

- **Expediente N.º: EXP202415839**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

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

HECHOS

PRIMERO: La Agencia Española de Protección de Datos tuvo conocimiento, a través de denuncia presentada el 15/10/2024, de ciertos hechos que podrían vulnerar la legislación en materia de protección de datos.

Con fecha 11/11/2024 la Directora de Agencia Española de Protección de Datos (en adelante, AEPD), instó a la Subdirección General de Inspección de Datos (SGID) a iniciar las actuaciones previas de investigación a las que se refiere el artículo 67 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), para investigar a D.G. DE LA GUARDIA CIVIL con NIF S2816003D (en adelante, D.G.G.C.) en relación con los siguientes hechos:

La parte denunciante, señala que en el Pliego de Prescripciones Técnicas del expediente ***EXPEDIENTE.1, para la contratación de la red de puntos de recarga de los vehículos eléctricos de la Guardia Civil, y más específicamente en lo relativo a la activación y autenticación del usuario frente al punto de recarga, se establece un sistema que requiere el reconocimiento facial para la recarga de vehículos eléctricos.

La parte denunciante, al considerarlo un tratamiento de datos abusivo, por existir otros sistemas de identificación, se dirigió al Delegado de Protección de Datos de la entidad denunciada, sin recibir una respuesta convincente, indicándole que no estaba en funcionamiento, habiéndose realizado únicamente la instalación y que se encontraba en fase de pruebas, sin fecha de inicio concreta de puesta en marcha.

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 la parte reclamada, 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 18/12/2024 como consta en el acuse de recibo que obra en el expediente.

Con fecha 8/01/2025 se recibe en esta Agencia escrito de respuesta del DPD de la D.G.G.C., indicando en esencia, que *“ante el requerimiento de información de la AEPD este DPD ha realizado la recomendación de la inmediata paralización de las recargas*

de vehículos eléctricos con uso de biometría, si se estuvieran realizando, en tanto no quede clarificado en qué circunstancias se están efectuando dichas labores de recarga y esté dado de alta el tratamiento de datos personales en el Registro de Actividades de Tratamientos de la DGGC. Igualmente se incide en la necesidad de proceder al borrado seguro, en su caso, de la biometría de aquellos Guardias Civiles que la hubieran prestado, aunque hubieran otorgado su consentimiento”.

TERCERO: 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:

Con fechas 18/12/2024, 17/2/2025 y 5/9/2025 se solicitó por la Inspección de Datos a la parte denunciada, información en relación con los hechos denunciados. Con fechas 8/1/2025, 3/3/2025, 4/3/2025, 6/3/2025, 3/6/2025 y 18/9/2025, tuvieron entrada en esta Agencia los respectivos escritos de respuesta a los requerimientos, en los que el representante de la D.G.G.C. informa de lo siguiente:

- La Dirección General de la Guardia Civil ha llevado a cabo un proyecto para la adquisición e instalación de una Red de Puntos de Recarga (PdR) con Plataforma de Gestión Centralizada (PGC), para la recarga de los Vehículos Eléctricos (VE) del Cuerpo de la Guardia Civil, a implementar durante el ejercicio económico del año 2023, en las dependencias que la D.G.G.C. mantiene a lo largo de todo el Territorio Nacional. Consta en el expediente ***EXPEDIENTE.1, como adjudicatario de la licitación la mercantil *****EMPRESA.1**.
- El Proyecto, según contempla el PPT, tendría un sistema biométrico de identificación facial para la activación de los puntos de recarga, que no almacenaría o transmitiría datos personales o información biométrica de los individuos, se limitaría a realizar una comparativa y en caso de ser esta positiva, facilitará un número de serie a la aplicación autorizadora, de forma telemática. El sistema biométrico de identificación facial realizaría la identificación facial mediante la lectura de un código QR conteniendo los vectores biométricos faciales del individuo y la comparación con los vectores biométricos faciales de este, obtenidos por el sistema en el momento de la identificación, a través de su cámara y el motor de biometría facial contenido en este. La tarjeta con el código QR, contendría los vectores biométricos faciales y número de serie, que sería personal e intransferible, requerimiento que persigue que el individuo sea el único propietario de su biometría. Para la generación de los códigos QR que contendría los vectores biométricos y número de serie de los individuos autorizados a realizar operaciones de recarga, se suministraría una herramienta software que lo realizaría, pudiendo obtener los vectores biométricos del individuo a partir de su foto.
- Desde la fecha en la que se inició la ejecución del proyecto, en enero de 2023 se han utilizado tres procedimientos distintos para la activación y uso de los puntos de recarga

Desde enero de 2023 hasta el segundo semestre de 2024 informan de un procedimiento en fase de pruebas que conllevaba el tratamiento de datos

biométricos de los usuarios para el reconocimiento facial. Fue descartado ante la falta de viabilidad tras una evaluación de impacto que no fue finalizada.

