- **Expediente N.º: EXP202413182**

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: Entrada de denuncia

Con fecha 17/09/2024, se presenta una denuncia contra EGARSAT, MUTUA COLABORADORA CON LA SEGURIDAD SOCIAL N.º 276 con NIF G64438997 (en adelante, EMCSS o EGARSAT). Los motivos en que basa la denuncia son los siguientes:

El denunciante se identifica como un trabajador autónomo afiliado a EMCSS, y pone de manifiesto que, al cumplimentar un trámite *(…)*, en el sitio web ******URL.1***, se puede acceder sin restricción a datos personales de trabajadores objeto de tratamiento por parte de este responsable.

SEGUNDO: Acuerdo de inicio de actuaciones previas de investigación

Con fecha 30/09/2024, la Directora de la Agencia Española de Protección de Datos acordó abrir una investigación de oficio e 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 EMCSS en relación con los hechos denunciados.

TERCERO: Inicio de actuaciones previas de investigación.

La SGID 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-Diligencias de investigación por Inspección de Datos

En fecha 23/10/2024, por parte de la Inspección de Datos, se accedió, a través del navegador Edge de Microsoft, a la dirección de internet indicada en la denuncia (***URL.1**), realizándose las siguientes comprobaciones:

- Dicho enlace permite el acceso a una aplicación web que contiene el logotipo EGARSAT de la que se desprende que tiene como finalidad la gestión de reclamaciones de los trabajadores de empresas que cuentan con los servicios de EGARSAT.
- La aplicación dispone de un menú con once opciones encabezada por la que se denomina "*Gestión de usuarios*" a la que se accede por defecto, y contiene aproximadamente 345 registros con los siguientes campos: Nombre, email y rol.
  El campo "*Nombre*", contiene en algunos casos un nombre y uno o dos apellidos y en la mayoría de los casos una dirección electrónica con el dominio egarsat.es.
  El campo "*email*" contiene una dirección electrónica bajo el dominio egarsat.es.
  Uno de los usuarios con el rol "*Admin*" es ***USUARIO.1**, que coincide con el que figura en la esquina superior derecha de la aplicación web, de lo que se desprende que es el usuario con el que se ha iniciado sesión en la aplicación a través del enlace.
- La tercera opción del menú se denomina "*incidencias externas*", que contiene un total de 3780 registros, con fecha de creación desde diciembre de 2016 hasta junio de 2024. El registro se compone de los siguientes campos: Nº Reclamación, Fecha Creación, Fecha Recepción, Centro, Nombre de quien la introduce, Trabajador, Empresa, Empresas/grandes cuentas, Área Resolución y Estado. El campo trabajador contiene datos personales correspondientes a nombre y apellidos.
- Cada registro dispone de una opción de acceder al detalle, que incluye, entre otros, el tipo de incidencia, fecha, tipo de contingencia, nombre, apellidos, DNI del trabajador, empresa y descripción de la incidencia. El campo "*descripción de la incidencia*" incluye, en algunos casos, datos relativos a la salud del trabajador introducidos a mano en la casilla, aportándose dos casos

2- En fechas 24/10/2024, 13/3/2025 y 8/9/2025 se solicitó, por la Inspección de Datos, a EMCSS información y documentación en relación con los citados hechos, recibiéndose, en fechas 5/11/2024, 18/3/2025 y 15/9/2025, los respectivos escritos de respuesta, de los que cabe destacar lo siguiente:

Tuvieron conocimiento de la brecha una vez recibido el requerimiento de la inspección de Datos y se realizaron las siguientes acciones inmediatas:

1. Abrir un expediente interno de Incidente de Seguridad.
2. Realizar Junto con el proveedor las siguientes acciones:
   1. Parar el servidor afectado
   2. Hacer un informe de lo ocurrido, elaborado por el encargado del tratamiento, del que adjuntan copia, para determinar el impacto y afectación, concluyendo que no ha habido un menoscabo de sus derechos fundamentales, ya que el servidor analizado no era el de

producción, si no uno de prueba, se determina que, por error, se modificó la configuración del Internet Information Server, y al reiniciar el servidor se publicó en internet,
3. Revisar los procedimientos de configuración del IIS.

