a la gestión de impagos, esta Compañía ha podido constatar que la inclusión de los datos de **A.A.A.** en el fichero de

solvencia patrimonial fue consecuencia de un error humano puntual, en el marco del proceso de revisión y notificación de una deuda que, finalmente, no resultaba ser exigible dado que desde OCTOPUS se acordó su anulación pero dicha decisión ejecutiva no fue ejecutada de forma completa.

Dicho error derivó de una asignación errónea de identificador interno en la base de datos, lo que provocó que, de forma involuntaria y sin voluntad de causar perjuicio, se asociaran a **A.A.A.** datos relativos a un supuesto impago que efectivamente no procedía por lo que por error humano se llevó a cabo la comunicación de dicha deuda a un fichero de solvencia conforme al procedimiento habitual, pero de forma materialmente incorrecta.

(...) en ningún momento existió intencionalidad, negligencia grave ni ánimo lesivo por parte OCTOPUS sino un error en la operativa de forma asilada que se detectado como resultado de los mecanismos de revisión establecidos tras la recepción de la reclamación.

Tan pronto como se ha tenido conocimiento del error, desde OCTOPUS con la colaboración del DPO y el Legal Counsel se ha activado de forma inmediata los protocolos de subsanación, procediendo a:

- a. Notificar a la entidad gestora del fichero de solvencia la solicitud de eliminación de la información inexacta.
- b. Confirmar la eliminación definitiva de los datos de **A.A.A.** tanto del fichero de solvencia como de cualquier sistema interno de información crediticia.

Se adjunta como **documento 6** el certificado emitido por EXPERIAN acreditando la efectiva cancelación de la inclusión de los datos de **A.A.A.** en los ficheros de insolvencia”.

Se comprueba que tal documento contiene el certificado citado de EXPERIAN de 23/9/2025.

“Desde OCTOPUS se lamenta profundamente los inconvenientes ocasionados a **A.A.A.** y pese a lo ocurrido una vez se ha tenido conocimiento de lo sucedido se ha reaccionado de forma rápida y eficaz para restituir los derechos del interesado y evitar la consolidación de perjuicios económicos, reputacionales o personales.

Asimismo, a raíz de esta incidencia, se han adoptado medidas técnicas y organizativas adicionales para reforzar los controles internos y minimizar el riesgo de que puedan producirse situaciones similares en el futuro. Entre otras acciones, se ha iniciado una revisión específica de los procedimientos vinculados a la validación previa a cualquier comunicación a ficheros de morosidad, en línea con el principio de exactitud del artículo 5.1.d del RGPD.

(...)

Décima.- Respecto a la acreditación del requerimiento previo de pago al reclamante

A efectos de atender el requerimiento efectuado se adjunta como **documento 7** el requerimiento previo pago”.

Se comprueba que dicho documento contiene el citado requerimiento de 30/6/2025 dirigido a la dirección postal de la parte reclamante.

“Desde OCTOPUS en colaboración con el DPO se está revisando y reforzando los mecanismos internos encaminados a evitar situaciones de inclusión errónea o inexactitud de datos, estableciendo procedimientos de control adicionales para la verificación previa tanto de la deuda como de la legitimación, así como la formación específica del personal concernido.

Tras lo ocurrido, desde el departamento legal de OCTOPUS se ha elaborado un comunicado interno dirigido a los empleados, en particular al departamento de Credit, con el objetivo de concienciar sobre lo sucedido y reforzar la importancia de evitar este tipo de errores dado que no se alinean con los principios de responsabilidad y profesionalidad que rigen la cultura corporativa de la compañía.

Se adjunta como **documento 8** el comunicado emitido por el departamento legal de OCTOPUS dirigido al departamento de Credit responsable del área de impagados”.

Se comprueba que dicho documento es de fecha 17/9/2025.

2) Se solicita más información a la parte reclamada y se recibe respuesta el 21/10/2025:

1-Respecto de la contratación fraudulenta online realizada desde <https://octopusenergy.es> y los datos recogidos: datos identificativos, de contacto, datos de facturación y pago, y datos de navegación o interacción digital.

“(…) OCTOPUS trata diversos datos personales en el marco del proceso de contratación online a través de su página web <https://octopusenergy.es>. En concreto y en relación con la contratación objeto de la presente reclamación (…) se indican los siguientes datos:

- o Nombre y apellidos: **A.A.A.**
- o Documento Nacional de Identidad (DNI): **(…)**
- o Código Universal del Punto de Suministro (CUPS): **(…)**
- o Dirección postal: **(…)**
- o Correo electrónico: *****EMAIL.2**
- o Últimos cuatro dígitos de la cuenta bancaria asociada al pago: (dato recogido)
- o Dirección IP desde la que se realizó la contratación: *****IP.2**

Con el objetivo de acreditar lo indicado en este apartado, se adjunta como **documento 1** el contrato que ha dado lugar a la presente reclamación”.

