- **Expediente N.º: EXP202100660**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: Entre el 7 y el 9 de julio de 2021, se han recibido seis reclamaciones ante la Agencia Española de Protección de Datos. Las mismas provienen de particulares y una también de la ASOCIACIÓN DE CONSUMIDORES Y USUARIOS EN ACCIÓN DE MADRID FACUA, y se dirigen contra la CONSEJERÍA DE SANIDAD DE LA COMUNIDAD DE MADRID, con NIF S7800001E. Los motivos en los que basan las reclamaciones son los siguientes:

La ASOCIACIÓN DE CONSUMIDORES Y USUARIOS EN ACCIÓN DE MADRID FACUA, haciéndose eco de informaciones que han aparecido en medios de comunicación, denuncia que el portal habilitado por la Comunidad de Madrid para obtener el Certificado COVID Digital, puesto en marcha el 7 de junio, posibilitaba que cualquier usuario pudiera acceder a datos personales de otro ciudadano, concretamente, si se introducían números de DNI o números NIE de forma aleatoria se podían acceder a datos personales de los titulares de esos documentos de identidad.

Por ello solicita que se inicien cuantas acciones sean precisas para que la Comunidad de Madrid no vuelva a incurrir en hechos de similar naturaleza.

En otra se indica, por un particular que, "*asociado al servicio web empleado para solicitar cita para la vacunación frente a COVID-19 hay un servicio que, sin autenticación ninguna, revela datos con sólo proporcionar números de DNI válidos. Si en la siguiente URL se sustituye el DNI "12345678A" por el DNI válido de un residente en la Comunidad de Madrid, se devuelven resultados en formato JSON indicando datos como: - Apellidos - Nombre - NIF - Fecha de nacimiento - Teléfono(s) de contacto proporcionado(s) a la Comunidad de Madrid - Número de la Seguridad Social – CIPA. La URL es:*
https://portalciudadanoccd[.]sanidadmadrid[.]org/ohgreenpass/citizen_mpi/fhir/Patient/?identifier=NNESP%7C12345678A&_format=json"

Este enlace conduce al portal web de la Consejería de Sanidad que permite la expedición del Certificado COVID Digital

En una reclamación se señala que el día 7 de julio del 2021, por un problema informático que hubo, en el ámbito sanitario quedaron sus datos expuestos. Usó el servicio de autocita de Comunidad de Madrid y el 6 de julio se vacunó de la primera dosis (pfizer) del covid, en el hospital Doce de Octubre. Solicita que sus datos (todos) permanezcan protegidos.

Junto a la reclamación aporta pantallazo de un justificante de cita previa a su nombre, pantallazo de un SMS de confirmación de cita, y un informe de vacunación, No se deduce, ni de la reclamación ni de la documentación aportada, qué datos han quedado expuestos ni de qué manera.

En otra se reseña que "*existe una URL pública de la consejería de sanidad, que permite acceder a mis datos personales por DNI o teléfono (los míos o los de cualquiera). Esto incluye nombre apellidos, fecha de nacimiento, teléfono, dirección, coordenadas de la dirección, nombre de mis hijos, de mi mujer, su fecha de nacimiento, su teléfono...*
https://portalciudadanoccd.sanidadmadrid.org/ohgreenpass/citizen_mpi/fhir/Patient/?identifier=NNESP%7C12345678A&_format=json
https://portalciudadanoccd.sanidadmadrid.org/ohgreenpass/citizen_mpi/fhir/Patient/?telecom=666666666&_format=json
Reclamo su retirada, y posiblemente la obligación para la CAM de informar a todos los afectados, en caso de que esto sea una brecha de datos que así lo requiera"

En otras se hacen eco de las noticias publicadas en prensa o televisión sobre estos hechos, como la noticia de "el diario" con titular " Un fallo en la web de la Sanidad de Madrid deja al descubierto los datos del rey, Pedro Sánchez o Aznar", https://www.eldiario.es/tecnologia/fallo-web-sanidad-madrid-deja-descubierto-datos-rey-miles-personas_1_8114359.html., manifestando asimismo su preocupación *por las brechas de seguridad que están ocurriendo en las últimas semanas en los servidores de la Consejería de Sanidad de la Comunidad, que están exponiendo de forma abierta datos personales muy sensibles de todos los madrileños (DNI, domicilio, números de teléfono,...) y datos bajo alta protección relacionados con la salud (datos sobre vacunación, anotaciones de profesionales sanitarios,...),* solicitando de la Agencia Española de Protección de Datos que se investiguen los mismos.