3. Comunicar una brecha de seguridad a la Agencia Española de protección de datos
4. Comunicación a los afectados vía correos electrónicos. Se envió un email a los afectados en fecha 5/11/2024 desde la cuenta *(…)* mediante un proceso automático de java. Aportan fichero logs de envío *(…)* y plantilla del email.

La aplicación a la que se accede desde el enlace, *(…)*, tiene como finalidad la gestión, seguimiento y resolución de las reclamaciones presentadas por los usuarios, permitiendo un registro detallado y accesible de cada incidencia.

El acceso que permite el enlace es a un entorno de pruebas en el que se restauraron con fechas 1/7/2024 y 4/7/2024 copias de la base de datos que se explota en el entorno de producción.

Los datos almacenados en la base de datos de reclamaciones, según manifiestan, al tratarse en la mayoría de los casos de actos sanitarios se ha establecido un periodo de conservación de 5 años.

No se ha realizado un análisis de riesgo ya que, según manifiestan, el tratamiento no conlleva riesgo para los derechos y libertades de las personas, en concreto: 1. No hay Tratamientos a gran escala. 2. No se tratan datos sensibles 3. No se realizan evaluaciones sistemáticas y exhaustivas, ni tampoco hay tratamientos automatizados, ni la elaboración de perfiles. 4. No hay monitoreo a gran escala 5. No se han utilizado innovaciones tecnológicas que pueden tener un impacto significativo en la privacidad de los datos personales.

Aportan copia del documento “Informe de Actuaciones Relacionadas con el Incidente de Seguridad en el Sitio Web de Pruebas de EGARSAT”, elaborado por el encargado del tratamiento, en el que se recogen, entre otros, los siguientes puntos:

Respecto de los datos afectados

Manifiestan que, mediante el enlace mencionado, era posible visualizar datos de los trabajadores:

- Datos de usuarios que utilizan la aplicación: Email y Nombre de los empleados que utilizan la aplicación (USUARIOS)

- Datos de usuarios relacionados con incidencias: Nombre del trabajador, Correo electrónico del trabajador y DNI del trabajado, Nombre de la empresa y CIF/NIF de la empresa.

- Otros datos de las empresas colaboradores: Numero y nombre del colaborador.

Cronología de los hechos:

- El día 1/7/2024 se realizó una restauración de datos para pruebas de unificación de encuestas e histórico.
- El día 04/07/2024 se realizó una restauración de una copia de seguridad del 12 de junio para pruebas específicas de histórico y unificación de datos.
- El día 18/07/2024 se finalizaron las pruebas y se solicitó el cierre del sitio web de pruebas.
- El día 23/7/2024 se realizó el cierre del sitio de pruebas y se desplegaron los cambios en producción.
- El día 23/7/2024 el departamento de seguridad identificó que, aunque se había solicitado el cierre, el sitio seguía vinculado a la BDD, reactivándose al reiniciar el sistema.
- El día 24/10/2024 el departamento de seguridad procedió a la eliminación de enlaces en el servidor y restricción temporal de acceso al equipo de desarrollo tras la solicitud de un cliente.
- El día 25/10/2024 el departamento de seguridad procedió a la eliminación completa del servicio de reactivación automática para evitar reaperturas no autorizadas del sitio de pruebas.
- El día 25/10/2024 el departamento de seguridad catalogó el incidente como infracción grave y creación de una política de acceso y uso de copias de seguridad, requiriendo autorización mediante ADFS (autentica a los usuarios en aplicaciones incompatibles con el Directorio Activo integrado en Windows) para el entorno de pruebas.

