



Expediente Nº: E/00959/2018

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad QUIRON PREVENCIÓN, S.L., en virtud de denuncia presentada por Doña **B.B.B.**, y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 14 de febrero de 2018, tuvo entrada en esta Agencia un escrito remitido por Doña **B.B.B.**, en el que expone lo siguiente:

Solicitó documentación al Servicio de Prevención de riesgos de su empresa, porque le hicieron un informe de no apto; la información la necesitaba para el Servicio de Prevención Mancomunada de la Caixa de Riesgos Laborales.

Tras varios correos electrónicos y solicitudes, el citado Servicio de Prevención accedió al envío, que se realizó por correo ordinario en dos ocasiones, sin embargo la documentación no llegó a la denunciante.

Aporta copia de los siguientes correos electrónicos:

Remitido a la denunciante, con fecha 24 de enero de 2018, desde la dirección ***EMAIL.1 (firmado por **A.A.A.**, ***CARGO.1 de Quirón Prevención), en el que se le informa de que, *“Por mi parte se ha enviado por correo ordinario en dos ocasiones y otras dos por mail, no acabo de entender porque no te llegan. Si te parece puedo ofrecerte enviar una copia a mis compañeros del centro de Palma y que la recojas en persona”*.

Contestación de la denunciante al correo anterior, de la misma fecha, con el texto *“De acuerdo **A.A.A.** que me avisen cuando la tengan para recogerla.”*

Remitido por la denunciante, con fecha 25 de enero de 2018 a varias direcciones, entre las que se encuentra la de **A.A.A.**, con el texto *“**A.A.A.**, me preocupa que información confidencial mía se haya perdido dos veces y no sepamos en poder de quién está. La confidencialidad de datos se ve plenamente vulnerada. Tendrías que haberlo enviado por correo certificado”*.

Así mismo, aporta copia del escrito dirigido a la denunciante por la Inspección Provincial de Trabajo y Seguridad Social de Illes Balears, de fecha 14 de diciembre de 2017, en el que le informan de que se han extendido Actas de Infracción a la entidad (CAIXABANK S.A.) por diversos motivos relacionados con la denunciante.

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

QUIRON PREVENCIÓN S.L., ha remitido a esta Agencia, con fecha 26 de marzo de 2013, la siguiente información en relación con los hechos denunciados:



1. Aportan copia impresa de los datos que constan en sus ficheros relativos a la denunciante relativos a su informe de salud, derivado del reconocimiento médico que se le realizó, en materia de prevención, así como las conclusiones médicas que se derivan del reconocimiento. Las medidas de vigilancia y control de la salud se llevaron a efecto por personal sanitario.
2. Respecto al procedimiento establecido por la entidad para el envío de los informes médicos por medios electrónicos, se aplican mecanismos de encriptación, cifrando los datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.
3. Se utiliza un archivo en formato protegido ZIP, que esta a su vez protegido por contraseña, a ambos lados de la comunicación y que se tiene que definir singularmente en cada uno de los archivos que contiene. La contraseña se comunica al destinatario por un canal diferente del correo electrónico.
4. Además, en los envíos realizados a la denunciante, se utilizó el protocolo criptográfico denominado "Transport Layer Security (TSL)", que proporciona una garantía de comunicación segura de envíos electrónicos en la red internet. A este respecto aportan un certificado documental emitido por el departamento de sistemas de la entidad, que especifica técnica y detalladamente el concepto y alcance de este protocolo criptográfico de seguridad.
5. Respecto al procedimiento establecido para la remisión de información que contiene datos médicos, por vía no electrónica, se procede a su envío o bien por mensajería, siempre en sobre cerrado o bien se procede a su entrega al interesado en la sede de la empresa, personalmente y en mano, citando previamente al solicitante.
6. En particular, respecto a los hechos denunciados:
 - a. Con fecha 8 de septiembre de 2017, se procede a realizar el reconocimiento médico a la denunciante y con fecha 3 de octubre de 2017, se emite el correspondiente informe con el resultado de "NO APTO".
 - b. Con fecha 5 de diciembre de 2017, a petición de la interesada, se le remite la información al correo electrónico facilitado por la interesada, utilizando los protocolos de seguridad indicados. La destinataria contesta informando de que no puede acceder a la documentación que se le adjunta, por razones técnicas.
 - c. Con fecha 11 de diciembre de 2017, se remite un correo electrónico a la denunciante informándole de que no se le puede enviar en un formato diferente por los protocolos de seguridad establecidos, ofreciéndole la alternativa de recogerlo personalmente o bien de enviárselo por correo postal.
 - d. Con fecha 19 de diciembre de 2017, la denunciante facilita su dirección y ese mismo día se le remite la documentación por correo postal. Con fecha 28 de diciembre de 2017, el envío se devuelve a la empresa, por el Servicio de Correos, por error en la dirección.
 - e. Con fecha 29 de diciembre de 2018, la denunciante confirma que la dirección es correcta por lo que al día siguiente se procede a realizar un



