- **Procedimiento Nº: E/09387/2019**

- **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 20/12/2018, la Directora de la Agencia Española de Protección de Datos acuerda iniciar las presentes actuaciones de investigación en relación a la notificación de una brecha de seguridad producida por EN MAREA, con NIF ***V70498191,*** al ser comprometida la confidencialidad y disponibilidad de los datos de los afiliados a este partido político.

La notificación de brecha de seguridad efectuada el 30/11/2018 contiene, entre otra, la siguiente información:

• Fecha de detección de la brecha: 27/11/2018

• Fecha de inicio de la brecha: 26/11/2018

• Brecha resuelta a 28/11/2018.

• Justificación de la notificación tardía: Asegurar la certeza de la posible gravedad de los hechos mediante el estudio detallado de los hechos ocurridos.

• Responsable del tratamiento: EN MAREA, cuyos datos se han incluido en el apartado de Entidades Investigadas.

• Resumen de la brecha: *"El día 27 de noviembre se tuvo conocimiento de que personas indeterminadas pertenecientes al Comité Electoral de EN MAREA (órgano designado para el control de proceso electoral según el "reglamento para a elección do consello das mareas e da comisión de garantías de EN MAREA") accedieron a la plataforma MEDRANDO (fichero de datos personales de las personas afiliadas) mediante claves de acceso solicitadas al técnico contratado por EN MAREA, sin seguir las instrucciones de acceso para cumplir correctamente con las funciones encomendadas reglamentariamente y legalmente, al tiempo que se me bloqueó mi propio acceso y el de todo el personal autorizado previamente para realizar sus funciones."*

• Tipología: Brecha de confidencialidad (acceso no autorizado).

• Medio por el que se ha materializado la brecha: Posible acceso mediante cesión de claves no autorizada.

• Que antes de la brecha se aplicaron las siguientes medidas preventivas:

o Restitución de claves a la persona responsable.

o Anulación de claves concedidas irregularmente.

o Requerimiento de identificación de personas con accesos irregulares.

o Requerimiento de razones de bloqueo de acceso a responsable.

o Requerimiento comité electoral de cesión de situación irregular.

o Contratación experto informático para auditar el acceso.

• Que las categorías de datos afectados son:

o Datos básicos.

o DNI, NIE y/o pasaporte.

o Credenciales de acceso o identificación.
o Datos de contacto.
o Datos sobre opinión política.

• Que el perfil de los sujetos afectados es afiliados a partido político afectando a un número aproximado de 4400 personas.

• Que la naturaleza del impacto potencial sobre los sujetos es el conocimiento de su afiliación política.

• Que cataloga la severidad de las consecuencias como “Alta”.

• Que las medidas tomadas para solucionar la brecha y minimizar el impacto fue la restitución de claves y contratación de un servicio externo que audite el posible impacto sobre los afectados.

El 12/12/2018 EN MAREA remite a esta Agencia documento de Auditoría de Seguridad Informática fechada el 08/12/2018. Las investigaciones objeto de esta auditoría comenzaron el 29/11/ 2018 y son realizadas a la plataforma de votaciones Medrando accesible en la dirección https://medrando.enmarea.gal, concluyendo que personas externas a la Coordinadora de EN MAREA, el 26/11/2018 accedieron al panel de administración de Medrando, no constando que se alterara la base de datos.

Asimismo, se han recibido dos reclamaciones relacionados con el incidente de seguridad notificado a esta AEPD: escrito de D. ***A.A.A.*** (reclamante 1), y D. ***B.B.B.*** (reclamante 2).

El 23/08/2019 EN MAREA remite escrito a la Agencia conteniendo la siguiente información:

1. Estructura orgánica de EN MAREA. Se aporta Reglamento para la elección del Consello de las mareas y de la Comisión de Garantías, así como los Estatutos.

2. Respecto a los tipos de usuarios y perfiles de la plataforma *Medrando*, que existen dos tipos de usuarios: usuario normal, el cual solo accede a su información personal y, usuario con rol administrador, el cual podía acceder a los datos de los usuarios en el panel de control. El acceso a documentación, como el DNI, requiere la introducción de una contraseña adicional por parte de un usuario administrador. Solo el responsable del censo tenía este acceso.

