- **Procedimiento Nº: E/03671/2020**

940-0419

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 2 de enero de 2020, el Delegado de Protección de Datos de PODEMOS presenta notificación de una brecha de seguridad. Indica que, el día 31 de diciembre de 2019, a raíz de una publicación en un medio de comunicación de documentos de carácter personal y financiero de un trabajador de la organización advirtieron el problema. Señala que la brecha está resuelta.

El resumen del incidente es el siguiente: el anterior Delegado de Protección de Datos de Podemos, el sábado 30 de noviembre de 2019, se descargó documentación relativa a 100 trabajadores de la organización. El día 2 de diciembre de 2019, fue cesado y despedido disciplinariamente, entre otros motivos, al constatarse actuaciones no permitidas frente a una compañera, prevaliéndose de su cargo. El acceso a la información es evidenciado por el rastro que dejo el trabajador y localizado por el equipo de informática y ciberseguridad.

Se declara una brecha de tipología confidencialidad (acceso no autorizado), en un contexto interno.

Los sistemas de gestión de datos de carácter personal pueden ser gestionados por trabajadores que, por razón de su cargo, deban usarlos. Pero su uso está restringido a que sean necesarios para la gestión y administración. Los sistemas generan rastros con identificación de personas/ordenadores que son perfectamente identificables y analizables.

Los datos afectados fueron datos básicos; datos de DNI, NIE o pasaporte; y datos económicos y financieros de, aproximadamente, 100 empleados. Las posibles consecuencias son la divulgación a terceros/internet.

Desde el momento de su despido, no tiene acceso a ningún sistema de gestión de datos personales, ni de la organización, ni de militantes ni de trabajadores.

Exponen que se interpondrá denuncia tanto en la vía penal como en el ICAB.

La severidad de la brecha es media, pero se informará de la misma a los afectados el día 8 de enero de 2020.

Por último, indican que no hay ninguna implicación transfronteriza.

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, 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.*"

El artículo 33 del RGPD señala lo siguiente:

"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."

En el presente caso, consta una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una posible brecha de confidencialidad, conocida a raíz de una publicación en un medio de comunicación de documentos de carácter personal y financiero de un trabajador de la organización.

En la propia comunicación se refieren las medidas de seguridad que tienen incorporadas en cuanto a los perfiles de accesos y a los controles realizados. Así se indica que solo los trabajadores que por sus funciones deben acceder a los sistemas de gestión de datos de carácter personal son los autorizados. Y aún estando autorizados, los accesos se han de limitar a que sean necesarios para la gestión y administración.

Los sistemas generan rastros con identificación de personas/ordenadores que son perfectamente identificables y analizables. Los accesos a la información fueron

controlados posteriormente por el equipo de informática y ciberseguridad, verificando quien había accedido a los datos.

El Delegado de Protección de Datos estaba autorizado a esos accesos para el desarrollo de su trabajo. Además, en el momento de acceder a los datos de los trabajadores, continuaba en el desempeño de sus funciones.

De todo lo anterior se desprende que Podemos disponía de razonables medidas técnicas y organizativas preventivas a fin de evitar este tipo de incidencias y acordes con el nivel de riesgo.

Asimismo, Podemos afrontó el incidente ahora analizado, lo que ha permitido de forma diligente la identificación, análisis y clasificación del incidente de seguridad de datos personales, así como la reacción ante la misma al objeto de notificar y minimizar el impacto. A pesar de notificar la brecha como de severidad media, declaran que se van a dirigir a los trabajadores a cuyos datos se accedió el 30 de noviembre de 2019 para comunicar la brecha, conforme a lo dispuesto en el artículo 34.3.c) del RGPD.

No constan reclamaciones ante esta Agencia de personas afectadas.

En consecuencia, Podemos disponía de forma previa de medidas técnicas y organizativas razonables en función del nivel de riesgo para evitar este tipo de incidencia. No obstante, se recomienda la realización de un informe final sobre el incidente notificado. Este Informe es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos y servirá para prevenir la reiteración de una brecha de similares características como la ahora analizada.

Por lo tanto, 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 Podemos.

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-Ad-

ministrativa, 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