- **Expediente N.º: EXP202501010**

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: En fecha 27 de noviembre de 2024, se presentó reclamación ante la Agencia Española de Protección de Datos contra la D.G. DE LA GUARDIA CIVIL (en adelante, la parte reclamada o DGGC). Los motivos en que basa la reclamación son los siguientes:

La parte reclamante pone en conocimiento de la AEPD la posible comisión de varias infracciones de la normativa de protección de datos en un centro de trabajo de la Guardia Civil en ******LOCALIDAD.1***, siendo presuntamente responsable *(…)*. Los hechos fueron previamente denunciados por vía interna, concluyéndose que no existía infracción, motivo por el cual se trasladan a esta Agencia.

En concreto manifiesta que durante el periodo 2022-2024, se produjeron envíos masivos de correos electrónicos a cuentas personales de varios miembros (…) que contenían datos personales e infracciones penales de ciudadanos. Estas comunicaciones, denominadas "Novedades", incluían información identificativa y hechos relacionados con denuncias o detenciones, y eran remitidas fuera de los canales seguros corporativos, a direcciones privadas sin las debidas garantías de seguridad, afectando a miles de ciudadanos sin su consentimiento ni información previa.

Junto a la reclamación aporta: captura de pantalla con la petición de cómo escribir las Novedades.

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), mediante notificación electrónica, fue recibido en fecha 23/01/2025, como consta en el acuse de recibo que obra en el expediente.

En fecha 31/01/2025 se recibe en esta Agencia escrito de respuesta por parte del Delegado de Protección de Datos de la DGGC en la que *se solicita que sea facilitada*

a este DPD la información expuesta en el presente escrito, y esencial para atender correctamente el requerimiento y cumplimentar su solicitud de información."

TERCERO: En fecha 27 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:

En fecha 7 de mayo de 2025 se realiza un primer requerimiento de información a la parte reclamada, la cual responde con fecha 23 de junio de 2025, proporcionando la siguiente información y manifestaciones en su escrito de respuesta:

> *"El **(…),** responde a la identificación profesional **(...)** y cabe poner en contexto de esta AEPD que fue objeto de un parte disciplinario dirigido contra él por los mismos hechos, sobre el que se instruyó expediente por falta grave **(...)** a instancia del *****PUESTO.1**, concluido sin responsabilidad disciplinaria.*

La parte reclamada alega la probable prescripción de los hechos (desconocen si ha quedado acreditado la fecha exacta de ocurrencia de los hechos que se imputan al ***(…)*** y la autenticidad e integridad de las pruebas (desconocen si se han respetado las garantías relativas a la debida cadena de custodia de las supuestas pruebas).

En relación con el envío de Novedades a correos particulares:

DGGC señala que "*se ha verificado la remisión desde el **(…)***."

1. Procedimiento establecido para el envío de Novedades a los ***(…)*** (datos personales de denunciante/detenido/investigado, así como un relato de los hechos), indicando si se contempla el envío a correos particulares ***(…).***

La parte reclamada no proporciona el procedimiento establecido para el envío de Novedades a ***(…)***. Especifica:

> "*No se contempla el envío de novedades a cuentas particulares, dado que vulnera lo establecido en la **(…)**, que establece que "…todas las entradas y salidas de datos de carácter personal que se efectúen mediante correo electrónico se realizarán desde cuentas o direcciones de correo oficiales". Teniendo en cuenta que los componentes **(…)** tienen acceso a una cuenta con correo electrónico oficial, no es necesario el empleo de cuentas particulares*."

2. Análisis de riesgos y medidas de seguridad implementadas para el envío de novedades a correos *(…)*.

DGGC aclara que no se considera oportuno puesto que no se contempla la remisión a cuentas particulares.

3. Copia de las instrucciones facilitadas a los usuarios en relación con el envío de datos personales de ciudadanos a correos particulares.

Añade que no se ha trasladado ninguna instrucción específica por los mismos argumentos precedentes.

4. Tiempo durante el que se conservan estos correos en los buzones personales de los destinatarios.

> "*El borrado de datos de las cuentas personales de los usuarios que, eventualmente, pudieran haber recibido dichas novedades, es responsabilidad de los mismos*."

5. En caso de que el envío de Novedades a correos particulares no esté contemplado en los procedimientos de ***(…)***, medidas adoptadas para evitar esta práctica.

> *Con posterioridad a la mala praxis observada en la transmisión (…), a fecha 18 de noviembre de 2024, se dictaminaron instrucciones concernientes a la transmisión de novedades* ***(…)***.

Con fecha 20 de octubre de 2025 se realiza un segundo requerimiento de información a la parte reclamada, la cual responde con fecha de registro 4 de noviembre de 2025, proporcionando la siguiente información y manifestaciones en su escrito de respuesta:

En relación con el envío de Novedades a correos particulares, la parte reclamada informa sobre el rango de fechas en el que se llevó a cabo este intercambio de correos y el número total de ciudadanos afectados:

> "*el primer correo se envió el día (…), y el último correo el día (…).*
> *[…]*
> *se enviaron (…) correos electrónicos relativos a hechos delictivos y (…) correos electrónicos por detenido e investigado, con una suma total de (…) personas afectadas."*

Con fecha 25 de marzo de 2026 se realiza un tercer requerimiento de información a la parte reclamada, la cual responde con fecha de registro 6 de abril de 2026, proporcionando la siguiente documentación en un fichero adjunto a su escrito de respuesta:
-Copia de las instrucciones dictaminadas por *(...)*, con fecha de firma *(…)*, concernientes a la transmisión de novedades.
- Copias del Orden del día de la ******REUNIÓN.1***.