3. Señala los usuarios con perfil administrador en la plataforma *Medrando* en el momento del acceso no autorizado.

Asimismo, indica quien era el responsable del censo en el momento del incidente y que el responsable del tratamiento de los datos personales que se realiza en la plataforma *Medrando* era EN MAREA y que la gestión técnica de la plataforma *Medrando* la realizaba la entidad BISAGRA COMUNICACIÓN, S.L. y aporta copia del contrato de Acuerdo de Encargo del Tratamiento entre EN MAREA y BISAGRA COMUNICACIÓN, S.L.

La Delegada de Protección de Datos fue designada y comunicada dicha designación a esta Agencia el 11/09/2018.

Que la plataforma *Medrando* en la actualidad ya no se utiliza para la gestión del censo de EN MAREA habiendo sido sustituida por la localizada en la URL *https://censo.enmarea.gal*.

4. Posteriormente realiza un relato cronológico de los hechos ocurridos manifestando que 26/11/2018, personas del Comité Electoral, a través de un correo electrónico, requirieron a BISAGRA COMUNICACIÓN, S.L., acceso al fichero como administradores, quien se las facilitó, retirando el acceso a la persona designada por EN MAREA como responsable del censo.

Que el mismo día 26/11/2018 se revocaron los accesos concedidos a los miembros del Comité Electoral y se repuso el acceso al anterior responsable, quien dirigió comunicación por escrito, fechada a 27/11/2018, a los miembros del Comité Electoral para advertirles de la incidencia detectada y requerirles, primero, para no acceder bajo ninguna circunstancia al fichero (censo electoral) y, segundo, para abstenerse de cualquier cesión a terceras personas de la información accedida o proceder a recuperar cualquier copia o acceso que hubiese sido distribuido.

Para determinar con exactitud la magnitud de la incidencia, con fecha 29/11/2018, se encargó una auditoría y análisis forense para determinar el alcance y las posibles consecuencias de la incidencia.

Aún sin conocer el alcance de la incidencia y en previsión de que pudiese suponer una violación de la seguridad de los datos conforme al Reglamento UE 2016/679, se notificó la incidencia como brecha de seguridad a la Agencia Española de Protección de Datos.

Asimismo, tras el incidente, EN MAREA puso fin a su relación con BISAGRA COMUNICACIÓN, S.L. y contrató los servicios de hosting y mantenimiento de la plataforma Medrando a un nuevo proveedor, LEDMON MARKETING Y MULTIMEDIA S.L.U., y la Comisión de Ética y Garantías resolvió suspender cautelarmente con efecto inmediato a los miembros del Comité Electoral

5. No consta que se produjese utilización de los datos personales por terceros, ni parece que se extrajese dato alguno de la plataforma. Los accesos se realizaron por miembros del Comité Electoral de EN MAREA sin que conste uso o manipulación de los datos por su parte.

Hasta el momento no se ha procedido a comunicar la incidencia a los afectados al ser un número muy reducido y no haber evidencias de que la quiebra de seguridad pueda haber supuesto el acceso a la información por parte de terceras personas que no pudiesen conocer esa información en función de su cargo o funciones dentro de la organización.

6. Para el asesoramiento en materia de protección de datos así como para la realización del análisis de riesgos, EN MAREA contrató los servicios de la empresa PRODASVA CONSULTORÍA Y GESTIÓN S.L.

7. Atendiendo al análisis de riesgos realizado que determinó que las actividades de tratamiento realizadas por EN MAREA no entrañan un alto riesgo para

los derechos y libertades del interesado, no se requería una evaluación de impacto relativa a la protección de datos. Por otro lado, de conformidad con el art. 35 RGPD, la evaluación de impacto no resulta necesaria por tratarse de un tratamiento que ya se venía realizando con anterioridad a la entrada en aplicación del RGPD.

Se aporta registro de actividades del tratamiento y análisis de riesgos el cual contiene:

a. Una descripción teórica de la gestión de riesgos.
b. Y se señala que:

"Las actividades de tratamiento llevadas a cabo por EN MAREA no están expuestas a riesgos relevantes que motiven la necesidad de realizar una EIPD en profundidad.

Las medidas técnicas y organizativas que garanticen los derechos y libertades de los interesados, considerando que el nivel de riesgo al que están expuestas las actividades de tratamiento no es elevado, se pueden simplificar con un enfoque de mínimos recogidos en el siguiente punto".

Se aporta documento con las medidas técnicas y organizativas mínimas llevadas a cabo por EN MAREA con, entre otro, el siguiente contenido:

a. Medidas organizativas.

Todo el personal con acceso a datos personales tiene conocimiento de sus obligaciones con relación a los tratamientos de datos personales y ha sido informado acerca de dichas obligaciones.

b. Medidas técnicas respecto a:

Identificación de los usuarios.
Respecto a ordenadores y dispositivos.