SEGUNDO: Con fecha 9 de julio de 2021, la DIRECCIÓN GENERAL DE SALUD PÚBLICA de la CONSEJERÍA DE SANIDAD DE LA COMUNIDAD DE MADRID con NIF S7800001E, presentó, a través de su Comité de Delegado de Protección de Datos, notificación de brecha de seguridad indicando lo siguiente:

Fecha detección de la brecha: el 07/07/2021 a las 17: 42.
Fecha de inicio de la brecha: 07/07/2021.
Brecha resuelta.
Encargado del tratamiento: INDRA SOLUCIONES TECNOLOGICAS DE LA INFORMACIÓN SLU., con NIF B88018098 (en adelante INDRA)

(…)

Desconocen, en ese momento, el número de afectados y el perfil son personas vacunadas contra el COVID y que dispongan del certificado digital.

Los afectados serán informados a través de la prensa o de la web.

TERCERO: Como consecuencia de la notificación de la brecha de seguridad referida, con fecha 19 de julio de 2021 se ordena por la Directora 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.

CUARTO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de dichas reclamaciones a la CONSEJERÍA, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue recogido en fecha 31 de agosto de 2021 como consta en el acuse de recibo que obra en el expediente.

Con fecha 21 de septiembre de 2021 se recibe en esta Agencia escrito de respuesta del Comité de DPD del organismo responsable del tratamiento, solicitando que, de conformidad con el artículo 57 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se acumule el procedimiento relativo a las actuaciones de traslado y admisión (EXP202100624) al procedimiento de actuaciones de investigación (EXP202100660), por ser coincidentes los hechos sobre los que se fundamentan, habiendo recibido sendos requerimientos de información de esta Agencia en el marco de los dos expedientes y que versan ambos sobre la brecha de seguridad producida en el portal web del ciudadano para la obtención del Certificado COVID Digital de la Unión Europea.

QUINTO: Con fecha 22 de septiembre de 2021, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por los reclamantes.

SEXTO: 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 las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 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:

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se han investigado las siguientes entidades:
CONSEJERÍA DE SANIDAD de la Comunidad de Madrid con NIF S7800001E con domicilio en C/ MELCHOR FERNÁNDEZ ALMAGRO, Nº 1 - 28029 MADRID (MADRID)
DIRECCION GENERAL DE SALUD PÚBLICA de la entonces Viceconsejería de Salud Pública y Plan Covid-19 y actualmente Viceconsejería de Asistencia Sanitaria y Salud Pública de la Consejería de Sanidad de la Comunidad de Madrid, con NIF S7800001E.

Algunas de las noticias publicadas con relación a este caso son:

https://www.elespanol.com/espana/madrid/20210707/brecha-seguridad-desvela-madrilenos-rey-sanchez-casado/594692060_0.html
https://www.elespanol.com/espana/20210712/madrid-sigue-sin-obtener-certificado-covid-semana/595941729_0.html
https://www.eldiario.es/tecnologia/fallo -web-sanidad-madrid-deja-descubierto-datos-rey-miles-personas_1_8114359.html
https://www.telemadrid.es/programas/telenoticias-2/brecha-seguridad-datos-privados-madrid-0-2357164308--20210707083051.html

En la noticia de El Español, de 7 julio de 2021, se menciona que *"El portal de la Comunidad de Madrid para conseguir el certificado Covid digital permitía a cualquier usuario acceder a datos personales de miles de ciudadanos debido a un fallo de seguridad". "El error dejaba introducir el DNI de cualquier persona, entre ellos el del Rey Felipe VI, el de Pedro Sánchez o el de Pablo Casado, y conseguir sus datos personales, como la dirección o los números de teléfono"*

