- Procedimiento Nº: E/05308/2020

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: La reclamación interpuesta por CORPORACIÓN DE RADIO Y TELEVISIÓN ESPAÑOLA S.A. (en adelante, el reclamante) tiene entrada con fecha 14 de noviembre de 2019 en la Agencia Española de Protección de Datos. La reclamación se dirige contra CONSEJERIA DE SANIDAD DE LA COMUNIDAD DE MADRID - SERVICIO MADRILEÑO DE SALUD, con NIF S7800001E (en adelante, el reclamado) y los motivos en que basa la reclamación son, en síntesis, que el reclamado tuvo que dar de alta a su personal sanitario en el sistema SISPAL a fin de poder registrar las vacunas de la gripe de sus trabajadores; que las entidades con acceso al programa no deberían poder visualizar datos de carácter personal reales y sin disociar de trabajadores que no correspondan a la propia entidad, ya que esto vulnera el principio de minimización de datos, integridad y confidencialidad del RGPD, no siendo necesario que se pueda acceder a datos de trabajadores de otras empresas que también van a ser vacunados; que el formulario facilitado por el Sistema Madrileño de Salud les atribuye la condición de encargado del tratamiento de datos de trabajadores que no pertenecen a la corporación y no se encuentra adaptado a la nueva normativa; que hay una ausencia de medidas de seguridad de los datos personales.

SEGUNDO: Tras la recepción de la reclamación, la Subdirección General de Inspección de Datos procedió a realizar las siguientes actuaciones:

El 12/12/2019 fue trasladada al reclamado la reclamación presentada para su análisis y comunicación al reclamante de la decisión adoptada al respecto. Igualmente, se le requería para que en el plazo de un mes remitiera a la Agencia determinada información:

- Copia de las comunicaciones, de la decisión adoptada que haya remitido al reclamante a propósito del traslado de esta reclamación, y acreditación de que el reclamante ha recibido la comunicación de esa decisión.

- Informe sobre las causas que han motivado la incidencia que ha originado la reclamación.

- Informe sobre las medidas adoptadas para evitar que se produzcan incidencias similares.

- Cualquier otra que considere relevante.

El reclamado en fecha 13/01/2020 alegaba: que se solicitó a la DGSP, como responsable del tratamiento de los datos objeto de la presente reclamación, que se llevaran a cabo las investigaciones oportunas con el fin de determinar la concurrencia de los hechos señalados en la reclamación, así como que se informara de las medidas

que se pudiesen haber tomado al respecto; que se han realizado las gestiones necesarias para actualizar el referido formulario a la normativa vigente aplicable y que se trata de un modelo genérico utilizado como base para facilitar la gestión de los distintos accesos que puedan ser requeridos a sistemas de la Consejería de Salud, si bien, dicho modelo puede ser modificado adaptándose a las distintas casuísticas que se presenten en atención a las finalidades, medios, entidades participantes, etc., adecuándose a cada situación en concreto.

En lo referente a la funcionalidad del sistema SISPAL y a la visualización de datos de pacientes a través de dicha aplicación la Dirección General de Salud Pública (DGSP), expone que en el sistema SISPAL se recoge la historia clínica vacunal de los ciudadanos de la Comunidad de Madrid siendo necesario tener registrada, de forma individualizada, toda vacuna que se administre en la Comunidad de Madrid en aplicación de las competencias que dispone la DGSP en materia de salud pública, y en concreto en la elaboración e impulso a los programas de vacunación, tal y como señala la Ley 33/2011, de 4 de octubre, General de Salud Pública en su art. 19.2.c): *"Las Administraciones públicas, en el ámbito de sus respectivas competencias: (...) Impulsarán otras acciones de prevención primaria, como la vacunación, que se complementarán con acciones de prevención secundaria como son los programas de detección precoz de la enfermedad".*

Que el sistema SISPAL cuenta con una serie de medidas dispuestas con el fin de consolidar la seguridad de la información que en ella se registre.

TERCERO: El 05/06/2020, de conformidad con el artículo 65 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por el reclamante contra el reclamado.

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 32 del RGPD, Seguridad del tratamiento, dispone 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".

Hay que señalar que el RGPD no establece un listado de las medidas de seguridad que son de aplicación de acuerdo con los datos que son objeto de tratamiento, sino que establece el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas adecuadas al riesgo que conlleve el tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y finalidades del tratamiento, los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas.