Se aporta modelo de documento de información sobre medidas de seguridad a miembros de EN MAREA.

Se aporta documento sobre el procedimiento establecido ante brechas de seguridad.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 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 Directora de la Agencia Española de Protección de Datos.

II

El RGPD define las quiebras de seguridad de los datos personales como aquellos incidentes que ocasionan la destrucción, pérdida o alteración accidental o ilícita de datos personales, así como la comunicación o acceso no autorizado a los mismos.

Desde el pasado 25/05/2018, la obligación de notificar a la Agencia las brechas o quiebras de seguridad que pudiesen afectar a datos personales es aplicable a cualquier responsable de un tratamiento de datos personales, lo que subraya la importancia de que todas las entidades conozcan cómo gestionarlas.

Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales en el sentido señalado en el artículo 32 del RGPD debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas.

El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación.

Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continúas o similares.

También hay que señalar, que la notificación de una quiebra de seguridad no implica la imposición de una sanción de forma directa, 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.

En concreto el artículo 32 del RGPD *"Seguridad del tratamiento",* establece que:

"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".

En el artículo 33 del RGPD establece la forma en que ha de notificarse una violación de la seguridad de los datos personales a la autoridad de control, determinando lo siguiente:

"1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;
d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

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

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo."

Y el artículo 34 del Reglamento mencionado indica cuando es necesario informar de una violación de la seguridad de los datos personales al interesado, señalando lo siguiente:

"1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;
b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;
c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3."

En este mismo sentido se señala en los Considerandos 85 y 86 del RGPD:

(85) Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida.

(86) El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación. Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continuas o similares.

III

En el caso examinado, de la documentación obrante en el expediente ofrece indicios evidentes que de la brecha de seguridad provocada en los sistemas de la entidad vulneró el artículo 32 del RGPD, Seguridad del tratamiento, relacionada con el acceso a datos de carácter personal por parte de los miembros de comité electoral de En Marea.

Consta que la brecha fue detectada el 27/11/2018, habiendo sido resuelta el 28/11/2018 y notificada el 30/11/2018, justificando la demora en la necesidad de asegurar la incidencia de confidencialidad ocurrida mediante un estudio detallado y exhaustivo de los hechos.

Las investigaciones llevadas a cabo con el fin de identificar el fallo de seguridad producido en los sistemas, alcance, medidas a adoptar, etc., determinaron que personas pertenecientes al comité electoral de la formación accedieron mediante claves que le fueron aportadas por el técnico contratado sin seguir las instrucciones establecidas en estos casos. Rápidamente se anularon las claves concedidas, requiriendo la identificación de aquellas personas que habían provocado los accesos irregulares, suspendiendo cautelarmente con efecto inmediato a los miembros del Comité Electoral y el establecimiento de nuevas claves y credenciales de acceso, así como la contratación de un servicio externo de auditoria y análisis forense para determinar el alcance y consecuencias de la incidencia.

Hay que señalar que con independencia del incidente de confidencialidad las medidas técnicas y organizativas que habían sido adoptadas por la formación política eran adecuadas y proporcionadas al nivel del riesgo existente que presentaba el tratamiento de datos, no teniendo constancia de que se hubiera producido extracción, uso o manipulación de datos de carácter personal por parte de terceros.

Asimismo, se decidido no comunicar el incidente a los afectados al tener evidencias de que el acceso a la información se produjo por personas que podían conocer la misma como consecuencia de la función o el cargo que desempeñaban dentro de la organización, personas encargadas de la verificación de datos del censo.

IV

Por lo tanto, se ha acreditado que la actuación del reclamado como entidad responsable del tratamiento ha sido acorde con la normativa sobre protección de datos personales analizada en los párrafos anteriores.

Por lo tanto, de acuerdo con lo señalado,

Por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

1. PROCEDER al ARCHIVO de las presentes actuaciones.

2. NOTIFICAR la presente resolución a EN MAREA, con NIF ***V70498191,*** junto con el ANEXO 1 y a cada uno de los reclamantes con el ANEXO que le corresponda en el que se incluye su identificación.

.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública 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 Directora 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.

Mar España Martí
Directora de la Agencia Española de Protección de Datos

ANEXO I

Reclamante 1: D. A.A.A.
Reclamante 2: D. B.B.B.

ANEXO II

Reclamante 1: D. A.A.A.

ANEXO III

Reclamante 2: D. B.B.B.