En mismo medio, el 14 de julio de 2021, publica otra noticia donde se menciona que en esa fecha la web en cuestión sigue inoperativa. Indican que *"Fuentes oficiales afirman que "se están terminando de implantar los filtros de seguridad tras la última actualización del sistema que se hizo el pasado miércoles y tras los accesos indebidos que se produjeron esa tarde. Estará operativa de nuevo en breve".*

En la noticia de El Diario, de fecha 07/07/2021, se cita que *"La Comunidad de Madrid tumba el portal del certificado COVID, donde un error revelaba el nombre, teléfono y dirección de cualquier ciudadano introduciendo su DNI en la url "…"La Comunidad de Madrid ha reconocido la existencia de la brecha y bloqueado el acceso al portal del certificado COVID durante la tarde de este miércoles. Fuentes de la Consejería de Sanidad han explicado a elDiario.es que "la incidencia ha venido ocasionada por la subida de una actualización que pasó los protocolos de pruebas y que en el proceso de puesta en marcha generó una brecha"…"Esa brecha, aseguran las mismas fuentes, "ha quedado solventada en horas tras ser detectada por los servicios de calidad". No obstante, elDiario.es tiene constancia de que la Comunidad de Madrid fue avisada por expertos en ciberseguridad de la peligrosa situación que estaba provocando su sistema del certificado COVID. Fuentes del sector habían informado de la presencia del fallo a el Diario.es, que se encontraba revisando su alcance cuando la Comunidad tumbó todo el sistema como medida de seguridad".* La noticia incluye una impresión de pantalla que lo que parece formato JSON (formato determinado de intercambio de datos que utiliza texto legible, y que facilita el análisis de los datos con determinadas herramientas) que muestra el nombre y apellidos del Rey de España.

En la noticia de Telemadrid se menciona que *"se podía acceder a los datos al menos hasta la tarde de este miércoles 7 de julio".* En esta noticia se incluyen impresiones de pantalla de los datos supuestamente accesibles, también en formato JSON antes citado, apreciándose las siguientes tipologías de datos: nombre y apellidos, números de teléfono móvil, fechas de nacimiento, objeto de vacuna (SARS-COV-2), marca de la vacuna y brazo donde se inocula. Se aprecian otros campos en los que aparecen los textos "Mayor vulnerabilidad" "Grupo de Riesgo para COVID-19 por…"

Casi todos los datos se encuentran tachados para evitar su visualización completa y la identificación de las personas. En esta noticia informan que para acceder a los datos

se necesita disponer de un programa proxy, algunos de los cuales son gratuitos y de fácil descarga a través internet. Indican que así, simplemente con meter un DNI aleatorio, se podía obtener mucha información de cualquier ciudadano residente en Madrid, como nombre y apellidos, número de teléfono, número de Seguridad Social o sus direcciones y que también es reconocible un identificador interno que queda expuesto con el cual se puede obtener donde y cuando ha sido vacunado, en que brazo y el nombre del sanitario que se la ha administrado.

Se ha solicitado información y documentación a la reclamada, y de la respuesta recibida se desprende lo siguiente:

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

Fecha detección de la brecha: Exacta 07/07/2021 a las 17:42.
Fecha de inicio de la brecha: 07/07/2021.
Fecha de resolución estimada/exacta: 07/07/2021, a las 18:32

(…)

Respecto de las causas que hicieron posible la brecha

(…)

Respecto de los datos afectados

(…)

Posibles consecuencias para los afectados.

(…)

Respecto de la notificación a los afectados, los representantes de la reclamada han manifestado lo siguiente:

(…)

Respecto del encargo de tratamiento

(…)

Respecto al Responsable del Tratamiento y la firma del contrato de servicios con INDRA

(…)

SÉPTIMO: Con fecha 15 de julio de 2022**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la CONSEJERÍA DE

SANIDAD, DIRECCIÓN GENERAL DE SALUD PÚBLICA (en adelante la CONSEJERÍA), con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), por la presunta infracción del Artículo 5.1.f) del RGPD y Artículo 32 del RGPD, tipificadas respectivamente en el Artículo 83.4 del RGPD y Artículo 83.5 del RGPD.

