Procedimiento Nº: PS/00431/2018

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos ante ***BALMORE ATLANTIC SL***, en virtud de actuación realizada de oficio y en base a los siguientes:

ANTECEDENTES

PRIMERO: Con fecha 05/09/2018 la Directora de la Agencia Española de Protección de Datos (en lo sucesivo AEPD), acordó iniciar de oficio las presentes actuaciones de investigación en relación con la noticia difundida por los medios de comunicación, relacionada con la posibilidad que tendrían los clientes de las tiendas *Xiaomi Mi Store Sol* y *Xiaomi Mi Store La Vaguada* propiedad de **BALMORE ATLANTIC, S.L.** (en adelante, BALMORE) cuando utilizan los terminales móviles que se encuentran en exposiciones a su disposición, de acceder a los correos electrónicos remitidos desde estas tiendas que en ocasiones contienen datos personales de empleado y clientes.

También con fecha 03/09/2018 **FACUA CONSUMIDORES EN ACCION**, en representación de D. ***A.A.A.***, había presentado reclamación ante la AEPD contra BALMORE por los siguientes hechos: brecha de seguridad en la citada empresa permitiendo acceder a datos personales tanto de clientes como de empleados.

SEGUNDO: A la vista de los hechos denunciados y de las actuaciones de investigación realizadas, se constata lo siguiente:

El 03-09-2018 fue publicada una noticia en el medio digital *"El Confidencial"* informando de una brecha de seguridad debida al descuido de un dependiente que en fecha 01-07-2018 configuró la cuenta de correo de demostración asignada a los dispositivos de exposición desde un terminal para uso de gestiones internas de la tienda.

Esto provocó que los correos enviados desde este terminal fueran visibles en algunos dispositivos expuestos en la tienda.

Los correos podían ser visualizados cuando los visitantes de la tienda accedieran a la aplicación de correo instalada en los móviles.

La resolución de la incidencia se realizó en fecha 03-09-2018 con las siguientes medidas:

1. Eliminar la cuenta de Gmail de los dispositivos en exposición
2. Asignación de un Delegado de Protección de Datos
3. Inhabilitación del uso de Gmail
4. Formación a todos los trabajadores.

Además, la entidad ha adoptado las siguientes medidas organizativas y técnicas.

MEDIDAS ORGANIZATIVAS

Todo el personal con acceso a los datos personales tiene conocimiento de sus obligaciones con relación a los tratamientos de datos personales y son informados acerca de dichas obligaciones. La información mínima conocida por todo el personal será la siguiente:

- DEBER DE CONFIDENCIALIDAD Y SECRETO

■ Se evita el acceso de personas no autorizadas a los datos personales, a tal fin se evita: dejar los datos personales expuestos a terceros (pantallas electrónicas desatendidas, documentos en papel en zonas de acceso público, soportes con datos personales, etc.), esta consideración incluye las pantallas que se utilicen para la visualización de imágenes del sistema de video vigilancia. Cuando se ausente del puesto de trabajo, se procede al bloqueo de la pantalla o al cierre de la sesión.
Los documentos en papel y soportes electrónicos se almacenan en lugar seguro (armarios o estancias de acceso restringido) durante las 24 horas del día.
■ No se desechan documentos o soportes electrónicos (cd, pendrives, discos duros, etc.) con datos personales sin garantizar su destrucción.
■ No se comunican datos personales o cualquier información personal a terceros, se presta atención especial en no divulgar datos personales protegidos durante las consultas telefónicas, correos electrónicos, etc.
■ El deber de secreto y confidencialidad persiste incluso cuando finaliza la relación laboral del trabajador con la empresa.

- DERECHOS DE LOS TITULARES DE LOS DATOS

Se ha informado a todos los trabajadores acerca del procedimiento para atender los derechos de los interesados, definiendo de forma clara los mecanismos por los que pueden ejercerse los derechos (medios electrónicos, referencia al Delegado de Protección de Datos si lo hubiera, dirección postal, etc.) teniendo en cuenta lo siguiente:

Previa presentación de su documento nacional de identidad o pasaporte, los titulares de los datos personales (interesados) podrán ejercer sus derechos de acceso, rectificación, supresión, oposición y portabilidad. El responsable del tratamiento deberá dar respuesta a los interesados sin dilación indebida.