- nuevo envío postal de la documentación, que también fue devuelto por el Servicio de Correos.
- f. Según manifiestan, los dos envíos fueron devueltos a la empresa, por lo que en ningún momento se produce ninguna pérdida de la documentación.
 - g. Con fecha 23 de enero, la denunciante indica, mediante correo electrónico dirigido a la empresa y a CAIXABANK, que no ha recibido ninguna documentación en el domicilio indicado.
 - h. Con fecha 24 de enero de 2018, se informa a la denunciante de que la documentación ha sido enviada y se le ofrece la opción de poner a su disposición una copia de la documentación solicitada, en el establecimiento de la entidad de Palma de Mallorca, donde ella reside y donde se le realizó el reconocimiento médico.
 - i. La denunciante acepta esta última opción mediante el correo electrónico que remite con fecha 24 de enero de 2018 con el texto *"de acuerdo, que me avisen cuando la tengan para recogerla"*.
 - j. Con fecha 6 de febrero se le informa de que ya dispone de la documentación en el centro de la empresa en Palma de Mallorca, concretándole la dirección de recogida y la persona que se la entregará: el director médico.
 - k. Con fecha 16 de febrero de 2018, se informa por parte de la Dirección Médica de la empresa de que la denunciante ha recogido ya la documentación en el punto de recogida.
7. Aportan copia de los correos electrónicos detallados que se han intercambiado con la denunciante en relación con su solicitud de copia de su documentación médica y de los envíos de la misma, desde el 22 de noviembre de 2017 en el que la denunciante solicita, por esa vía, su expediente médico completo, hasta el 6 de febrero de 2018, en el que le informan de que dispone de toda la documentación en el centro de Palma de Mallorca, en ese periodo se realizan dos envíos de la documentación por correo electrónico, con fechas 5 y 11 de diciembre de 2017, a los que la denunciante contesta manifestando que no puede abrir los archivos que ha recibido.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

El artículo 126.1, apartado segundo, del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RLOPD) establece:

“Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso.”

III

La denuncia se concreta en el extravío que se ha producido de datos de salud de la denunciante al enviárselos la entidad de prevención de riesgos laborales Quirón Prevención.

El artículo 9 de la LOPD dispone lo siguiente:

“1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.”

El transcrito artículo 9 de la LOPD establece el principio de seguridad de los datos, imponiendo al responsable del fichero la obligación de adoptar las medidas de índole técnica y organizativa que garanticen tal seguridad, así como para impedir el acceso no autorizado a los mismos por ningún tercero.

Para poder delimitar cuáles son los accesos que la Ley pretende evitar, exigiendo las pertinentes medidas de seguridad, es preciso acudir a las definiciones de “fichero” y “tratamiento” contenidas en la LOPD.

En lo que respecta al concepto de “fichero” el artículo 3.b) de la LOPD lo define como “todo conjunto organizado de datos de carácter personal”, con independencia de la modalidad de acceso al mismo.

Por su parte el artículo 3.c) de la citada Ley Orgánica considera tratamiento de datos cualquier operación o procedimiento técnico que permita, en lo que se refiere al objeto del presente procedimiento, la “comunicación” o “consulta” de los datos personales tanto si las operaciones o procedimientos de acceso a los datos son automatizados o no.



Sintetizando las previsiones legales citadas puede afirmarse que:

a) Las operaciones y procedimientos técnicos automatizados o no, que permitan el acceso –la comunicación o consulta- de datos personales, es un tratamiento sometido a las exigencias de la LOPD.

b) Los ficheros que contengan un conjunto organizado de datos de carácter personal así como el acceso a los mismos, cualquiera que sea la forma o modalidad en que se produzca, están, también, sujetos a la LOPD.

c) La LOPD impone al responsable del fichero la adopción de medidas de seguridad, regulado en normas reglamentarias.

d) El mantenimiento de ficheros carentes de medidas de seguridad que permitan accesos o tratamientos no autorizados, cualquiera que sea la forma o modalidad de éstos, constituye una infracción del artículo 9 de la LOPD tipificada como grave en el artículo 44.3.h) de la citada Ley.

El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, define en su artículo 5.2 ñ) el “Soporte” como el *“objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos”*.

Por su parte el artículo 81.1 del mismo Reglamento señala que *“Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico”*. Las medidas de seguridad de nivel básico están reguladas en los artículos 89 a 94, las de nivel medio se regulan en los artículos 95 a 100 y las medidas de seguridad de nivel alto se regulan en los artículos 101 a 104.

Las medidas de seguridad se clasifican en atención a la naturaleza de la información tratada, esto es, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la misma. En el caso que nos ocupa, como establece el artículo 81.3.a) del Reglamento de desarrollo de la LOPD, además de las medidas de nivel básico y medio, deberán adoptarse las medidas de nivel alto a los ficheros o tratamientos de datos de carácter personal que se refieran a datos de salud.

Entre estas medidas de nivel alto se encuentra la prevista en el artículo 104 del citado Reglamento, en relación con las medidas de seguridad de nivel alto establece:

“Telecomunicaciones.

Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.”

Esta es la concreta medida de seguridad de las legalmente previstas en la que se hubiera podido incurrir vulnerando el principio de seguridad de los datos.

En las alegaciones presentadas, la entidad de prevención de riesgos laborales presenta un informe sobre el protocolo de seguridad que aplican para garantizar la confidencialidad y seguridad de la información que se trasladó por correo electrónico; comprobando, como se detallaba en los antecedentes que viajaba encriptada.



En este informe, el Servicio de Seguridad comunica que el remitente cifra un mensaje usando una clave y el destinatario lo descifra con la misma clave.

En cuanto a los dos envíos realizados por correo certificado que incluían la información personal solicitada, la dirección a la que se enviaron fue la que la propia denunciante había indicado. Ambos envíos fueron devueltos, por lo que no se ha producido incumplimiento a las medidas de seguridad por parte de Quirón Prevención, S.L.

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a QUIRON PREVENCIÓN, S.L., y a Doña **B.B.B.**

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, 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 del referido texto legal.

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