Solicitada copia de las instrucciones dictaminadas por ***(...)*** concernientes a la transmisión de novedades, DGGC aporta documento, con fecha de firma *(…)*. Consiste en un documento firmado por el ******PUESTO.2*** y destinatarios: ***(…)***, que

incluye consideraciones relacionadas con la incorporación de información en los partes diarios de novedades y del que se extrae, entre otras manifestaciones:

> *"se debe tener presente el principio de minimización de datos"*
>
> *"durante la tramitación de las novedades para su remisión de forma fidedigna a (…), se debe realizar un tratamiento de las mismas al objeto de recabar los datos necesarios y presentarlos de forma precisa, omitiendo todos aquellos datos que carezcan de interés"*
>
> *"la información de carácter personal se debe transmitir codificada al objeto que solo las personas responsables puedan recabar los datos de su interés."*
>
> *"Respecto del resumen diario de novedades, […] debe omitir, en todos los casos, la referencia a cualquier dato de carácter personal de los autores, víctimas, perjudicados, etc."*
>
> *"la remisión de los partes diarios de novedades (PDN) a cuentas de correo corporativo "no unipersonales" permite (no impide, al menos) un hipotético mal uso de la información distribuida. Para evitarlo, se plantean dos opciones:*
> *a) remisión del documento a cuentas "no unipersonales", pero protegidos con una contraseña que previamente se ha facilitado a determinadas personas, de manera individualizada. […]*
> *b) remisión del documento a cuentas corporativas personales, no siendo necesario que el documento adjunto esté protegido con clave."*

Solicitadas evidencias de acciones formativas impartidas por la DGGC en materia de protección de datos que demuestren las medidas adoptadas para evitar incidentes similares, DGCC especifica la iniciativa*: I Jornadas "Seguridad de la Información y Protección de Datos",* celebradas entre los días 15 y 16 de octubre de 2024, y la convocatoria mensual a una reunión para ***(…)***. Aporta documento que consiste en copias del Orden del día de la ******REUNIÓN.1***:

. - (Pág. 3): Orden del día de la ******REUNIÓN.1*** de fecha *(…)*. Incluye:
- *Aspectos relacionados con el servicio:*
  - *Fotografías documentos de identidad a efectos identidad.*
  - *Comunicaciones datos sensibles.*

. - (Pág. 4): Orden del día de la ******REUNIÓN.1*** de fecha *(…)*. Incluye:
- *Empleo de tratamientos para eventos de masas (CCTV, etc.)*

. - (Pág. 5): Orden del día de la ******REUNIÓN.1*** de fecha *(…)*. Incluye:
- *Notificaciones en el ámbito de Guardia Civil: problemática desde el punto de vista de la protección de datos personales:*

. - (Pág. 6): Orden del día de la ******REUNIÓN.1*** de fecha *(…)*. Incluye:
- *. - Sanción por remisión de datos personales sin cifrar, vía GW*
- *. - Aspectos relacionados con el servicio*
  - *Instrucciones de uso de IMBOX Defense*

Respecto a las acciones formativas, se evidencia la realización de dichas jornadas en las páginas 226 y 323 del documento que se puede descargar desde el enlace:

******URL.1***

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

En el presente caso, ha quedado acreditado que, entre septiembre de 2021 y noviembre de 2024, se remitieron comunicaciones ("Novedades") que contenían datos personales, incluyendo información relativa a infracciones penales, a cuentas de correo electrónico particulares de miembros de la Unidad.

Asimismo, la propia DGGC, al mismo tiempo que niega que dicha práctica haya sido autorizada, reconoce que la misma no se ajusta a la normativa interna de seguridad, que establece la obligación de utilizar exclusivamente cuentas de correo corporativas para el tratamiento de datos personales.

No obstante, también ha quedado acreditado que, con posterioridad a los hechos:

Se dictaron instrucciones por *(...)* (noviembre de 2024) regulando la transmisión de novedades, incorporando expresamente principios de protección de datos como el principio de minimización de datos, la obligación de omitir datos que carezcan de interés, la transmisión de información de carácter personal de forma codificada, se establecieron criterios para el uso de cuentas corporativas, evitando el uso de correos electrónicos personales, se han llevado a cabo acciones formativas en materia de protección de datos, incluyendo jornadas específicas (octubre de 2024) y la convocatoria mensual de reuniones de mandos sobre esta materia.

Estas actuaciones evidencian la adopción de medidas correctoras destinadas a adecuar los tratamientos de datos a la normativa vigente y evitar la reiteración de los hechos denunciados.

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, 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 la D.G. DE LA GUARDIA CIVIL 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