OCTAVO: Notificado el citado acuerdo de inicio conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), la CONSEJERÍA presentó escrito de alegaciones en el que, en síntesis, manifiesta que:

Primera. - Debe tenerse en consideración que en la Consejería de Sanidad de la Comunidad de Madrid se cuenta actualmente con un número elevado de tratamientos de datos personales (más de 500 tratamientos declarados) que da cobertura a más de 6 millones de habitantes, entre los que se tratan datos de categoría especial, como son los datos de salud, a través de más de 700 sistemas de información que se utilizan por las distintas unidades que presenten el servicio sanitario a los ciudadanos de la Comunidad de Madrid.

Como puede observarse el servicio esencial que se presta desde la Consejería de Sanidad de la Comunidad de Madrid conlleva una gestión compleja que abarca a varios responsables y debe tenerse en consideración que los hechos ocurridos reflejan un porcentaje ínfimo en relación a todas las operaciones que se realizan por la CSCM a diario.

Adicionalmente, como se reflejaba en la información ya proporcionada, para la fecha en la que se produjo el incidente se estima que estos requisitos los cumplían alrededor de 4 millones de ciudadanos.

Y que efectivamente no se accedió al total de la información de los referidos 4 millones de ciudadanos, puesto que el número de intentos de acceso no legítimos recibidos durante la brecha fueron 12.862 solicitudes de acceso a datos demográficos.

Así pues, teniendo en cuenta los millones de certificados Covid emitidos en la Comunidad, únicamente se han podido constatar 3 intentos de acceso a datos relacionados a la vacuna durante el periodo de afectación. Teniendo en cuenta adicionalmente que, como indicábamos, para poder acceder a la información de un ciudadano el número de DNI utilizado debía coincidir con el DNI de uno de los ciudadanos de la Comunidad de Madrid que en ese momento se encontrase en la base de datos del sistema, lo cual es un hecho muy poco probable.

Segunda. - Por otro lado, debe tenerse en cuenta igualmente que, el momento en el que ocurrieron los hechos descritos, nos encontrábamos en los puntos más críticos de la pandemia en la que acababa de iniciarse el proceso de vacunación y se buscaba llegar y proporcionar la información necesaria a los ciudadanos con la mayor brevedad posible.

Este estado de emergencia sanitaria provocó que resultase necesario desarrollar un gran número de nuevas herramientas con gran celeridad para poder prestar el mejor

servicio a los ciudadanos y poder superar el estado de pandemia provocado por el COVID19 lo antes posible.

Tercera. - Los ciberataques se han vuelto cada vez más sofisticados, ya que la tecnología evoluciona, constantemente, y los ciberdelincuentes buscan nuevas formas y métodos de penetrar en los sistemas, elaborar malware más complejos y novedosos, etc.

En atención a lo expuesto, se han establecido medidas para la mejora continua de la gestión de las crisis y ciberincidencias, centradas en la prevención, detección y respuesta a incidentes de seguridad. En concreto, se han implementado las siguientes medidas destinadas a reforzar la seguridad:

(…)

Por lo anteriormente expuesto, solicita que se proceda a la resolución de archivo del procedimiento iniciado, dado que se trata de unos hechos ocurridos en condiciones excepcionales de emergencia sanitaria, donde se primaba especialmente la salud del conjunto de la población, y se han adoptado medidas para que no vuelvan a suceder.

NOVENO: Con fecha 13 de febrero de 2023, se formuló propuesta de resolución, en la que se propone que por la Directora se imponga a CONSEJERÍA DE SANIDAD DE LA COMUNIDAD DE MADRID, DIRECCIÓN GENERAL DE SALUD PÚBLICA, con NIF S7800001E:

- por una infracción del Artículo 5.1.f) del RGPD, tipificada en el Artículo 83.5 del RGPD, una sanción de APERCIBIMIENTO.

- por una infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD, una sanción de APERCIBIMIENTO.

Esta propuesta de resolución, que se notificó a CONSEJERÍA conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), fue recogida en fecha 14 de febrero de 2023, como consta en el acuse de recibo que obra en el expediente.

No consta la presentación de alegaciones a la propuesta de resolución.

De las actuaciones practicadas en el presente procedimiento y de la documentación obrante en el expediente, han quedado acreditados los siguientes:

HECHOS PROBADOS

PRIMERO: Con fecha 07/06/2021, la CONSEJERIA activó un sistema vía web para que los ciudadanos pudieran obtener el Certificado Covid Digital.