En relación con la última de estas circunstancias, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales: destrucción, pérdida o alteración accidental o ilícita de datos personales, comunicación o acceso no autorizados a dichos datos, y que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales.

Y entre estas medidas se encuentran: la seudonimización y el cifrado, la capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, la capacidad para restaurar la disponibilidad y acceso a datos tras un incidente, proceso de verificación (que no auditoría), evaluación y valoración de la eficacia de las medidas.

En este mismo sentido el considerando 83 del RGPD señala que:

"(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el

cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como 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, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales".

En primer lugar, por lo que se refiere al formulario de Solicitud Masiva para Accesos Externos a Aplicaciones Corporativas según manifiesta el reclamado que se han realizado las gestiones necesarias para actualizar el referido formulario a la normativa vigente aplicable aportando modelo del mismo adaptado al RGPD; se trata de un modelo genérico utilizado como base para facilitar la gestión de los distintos accesos, que puede ser modificado adaptándose a las distintas casuísticas que se presenten en atención a las finalidades, medios, entidades participantes, etc., adecuándose a cada situación en concreto.

En segundo lugar, consta acreditado que el reclamado tiene adoptadas las medidas de seguridad que se consideran adecuadas al permitir el acceso a personal sanitario de forma controlada a la base de datos de vacunas de la CAM para alimentarla desde todos aquellos lugares en los que se administren vacunas: centros de salud, consultorios, hospitales, residencias, etc., y en cuanto al acceso a la misma puede ser universal para todos aquellos usuarios autorizados por los artículos 9.2.h) y 9.3 del RGPD.

La CAM recoge la información sobre las vacunas que se suministran en todo su territorio al ser una de las competencias que le encomienda la ley general de salud pública: la historia clínica vacunal de los ciudadanos de la Comunidad de Madrid que denomina SISPAL.

En lo relativo a las medidas de seguridad adoptadas, en la respuesta remitida a este organismo se aporta informe de la DGSP conteniendo las relativas al sistema haciendo referencia a las mismas:

- La desconexión que se establece con la organización externa a la que se le dé acceso a SISPAL se lleva a cabo a través de una solución de comunicación segura desde puntos remotos hacia la red interna (intranet) de la Consejería de Sanidad de la Comunidad de Madrid y únicamente en aquellos supuestos en los que por razón de su función, sea necesario concederles el acceso en atención a los fines y requisitos definidos por los responsables funcionales de Salud Pública de la Comunidad de Madrid.

- Estos accesos externos a las aplicaciones alojadas en la plataforma de SISPAL, únicamente se confieren a personal sanitario, tanto médicos como enfermeros (por ejemplo en el caso de RTVE únicamente tienen acceso al sistema 3 personas) que además de estar sometidos a deber de confidencialidad y secreto profesional (art. 16 Ley Autonomía del Paciente), firman un acuerdo específico de confidencialidad de acceso a información de la CSCM (recogido en el citado ANEXO II

"Formulario de Solicitud Masiva para Accesos Externos a Aplicaciones Corporativas a Través de SSL actualizado").

- Cada cuenta está asociada a un identificador único, distribuyendo las credenciales de acceso de manera individual y llevando asignado un perfil de conectividad controlada y restringida al conjunto de recursos de la red de la CSCM permitiendo acceder a las funcionalidades estrictamente necesarias para cada perfil.

- Se realiza un registro de actividad de los usuarios, realizando un control de su actividad, almacenando las trazas de accesos a la aplicación de vacunas, controlándose sistemáticamente y auditando los accesos indebidos, en el caso de que se produzcan.

- Las descargas que puede hacer cada profesional con acceso a SISPAL están limitadas únicamente a las personas vacunadas en su servicio sanitario siendo una forma de control para su propio servicio.

- El principio de minimización en el tratamiento de datos está cubierto teniendo en cuenta las medidas descritas en cuanto a la restricción en el acceso a los sistemas, accediendo únicamente un número reducido de personas autorizadas, cuyas trazas se almacenan y se auditan de forma periódica.

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 la CORPORACIÓN DE RADIO Y TELEVISIÓN ESPAÑOLA S.A. y a la CONSEJERIA DE SANIDAD DE LA COMUNIDAD DE MADRID - SERVICIO MADRILEÑO DE SALUD, con NIF S7800001E**.**

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