Evaluación de Impacto y Análisis de Riesgos

Se llevó a cabo una Evaluación de Impacto en la Protección de Datos (DPIA) y un Análisis de Riesgos en relación con el incidente de seguridad detectado en el sitio de pruebas de EGARSAT, del que aportan el informe de conclusiones, en el que se desprende que se identificaron las Vulnerabilidades Específicas y se propone la adopción de medidas de seguridad, tras las cuales se concluye que el riesgo de exposición no autorizada se redujo a un nivel bajo. Se ha documentado el compromiso de mantener estas medidas y de realizar auditorías regulares para asegurar la eficacia de los controles implementados

Medidas de Seguridad Implementadas con posterioridad al incidente:

(…).

(…).

Gestión de Usuarios:

- ***(…).***
- ***(…).***
- ***(…)***.

Control de Accesos y Autenticación

- ***(…).***
- ***(…).***

Respecto de las causas que hicieron posible la brecha

- ***(…).***
- ***(…).***
- ***(…).***

Respecto del contrato de encargado del tratamiento

Aportan copia del contrato suscrito entre EGARSAT y DISEÑO Y DESARROLLO DE PROYECTOS Q2B, S.L. El objeto del contrato consiste en el "MANTENIMIENTO Y HOSTING DEL PROGRAMA (…)", indicados en el EXP. N.º (…)". Aportan copia del ANEXO I, "CONTRATO DE ENCARGO DE TRATAMIENTO DE DATOS PERSONALES".

Consta, con fecha de entrada en esta Agencia 30/10/204, la notificación de la brecha presentada por EGARSAT,

CUARTO: Entrada de dos reclamaciones

Con fechas 21/11/2024 y 19/12/2024, se recibieron dos reclamaciones, (reclamantes 1 y 2) según detalle en ANEXO GENERAL que manifiestan que han recibido una comunicación de brecha de EGARSAT, indicando el reclamante 2 que, aunque se le comunica que en la brecha de datos solo se han visto afectados su nombre y número del DNI, no puede saber el alcance real de la exposición, ya que su proceso *(…)* a cargo de EMCSS es seguido por dicha entidad actualmente y consta en los ficheros de EGARSAT.

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

Cuestiones previas

En el presente caso, consta que EMCSS gestiona las reclamaciones de trabajadores cuyas contingencias gestiona a través de la aplicación *(…)*. Durante una fase de pruebas terceros no autorizados pudieron acceder a los datos personales almacenados en la aplicación a través de durante el período 4/07/2024 a 24/10/2024.

EMCSS realiza entre otros tratamientos, la recogida/ registro/ organización/ almacenamiento/ conservación/ modificación/ consulta/ supresión/ destrucción de los siguientes datos personales de personas físicas, tales como: nombre/ número de identificación/ dirección de correo electrónico/ datos de salud.

EMCSS realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del citado artículo 4.7 del RGPD.

EMCSS contrató con DISEÑO Y DESARRROLLO DE PROYECTOS Q2B S.L., la gestión de la base de datos de *(…)*.

III

Violación de seguridad de los datos personales

El artículo 4 apartado 12 del RGPD define, de un modo amplio, las "*violaciones de seguridad de los datos personales*" (en adelante brecha de seguridad) como "*todas aquellas violaciones de la seguridad que ocasionen 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*."

En el presente caso, consta una brecha de seguridad de datos personales, al ser posible accesos desde una URL de internet (******URL.1***) a los datos personales contenidos en *(…)*.

Con fecha 23/10/2024, se constató por los Servicios de Inspección de esta Agencia que La brecha afectaba a 345 registros con campos de nombre, email y rol y 3780 registros campos: Nº Reclamación, Fecha Creación, Fecha Recepción, Centro, Nombre de quien la introduce, Trabajador, Empresa, Empresas/grandes cuentas, Área Resolución y Estado. El campo trabajador contiene datos personales correspondientes a nombre y apellidos

EMCSS ha manifestado que la violación de seguridad de los datos personales no fue consecuencia de una deficiencia en la gestión de usuarios y control de acceso al entorno de preproducción, sino de un error humano por parte del encargado de tratamiento.

(…).