Se comprueba que el email es distinto del facilitado por la parte reclamante en su reclamación, pero sí coinciden los datos de nombre y apellidos, DNI, dirección postal, CUPS de gas y electricidad.

2-Sobre el procedimiento de verificación de identidad de la persona que introduce los datos en su web para una contratación online.

“El procedimiento de verificación de identidad implementado en la plataforma de contratación online de OCTOPUS se encuentra respaldado por la normativa aplicable y está plenamente alineado con las prácticas habituales y aceptadas en el sector energético.

En la fecha en la que se llevó a cabo la contratación objeto de la reclamación y teniendo en cuenta que es el propio interesado quien introduce directamente sus datos personales en el formulario web y siendo un acto personalísimo, OCTOPUS entiende que este acto constituye el primer elemento de vinculación entre el contrato y su legítimo titular. Para llevar a cabo la contratación, el usuario debe aceptar expresamente las condiciones generales y particulares del servicio, y proceder a la firma electrónica del contrato. Posteriormente, el contrato es remitido a la dirección de correo electrónico facilitada por el usuario, lo que refuerza la trazabilidad del proceso.

Con el objetivo de acreditar la diligencia debida en la recogida de los datos durante el proceso de contratación, se adjunta como **documento 2** el formulario de contratación en el que se muestran los pasos para llevar a cabo la contratación”.

Se comprueba que dicho formulario requiere rellenar los campos: nombre, primer apellido, segundo apellido (opcional), NIF/NIE, número de teléfono, email; una casilla premarcada: “Mi dirección de facturación es la misma que la de suministro”; datos bancarios con nombre del titular e IBAN; leyenda: “Recibirás un email de *****PLATAFORMA.1**”; una casilla premarcada: “Declaro que soy la misma persona de los datos proporcionados y que he leído y acepto los términos y condiciones”; casilla con leyenda: “Escribe tu nombre completo para firmar” y una casilla para pulsar: Contratar.

“Sin perjuicio de lo anterior, en aplicación del principio de responsabilidad proactiva, desde noviembre de 2024 la entidad ha incorporado la herramienta *****HERRAMIENTA.1** como medida adicional, reforzando así los mecanismos de control y seguridad en sus procesos de contratación.

(...) con la implementación de dicha medida, OCTOPUS desarrolla su actividad conforme al principio de diligencia debida durante el proceso de contratación, en relación con el deber legal de cuidado, estructurado en cuatro elementos fundamentales: la identificación de riesgos, mediante la realización de análisis específicos como el aportado en la respuesta al primer requerimiento; la prevención, a través de la implantación de herramientas como *****HERRAMIENTA.1** orientadas a minimizar dichos riesgos; la mitigación, mediante el seguimiento activo de los riesgos detectados; y la rendición de cuentas, mediante una colaboración activa y transparente con los usuarios”.

3-Respecto del procedimiento de verificación de la firma digital en una contratación online.

“Con carácter previo a la contratación del suministro eléctrico a través de la web, el usuario realiza una acción afirmativa inequívoca (*opt-in*), mediante la cual declara ser el titular legítimo de los datos personales introducidos durante el proceso.

A continuación, el usuario procede a la firma electrónica del contrato, realizada mediante mecanismos que permiten vincular la acción al firmante, como la trazabilidad de la IP, el correo electrónico, el timestamp y el envío del contrato firmado al email facilitado.

(...) se adjunta una captura de pantalla del apartado relativo a la firma del contrato durante el proceso de contratación, así como una captura de pantalla relativa a la firma del contratante que ha dado lugar a la presente reclamación”.

Se comprueba que la captura de pantalla es el último paso del formulario citado antes de pulsar el botón de Contratar y los datos recabados para la firma: nombre y apellidos, NIF, Firmado digitalmente por y fecha, que se corresponden con los de la parte reclamante y fecha 12-06-2024, 16:15:22.

“(…) con carácter general la firma electrónica utilizada en un proceso de contratación de OCTOPUS cuenta con plena validez jurídica, conforme a lo dispuesto en el artículo 25.1 del Reglamento (UE) 910/2014 (eIDAS) y la normativa del sector energético por lo que no se pueden negar los efectos jurídicos por el hecho de ser una firma electrónica simple.

