

- **Expediente N°: E/09214/2020**

### 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: Como consecuencia de la notificación a la División de Innovación Tecnológica de esta Agencia de una brecha de seguridad de datos personales por parte del Responsable del Tratamiento MEDIASET ESPAÑA COMUNICACIÓN S.A con número de registro de entrada O00007128e2000008396 relativa a suplantación de identidad de empleados, se ordena a la Subdirección General de Inspección de Datos que valore la necesidad de realizar las oportunas investigaciones previas con el fin de determinar una posible vulneración de la normativa de protección de datos.

SEGUNDO: 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 los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 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:

#### ANTECEDENTES

Fecha de notificación de la brecha de seguridad de datos personales: 30/10/2020.  
Resumen de la notificación: ataques de seguridad e incidentes en el tratamiento de datos personales sufridos de manera continuada desde agosto de 2020, presuntamente motivados por jaqueo de tercero/s.  
Documentación aportada: No consta documentación adjunta a la notificación de brecha de seguridad a esta AEPD.

#### ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se ha investigado la siguiente entidad:  
MEDIASET ESPAÑA COMUNICACIÓN, S.A. (en adelante, la parte investigada), con NIF A79075438 y domicilio en CRTA. FUENCARRAL A ALCOBENDAS, N° 4 - 28049 MADRID (MADRID).

#### RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Respecto de la cronología de los hechos. Acciones tomadas con objeto de minimizar los efectos adversos y medidas adoptadas para su resolución final:

(...)

- 05/10/2020: (...)
- 08/10/2020: (...)



- 15/10/2020: (...)
- 16/10/2020: (...)
- 17/10/2020: (...)
- (...)
- 19/10/2020: (...)
- 29/10/2020: (...)
- o (...)
- o (...)
- o (...)
- o (...)
- o (...)
- o (...)

(...)

- (...)

(...)

- (...)
- (...)
- (...)
- (...)
- (...)
- (...)
- (...)
- (...)

Respecto de las causas que hicieron posible la brecha:

- (...)
- (...)

Respecto de los datos afectados:

- (...)
- o (...)
- o (...)
- o (...)
- (...)
- (...)
- (...)
- (...)
- (...)
- (...)

(...)

Información sobre la recurrencia de estos hechos y número de eventos análogos acontecidos en el tiempo:

- (...)

Respecto de las medidas de seguridad implantadas con anterioridad a la brecha de seguridad:

(...)

- (...)
- o (...)



- (...)
  - o (...)
  - o (...)
  - o (...)
- (...)
  - (...)
  - (...)
  - (...)
  - (...)

Respecto de las medidas de seguridad de tipo preventivo frente a la posible repetición en el futuro de la brecha 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 artículo 4 apartado 12 del RGPD define, de un modo amplio, las “violaciones de seguridad de los datos personales” (en adelante quiebra 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.”*

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, que regulan tanto 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.



## Artículo 32

### *“Seguridad del tratamiento*

*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”.*

## Artículo 33

*“Notificación de una violación de la seguridad de los datos personales a la autoridad de control*



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”.*

#### **Artículo 34:**

*“Comunicación de una violación de la seguridad de los datos personales al interesado*



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. L 119/52 ES Diario Oficial de la Unión Europea 4.5.2016

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 concrete 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.”

### III

En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como brecha de confidencialidad, ya que personas u organizaciones que no están autorizadas, o no tienen un propósito legítimo para acceder a los datos personales, han podido acceder.

De la documentación aportada por la parte investigada en el curso de estas actuaciones de investigación no se desprende que, con anterioridad a la brecha de seguridad, careciera de medidas de seguridad razonables en función de los posibles riesgos estimados.

Asimismo, no existen evidencias de que no hubiera actuado de forma diligente una vez conocida la brecha de seguridad, ni que las medidas adoptadas con posterioridad al incidente aquí analizado no fueran adecuadas.

Tampoco constan reclamaciones ante esta Agencia por parte de terceros, relacionadas con la presente brecha de seguridad.

Tras el requerimiento de información llevado a cabo por la Inspección de esta AEPD, la parte investigada ha informado de todas las actuaciones llevadas a cabo para paliar el

incidente. Informa, asimismo, de las nuevas medidas implementadas en orden de prevenir posibles ataques futuros.

#### IV

Por lo tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos.

Así pues, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,  
**SE ACUERDA:**

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a MEDIASET ESPAÑA COMUNICACIÓN, S.A. con NIF A79075438

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.

940-010921

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