Desde el segundo semestre de 2024 hasta enero de 2025: El procedimiento consistía en la obtención de un código QR de carácter provisional, válido por un periodo de un año, y para obtenerlo se debía acceder a través de un dispositivo oficial a una URL de la Guardia Civil, que llevaba a la página de “registro PdR”, donde el usuario se registraba y recibía un correo electrónico proporcionando el correspondiente código QR, que se podía utilizar para acceder al sistema, mediante el reconocimiento del mismo por la cámara, bien impreso en papel o mediante su exhibición, a través de la pantalla de un dispositivo electrónico.

Finalmente, confirman que desde enero de 2025 (desde el día 23/01/2025), se utiliza para la activación del punto de recarga una tarjeta RFID (tarjeta de radiofrecuencia) no personalizada, no teniendo almacenado ningún tipo de dato personal.

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

Tratamiento de categorías especiales de datos personales

El artículo 9 del RGPD, que regula el tratamiento de categorías especiales de datos personales, establece lo siguiente:

“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 sexual 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;
- b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión o de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;
- c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;
- d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;
- e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;
- f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;
- g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;
- h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;
- i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional;
- j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud."

III

Evaluación de impacto relativa a la protección de datos

La evaluación de impacto relativa a la protección de datos se regula en el artículo 35 del RGPD en los siguientes términos:

"1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

- a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
- b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o
- c) observación sistemática a gran escala de una zona de acceso público.

4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.

5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.

6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

7. La evaluación deberá incluir como mínimo:

- a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;
- b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
- c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y
- d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.

11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento."

IV

Conclusión

En el presente caso, la D.G.G.C. llevó cabo un proyecto para la adquisición e instalación de una Red de Puntos de Recarga (PdR) con Plataforma de Gestión

Centralizada (PGC), para la recarga de los Vehículos Eléctricos (VE) del Cuerpo de la Guardia Civil, a implementar en las dependencias que la DGGC mantiene a lo largo de todo el territorio nacional.

El procedimiento que conllevaba el tratamiento de datos biométricos fue usado en fase de pruebas desde enero de 2023 hasta el segundo semestre de 2024 y fue descartado ante la falta de viabilidad, a la vista de la realización del Estudio Previo de Análisis de Riesgo y Evaluación de Impacto. *el cual no fue finalizado, debido a que no se consideraba viable instaurar el procedimiento de identificación referido con anterioridad.*

Mediante este procedimiento se habrían generado códigos QR obtenidos con reconocimiento facial de los usuarios (miembros de la Guardia Civil) de los que se aporta certificado de borrado de los datos personales tratados.

Tal y como resulta de las actuaciones de investigación, desde el día 23/01/2025 se utiliza para la activación del punto de recarga una tarjeta RFID (tarjeta de radiofrecuencia) no personalizada, no teniendo almacenado ningún tipo de dato personal. Asimismo, con fecha 20/02/2025, se envió un correo electrónico a la empresa gestora de la PGC, comunicando que, a la mayor brevedad posible debía ser borrado cualquier tipo de dato personal que existiera en la Plataforma de Gestión Centraliza del Proyecto PdR.

Además de ello, a finales de enero de 2025, se ha realizado el bloqueo de la Plataforma de Registro, para que ningún usuario pudiera descargar ningún tipo de código QR. Si se accediera a la misma ((...)), *aparecería el mensaje de “Suspensión temporal del servicio por trabajos de actualización, ante cualquier incidencia diríjase a este negociado: Equipo técnico del Proyecto PdR”.*

A este respecto, cabe citar la Sentencia del Tribunal de Justicia de la Unión Europea (TJUE) de 24 de septiembre de 2024, dictada en el asunto C-768/2021, analiza un supuesto de brecha de datos personales en el que una Autoridad de Control (el Comisionado para la Protección de Datos y la Libertad de Información del Estado Federado de Hesse, Alemania) decidió no imponer sanción atendiendo a las circunstancias del caso concreto. En dicha sentencia se afirma lo siguiente:

“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 reconoce en esta sentencia 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 y 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 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, esta Agencia considera que, de forma excepcional, 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.

Así pues, 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 D.G. DE LA GUARDIA CIVIL.

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.

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos

940-101025