Tras tener conocimiento del incidente de seguridad la entidad aplicó las siguientes medidas;

(…).
(…).
(…).

Respecto de la Gestión de Usuarios manifiestan lo siguiente:

- ***(…).***
- ***(…).***
- ***(…)***.

Y en cuanto al Control de Accesos y Autenticación aducen que:

- ***(…)***.
- ***(…)***.
- ***(…)***.

De tales circunstancias, cabe señalar que la identificación de una brecha de seguridad no implica la imposición de una sanción de forma directa por esta Agencia, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

La seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que regulan la seguridad del tratamiento, la notificación de una violación de la seguridad de los datos personales a la autoridad de control, así como la comunicación al interesado, respectivamente.

De acuerdo con el artículo 32 del RGPD el responsable y el encargado del tratamiento, 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, aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. Entre estas medidas se deberán incluir medidas para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

En este caso, como se ha indicado, EMCSS aplicó medidas efectivas que evitaron el acceso al entorno de pruebas. También notificó la violación de la seguridad de los datos personales y comunicó el incidente a los afectados en cumplimiento de lo dispuesto en los arts. 33 y 34 del RGPD.

III
Conclusión

El considerando 129 del RGPD indica que "[…] *Los poderes de las autoridades de control deben ejercerse de conformidad con garantías procesales adecuadas establecidas en el Derecho de la Unión y los Estados miembros, de forma imparcial,*

equitativa y en un plazo razonable. En particular, toda medida debe ser adecuada, necesaria y proporcionada con vistas a garantizar el cumplimiento del presente Reglamento, teniendo en cuenta las circunstancias de cada caso concreto…"

La sentencia del Tribunal de Justicia de la Unión Europea, (STJUE) de 26/09/2024, 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

39 Por lo que se refiere, más concretamente, a las multas administrativas contempladas en el artículo 58, apartado 2, letra i), del RGPD, del artículo 83, apartado 2, de este Reglamento resulta que aquellas se imponen, según las características propias de cada caso, con carácter adicional o en sustitución de las demás medidas previstas en el citado artículo 58, apartado 2. Además, ese mismo artículo 83, apartado 2, precisa que, al decidir la imposición de una multa administrativa y su cuantía en cada caso individual, la autoridad de control debe tener debidamente en cuenta los elementos que figuran en las letras a) a k) de esta disposición, como la naturaleza, la gravedad y la duración de la infracción"
(…)

"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 fueron puestos de manifiesto ante esta AEPD con motivo de una presunta brecha de seguridad de los datos personales sufrida por EMCSS.

La AEPD constató que era posible el acceso a los datos personales, si bien EMCSS en cuanto tuvo conocimiento del incidente aplicó medidas dejando sin funcionamiento el servidor de pruebas de preproducción el mismo día en que recibió el requerimiento de información de esta AEPD, dando a su encargado instrucciones para que tomara las medidas adecuadas a fin de evitar que continuara siendo posible el acceso a los datos personales.

Durante las actuaciones previas de investigación, se ha comprobado asimismo que, EMCSS notificó la brecha a esta AEPD y la comunicó a los afectados, adoptando nuevas medidas sobre el entorno en pruebas y sus accesos.

Se subraya que cuando se produce la respuesta por EMCSS al primer requerimiento, se había cerrado la posibilidad de la permanencia en la brecha.

En consecuencia, de conformidad con la citada STJUE y atendiendo a las singulares circunstancias que conforman este caso, en particular, la desaparición del eventual acceso al entorno de pruebas, esta Agencia considera que no procede el despliegue de sus poderes correctivos previstos en el artículo 58 del RGPD.

Por 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 **EGARSAT, MUTUA COLABORADORA CON LA SEGURIDAD SOCIAL N.º 276** y al RECLAMANTE 1 y RECLAMANTE 2 que figuran en el ANEXO GENERAL.

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, 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.

1245-101025

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

ANEXO GENERAL

Reclamante 1 ***A.A.A.***

Reclamante 2 ***B.B.B.***