(...) la firma electrónica habilitada por OCTOPUS para llevar a cabo el proceso de contratación no se limita a la simple marcación de una casilla de aceptación en un entorno web, sino que OCTOPUS ha implantado un sistema que supera los estándares mínimos exigidos para este tipo de firma, ya que incorpora algunos de los requisitos propios de la firma electrónica avanzada establecidos en el artículo 26 del Reglamento eIDAS, como la imposibilidad de modificación posterior del documento firmado a través del timestamp.

(...) cuando el A.A.A. ejerció su derecho de desistimiento, OCTOPUS procedió de forma inmediata a la cancelación de su contrato”.

4-Respecto de las circunstancias de catalogación de la contratación como fraudulenta y comprobaciones realizadas.

“La contratación del suministro se desarrolló conforme a los protocolos establecidos, sin que se detectaran inicialmente indicios de irregularidad. La contratación se formalizó mediante la introducción de datos personales por parte del usuario, la aceptación de las condiciones y la firma electrónica del contrato, con las garantías descritas en los apartados anteriores y en cumplimiento de la normativa de protección de datos, contratación electrónica y del sector eléctrico.

No obstante, tras recibir una solicitud de desistimiento por parte de A.A.A., la entidad procedió de forma inmediata a la cancelación del contrato, en aplicación del principio de diligencia y respeto a los derechos del interesado, así como al inicio de un procedimiento interno de revisión de los hechos.

Como parte de las comprobaciones internas realizadas para determinar la posible existencia de fraude, se verificó la dirección IP desde la que se había realizado la contratación, identificando que el acceso se había producido desde una ubicación geográfica fuera del territorio nacional, concretamente desde Perú. Esta información, junto con la solicitud de desistimiento por parte del titular legítimo de los datos, llevó a la entidad a catalogar la contratación como fraudulenta.

Asimismo, en el ejercicio del principio de proactividad OCTOPUS procedió además al bloqueo de otros suministros asociados a la cuenta de correo como medida preventiva para evitar posibles fraudes. Estas actuaciones se enmarcan en el compromiso de OCTOPUS con la protección de los datos personales, la prevención del fraude digital, y el cumplimiento del principio de responsabilidad proactiva”.

5-Respecto de la descripción del sistema de contratación digital vigente en junio de 2024, fecha de la contratación fraudulenta.

“En junio de 2024, el proceso de contratación se desarrollaba íntegramente a través de la página web de OCTOPUS, mediante un procedimiento sencillo y transparente. Para formalizar el contrato, el cliente debía aceptar de manera expresa tanto las condiciones generales como las particulares del servicio, en base a los datos que él mismo facilitaba a la compañía. Una vez completado este paso, el sistema remitía automáticamente un correo electrónico de confirmación al cliente, en el que se incluían las condiciones contractuales aceptadas. Además, dichas condiciones quedaban permanentemente accesibles para el usuario desde su área privada en la web, lo que aseguraba la trazabilidad y disponibilidad de la información contractual en todo momento”.

Se comprueba que dicho email de confirmación con los contratos, anteriormente aportado, se envió al email *****EMAIL.1**, distinto del recogido en el formulario *****EMAIL.2** y distinto del aportado por la parte reclamante en la reclamación *****EMAIL.3**.

“(…) en esa fecha el sistema de contratación ya cumplía con las medidas de seguridad exigidas por la normativa, ofreciendo garantías suficientes frente a riesgos habituales en entornos digitales. No obstante, en aplicación del principio de responsabilidad proactiva y con el objetivo de seguir actuando con la diligencia debida, OCTOPUS ha seguido fortaleciendo sus sistemas de verificación e integridad estableciendo un sistema eficaz de medidas adecuadas al incorporar la solución tecnológica *****HERRAMIENTA.1**, diseñada para identificar patrones de comportamiento sospechosos y bloquear intentos de contratación desde ubicaciones geográficas fuera del territorio nacional. De este modo, aunque el sistema vigente en junio de 2024 ya ofrecía seguridad en

el proceso de contratación digital, la incorporación de ***HERRAMIENTA.1 ha supuesto un refuerzo adicional orientado a la prevención del fraude y a la máxima protección de los datos personales de los clientes”.

FUNDAMENTOS DE DERECHO

I

Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Presidencia de la Agencia Española de Protección de Datos.

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

II

Seguridad del tratamiento

El artículo 32 del RGPD estipula lo siguiente:

“1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

- a) la seudonimización y el cifrado de datos personales;*
- b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
- c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;*
- d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros."