Para el derecho de acceso se facilitará a los interesados la lista de los datos personales de que disponga junto con la finalidad para la que han sido recogidos, la identidad de los destinatarios de los datos, los plazos de conservación, y la identidad del responsable ante el que pueden solicitar la rectificación supresión y oposición al tratamiento de los datos.

Para el derecho de rectificación se procederá a modificar los datos de los interesados que fueran inexactos o incompletos atendiendo a los fines del tratamiento.

Para el derecho de supresión (al olvido) se suprimirán los datos de los interesados cuando los interesados manifiesten su negativa u oposición al consentimiento para el tratamiento de sus datos y no exista deber legal que lo impida.

Para el derecho de portabilidad los interesados deberán comunicar su decisión e informar al responsable, en su caso, sobre la Identidad del nuevo responsable al que facilitar sus datos personales.

MEDIDAS TÉCNICAS

IDENTIFICACIÓN

■ Cuando el mismo ordenador o dispositivo se utiliza para el tratamiento de datos personales y fines de uso personal se dispone de varios perfiles o usuarios distintos para cada una de las finalidades. Se mantienen separados los usos profesional y personal del ordenador.
■ Se dispone de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales.
■ Se garantiza la existencia de contraseñas para el acceso a los datos personales almacenados en sistemas electrónicos. La contraseña tiene al menos 8 caracteres, mezcla de números y tetras.
■ Cuando a los datos personales acceden distintas personas, para cada persona con acceso a los datos personales, se dispone de un usuario y contraseña específicos (identificación inequívoca).
■ Se garantiza la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. En ningún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común y el acceso de personas distintas del usuario.

DEBER DE SALVAGUARDA

A continuación, se exponen las medidas técnicas mínimas para garantizar la salvaguarda de los datos personales:

■ ACTUALIZACIÓN DE ORDENADORES Y DISPOSITIVOS: Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deben mantenerse actualizados en la media posible.
■ MALWARE: En los ordenadores y dispositivos donde se realiza el tratamiento automatizado de los datos personales se dispone de un sistema de antivirus que garantiza en la medida posible el robo y destrucción de la información y datos personales. El sistema de antivirus se actualiza de forma periódica.
■ CORTAFUEGOS O FIREWALL: Para evitar accesos remotos indebidos a los datos personales se vela para garantizar la existencia de un firewall activado en aquellos ordenadores y dispositivos en los que se realiza el almacenamiento y/o tratamiento de datos personales.
■ CIFRADO DE DATOS: Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se deberá valorar la posibilidad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.

■ COPIA DE SEGURIDAD: Periódicamente se realiza una copia de seguridad en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacena en lugar seguro, distinto de aquél en que esté ubicado el ordenador con los ficheros origínales, con el fin de permitir la recuperación de los datos personales en caso de pérdida de la información.

TERCERO: Con fecha 01/02/2019, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado, BALMORE, por la presunta infracción del artículo 32 del RGPD, de conformidad con lo previsto en el artículo 83.2 de la misma norma, considerando que la sanción que pudiera corresponder sería de APERCIBIMIENTO, sin perjuicio de lo que resultara de la instrucción.

CUARTO: Notificado el acuerdo de inicio, BALMORE, al tiempo de la presente resolución no ha presentado escrito de alegaciones.

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran los siguientes,

HECHOS PROBADOS

PRIMERO: El 05/09/2018 la Directora de la Agencia Española de Protección de Datos acordó iniciar de oficio las presentes actuaciones de investigación en relación con la noticia difundida por los medios de comunicación, relacionada con la posibilidad que tendrían los clientes de las tiendas propiedad de BALMORE cuando utilizan los terminales móviles que se encuentran en a su disposición en los expositorios, de acceder a los correos electrónicos remitidos desde estas tiendas que en ocasiones contienen datos personales de empleado y clientes.

SEGUNDO: El 03/09/2018 FACUA CONSUMIDORES EN ACCION, en representación de D. ***A.A.A.***, presentó reclamación contra BALMORE prácticamente por los mismos hechos: brecha de seguridad en la citada empresa permitiendo acceder a datos personales tanto de clientes como de empleados.