III

Conclusión

La reciente STJUE de 24 de septiembre de 2024, en el asunto C-768/2021, señala (el subrayado es de la AEPD):

"37 A este respecto, ha de señalarse que el RGPD deja a la autoridad de control un margen de apreciación en cuanto a la manera en que debe subsanar la deficiencia constatada, puesto que el artículo 58, apartado 2, del mismo confiere a dicha autoridad la facultad de adoptar diversas medidas correctoras. Así, el Tribunal de Justicia ya ha declarado que la elección del medio adecuado y necesario corresponde a la autoridad de control, que debe realizar tal elección tomando en consideración todas las circunstancias del caso concreto y cumpliendo con toda la diligencia requerida su misión consistente en velar por el pleno respeto del RGPD (véase, en este sentido, la sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 112).

38 Sin embargo, este margen de apreciación está limitado por la necesidad de garantizar un nivel coherente y elevado de protección de los datos personales mediante una aplicación rigurosa de las normas, como se desprende de los considerandos 7 y 10 del RGPD

...

41 En consecuencia, no puede deducirse ni del artículo 58, apartado 2, del RGPD ni del artículo 83 de este la existencia de una obligación a cargo de la autoridad de control de adoptar, en todos los casos, cuando constate una violación de la seguridad de datos personales, una medida correctora, en particular una multa administrativa, siendo su obligación, en tales circunstancias, reaccionar adecuadamente para subsanar la deficiencia constatada. (...) En estas circunstancias, como señaló el Abogado General en el punto 81 de sus conclusiones, el autor de una reclamación cuyos derechos han sido vulnerados no dispone de un derecho subjetivo a que la autoridad de control imponga una multa administrativa al responsable del tratamiento. (...)

43 A este respecto, no se excluye que, con carácter excepcional y habida cuenta de las circunstancias particulares del caso concreto, la autoridad de control pueda abstenerse de adoptar una medida correctora aunque se haya constatado una violación de la seguridad de datos personales. Tal puede ser el caso, en particular, cuando la violación constatada no haya persistido, por ejemplo cuando el responsable del tratamiento, que, en principio, había aplicado medidas técnicas y organizativas apropiadas en el sentido del artículo 24 del RGPD, haya adoptado, tan pronto como

haya tenido conocimiento de dicha violación, las medidas adecuadas y necesarias para que la violación finalice y no vuelva a producirse, habida cuenta de las obligaciones que le incumben, en particular, en virtud de los artículos 5, apartado 2, y 24 del mencionado Reglamento.

44 La interpretación según la cual la autoridad de control, cuando constata una violación de la seguridad de datos personales, no está obligada a adoptar en todos los casos una medida correctora con arreglo al artículo 58, apartado 2, del RGPD se ve corroborada por los objetivos perseguidos por este artículo 58, apartado 2, y por el artículo 83 de dicho Reglamento, respectivamente.

45 Por lo que respecta al objetivo perseguido por el artículo 58, apartado 2, del RGPD, del considerando 129 de este se desprende que esta disposición tiene por objeto garantizar la conformidad del tratamiento de datos personales con dicho Reglamento y la regularización de las situaciones de incumplimiento de este para que se ajusten al Derecho de la Unión, mediante la intervención de las autoridades de control nacionales (sentencia de 14 de marzo de 2024, Újpesti Polgármesteri Hivatal, C-46/23, EU:C:2024:239, apartado 40).

46 De lo anterior se infiere que la adopción de una medida correctora puede, con carácter excepcional y habida cuenta de las circunstancias particulares del caso concreto, no imponerse, siempre que la situación de infracción del RGPD ya haya sido subsanada y que se garantice la conformidad de los tratamientos de datos personales con dicho Reglamento por su responsable y que tal abstención de la autoridad de control no menoscabe la exigencia de una aplicación rigurosa de las normas, tal como se ha recordado en el apartado 38 de la presente sentencia.”.

El TJUE incide, por tanto, en el margen de apreciación que tienen las autoridades de control para, en el ejercicio de sus funciones, desarrollar y optar entre los poderes atribuidos por el artículo 58 del RGPD, teniendo en cuenta las circunstancias del caso concreto, así como velando por el pleno respeto del RGPD. La consigna que debe regir siempre la actuación de una autoridad de control es asegurar un nivel alto de protección de los datos personales.

Así, cabe que, aun cuando se hubiera constatado o se tuvieran indicios de que se ha producido una vulneración en materia de protección de datos, las autoridades de control se abstengan de ejercitar sus poderes correctivos cuando esta presunta infracción hubiera sido subsanada y se garantice la conformidad de los tratamientos de datos personales con el RGPD.

Lo señalado por el TJUE en la sentencia antes citada, refuerza la idea de proporcionalidad de actuación de las autoridades de control que se recoge, con anterioridad a que fuera dictada la mencionada sentencia, en los artículos 65.4 y 65.6 de la LOPDGDD, por los que se permite a la AEPD, en atención a las circunstancias del caso concreto, la inadmisión a trámite o el archivo de reclamaciones, cuando, tras el traslado de las mismas al responsable del tratamiento, este demostrara haber adoptado medidas para el cumplimiento de la normativa aplicable.

En el presente caso, los hechos que impulsaron el inicio de actuaciones previas de investigación conforme al artículo 67 de la LOPDGDD, tras la recepción de una reclamación por la AEPD, se referían a la contratación fraudulenta de energía con OCTOPUS mediante la cumplimentación de un formulario online que recogía los datos personales, de contacto y de facturación. El formulario incluía una casilla para declarar

que se es la misma persona de los datos proporcionados y otra para introducir el nombre completo para firmar. El contrato se firmaba digitalmente con dicho nombre completo y la fecha del momento, y se remitía al email recogido en el formulario, sin ninguna otra verificación de la identidad.

Durante las actuaciones previas de investigación se ha comprobado que, efectivamente, la dirección de email recogida en el formulario es distinta de la aportada por el reclamante a esta Agencia, así como la dirección que consta en los emails intercambiados por la parte reclamante.

No obstante, tras ser informada por el reclamante sobre la contratación fraudulenta, OCTOPUS procedió a anular los contratos y a gestionar su baja en el fichero de morosidad. Asimismo, en su contestación a esta Agencia con fecha 6 de octubre de 2025, OCTOPUS señala que, con posterioridad a los hechos reclamados, implantó en noviembre de 2024 nuevos mecanismos técnicos de verificación de identidad y medidas adicionales de seguridad a contrataciones fraudulentas, tales como:

- “a. Llevar a cabo una evaluación y supervisión interna del proceso de contratación para revisar el número de altas fraudulentas que se producen a partir de la implantación de las medidas correctoras y evaluar su eficacia. Desde la fecha de la reclamación se han reducido considerablemente, al haberse bloqueado más de 20.000 contrataciones fraudulentas, tal y como se puede apreciar en la captura de pantalla del sistema ***HERRAMIENTA.1, adjunto como Documento 5 (...).*
- b. Control interno para identificar accesos sospechosos desde ubicaciones no habituales fuera de España.*
- c. Establecimiento de alertas automáticas en los sistemas internos para notificar intentos repetidos de alta desde un mismo dispositivo.*
- d. Remisión de comunicado interno al personal de la Compañía recordando la existencia de procedimientos en cumplimiento de la normativa de protección de datos y direcciones de contacto del DPD y legal Counsel*
- e. Establecimiento de un plan de formación interno en 2025 que ya se ha llevado a cabo por el DPD a los distintos departamentos de la empresa. (...)*”

Esto pone de manifiesto la diligencia con la que el responsable del tratamiento actuó al reconocer las deficiencias en el sistema de verificación de la identidad.

Por otro lado, consecuencia de la contratación fraudulenta, se incluyeron los datos de la parte reclamante en un fichero de información crediticia. No obstante, consta en el expediente que, tras la recepción de la reclamación, OCTUPUS manifiesta que dicha inclusión fue consecuencia de un error puntual y acredita haber procedido a la eliminación de dicha información, informando a la parte reclamante al respecto.

En consecuencia, de conformidad con la STJUE de 24 de septiembre de 2024, en el asunto C-768/2021 y atendiendo a las singulares circunstancias que conforman este caso, en particular, la especial diligencia del responsable para asegurar el cumplimiento de la normativa de protección de datos, así como la desaparición del sistema de acceso objeto de investigación, esta Agencia considera que no procede el despliegue de sus poderes correctivos previstos en el artículo 58 del RGPD.

Todo ello sin perjuicio de las posibles actuaciones posteriores que esta Agencia pudiera llevar a cabo, aplicando los poderes de investigación y correctivos que ostenta.

Por lo tanto, de acuerdo con lo señalado, por la Presidencia de la Agencia Española de Protección de Datos

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a **OCTOPUS ENERGY ESPAÑA, S.L.** y a la parte reclamante.

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

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la Presidencia de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

940-101025

Lorenzo Cotino Hueso

Presidente de la Agencia Española de Protección de Datos