TERCERO: BALMORE acredita, en escrito remitido a la AEPD, haber adoptado una serie de medidas resolviendo la quiebra producida en sus sistemas, justificando la adopción de una serie de medidas, entre ellas: eliminando la cuenta de correo instalada en los dispositivos contenidos en los expositorios; inhabilitando el servicio de correo electrónico asignado y adoptando las medidas de carácter organizativo y técnico para evitar incidencias futuras.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en el art. 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), la Directora de la Agencia Española de Protección de Datos es competente para resolver este procedimiento.

II

La disposición transitoria tercera de la LOPDGDD establece: *"Régimen transitorio de los procedimientos:*

1. Los procedimientos ya iniciados a la entrada en vigor de esta ley orgánica se regirán por la normativa anterior, salvo que esta ley orgánica contenga disposiciones más favorables para el interesado."

El artículo 63.2 de la LOPDGDD establece 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."*

III

Se imputa a BALMORE la vulneración del artículo 32 RGPD, *Seguridad del tratamiento*, del RGPD que dispone 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".

BALMORE ha incurrido en infracción de la normativa sobre protección de datos materializado en la existencia de una brecha de seguridad derivada de la defectuosa configuración de una cuenta de correo desde un terminal para uso de gestiones internas de la tienda, provocando que los correos enviados desde dicho terminal estuvieran visibles en los dispositivos expuestos en la tienda cuando los clientes accedían a la aplicación de correo instalada en los terminales móviles.

No obstante, BALMORE contestó al requerimiento de los servicios de inspección de esta Agencia acreditando haber implantado las medidas adecuadas de carácter técnico y organizativo tendentes a impedir que se vuelva a incurrir en hechos como los que trae causa la iniciación del presente procedimiento sancionador.

IV

El artículo 83 del RGPD, *Consideraciones generales para la imposición de multas administrativas,* establece en su apartado 2.d) que:

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;

Y el apartado 4, letra a) señala que:

"4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) *las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;*

(…)

Por su parte, la LOPDGDD en su artículo 73 indica: *"Infracciones consideradas graves:*

"En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

(…)

d) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño, así como la no integración de las garantías necesarias en el

tratamiento, en los términos exigidos por el artículo 25 del Reglamento (UE) 2016/679".

(…)

V

No obstante, sin perjuicio de lo establecido en el artículo 83 del RGPD, el artículo 58.2 del RGPD dispone lo siguiente:

"Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

(…)

b) sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;

(…)

VI

Hay que señalar que tras el requerimiento efectuado a la parte reclamada, BALMORE ha acreditado haber adoptado con una razonable diligencia medidas de carácter técnico y organizativas reforzando la seguridad de los datos y evitar que en el futuro vuelva a producirse una quiebra como la que ha provocado la reclamación que trae causa el presente procedimiento.

De la misma forma, no se insta la adopción de ninguna medida concreta a tomar, ya que se ha acreditado la adopción de medidas entre ellas tal y como figura en los hechos: la eliminación de la cuenta de los expositivos en exposición en las tiendas ; la asignación de un DPD; la inhabilitación del uso de la cuenta de correo; formación a los trabajadores en materia de protección de datos; adopción de medidas de carácter organizativas y técnicas y su adaptación a los nuevos principios que ha supuesto el RGPD.

Para concluir, teniendo en cuenta la ausencia de intencionalidad, la ausencia de daños y perjuicios, el comportamiento y las medidas adoptadas por el responsable del tratamiento atenúan más si cabe su culpabilidad en el presente caso, por lo que procede sancionar con el apercibimiento.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada,

La **Directora de la Agencia Española de Protección de Datos RESUELVE:**

PRIMERO: IMPONER a **BALMORE ATLANTIC, S.L.,** con NIF ***B67035824,*** por una infracción del artículo 32 del RGPD, sancionada conforme a lo dispuesto en el artículo 83.4.a) del citado RGPD y, calificada de grave en el artículo 73.d) de la LOPDGDD, una sanción de **APERCIBIMIENTO** de conformidad con lo previsto en el artículo 58.2.b) del RGPD.

SEGUNDO: NOTIFICAR la presente resolución a **BALMORE ATLANTIC, S.L.,** con NIF ***B67035824*** y, conforme al art. 77.2 del RGPD, **INFORMAR** al reclamante,

FACUA CONSUMIDORES EN ACCION, en representación de D. ***A.A.A.***, sobre el resultado de la reclamación.

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 conforme al art. 114.1 c) de la LPACAP, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, 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.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

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