SEGUNDO: Consta acreditado que por un fallo en dicho sistema se permitía el acceso ilegítimo a datos personales (entre ellos de salud) al introducir números de DNI, debido a un error en el procedimiento de validación de usuarios.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina 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."

II
Cuestiones previas

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que la CONSEJERÍA realiza, entre otros tratamientos, la recogida, registro, organización, estructuración, conservación, utilización, acceso de los siguientes datos personales de personas físicas, tales como: nombre, número de identificación, datos de contacto, datos de salud, etc.

La CONSEJERÍA, realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del artículo 4.7 del RGPD.

El artículo 4 apartado 12 del RGPD define, de un modo amplio, las “violaciones de seguridad de los datos personales” (en adelante brecha 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.”

En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad al haberse producido un acceso indebido por terceros no autorizados a datos personales debido a un error en la verificación de la autenticación de acceso al portal web del ciudadano relativo al Certificado Digital COVID de la Unión Europea, que permitía dicho acceso.

Hay que señalar que la identificación de una brecha de seguridad no implica la imposición de una sanción de forma directa por esta Agencia, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

Dentro de los principios del tratamiento previstos en el artículo 5 del RGPD, la integridad y confidencialidad de los datos personales se garantiza en el apartado 1.f) del artículo 5 del RGPD. Por su parte, la seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que reglamentan 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, respectivamente.

III
Alegaciones aducidas

En respuesta a las alegaciones presentadas por la CONSEJERÍA al Acuerdo de Inicio, se señala lo siguiente:

Primero.- Alega la CONSEJERÍA que debe tenerse en consideración que cuenta actualmente con un número elevado de tratamientos de datos personales (más de 500), dando cobertura a más de 6 millones de habitantes, entre los que se tratan datos de categoría especial, como son los de salud, a través de más de 700 sistemas de información utilizados y que los hechos ocurridos reflejan un porcentaje ínfimo en relación a todas las operaciones que se realizan por la CONSEJERÍA a diario, ***(…).***

A este respecto, procede señalar que no procede admitir tales consideraciones como atenuante o como circunstancia que disminuya la gravedad de los hechos, más bien al contrario, pues precisamente por el elevado número de tratamientos que realiza y por afectar a datos de salud, la CONSEJERÍA está obligada a actuar con la especial diligencia que debe exigirse a un organismo de estas características, que realiza numerosos tratamientos de datos personales de forma masiva, entre ellos categorías especiales de datos.

Procede recordar la Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006), que respecto de entidades cuya actividad lleva aparejado el continuo tratamiento de datos de clientes, indica "…*el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las previsiones legales al respecto"*

Segundo. – Aduce la CONSEJERÍA que en el momento de los hechos se encontraba en los puntos más críticos de la pandemia y que, dado el estado de emergencia sanitaria resultó necesario desarrollar un gran número de nuevas herramientas con gran celeridad.

Frente a ello, además de lo señalado en el apartado anterior, relativo a la especial diligencia que le es exigible precisamente a la CONSEJERÍA por el tratamiento de datos personales que realiza, debe recordarse que, tanto el artículo 5.1.f del RGPD como el 32 del mismo texto legal, inciden en la necesidad de que el responsable del tratamiento adopte medidas técnicas y organizativas apropiadas para aplicar de forma efectiva los principios de protección de datos y garantizar un nivel de seguridad adecuado al riesgo, sin que pueda aceptarse como eximente la circunstancia de premura alegada por emergencia sanitaria.

No cabe por tanto, apreciar en el presente caso estado de necesidad que justifique la puesta en producción de una aplicación de forma defectuosa o con errores, que permita el acceso ilegítimo a datos personales -entre ellos, de salud- de un elevado número de ciudadanos, sin realizar previamente las comprobaciones necesarias para determinar su correcto funcionamiento, en especial, el cumplimiento de todas las obligaciones impuestas por el RGPD y demás normativa de aplicación, y cuyo uso precipitado puede ocasionar un mal mayor que aquel que se pretende evitar.

Tercero. – Alega la CONSEJERÍA que los ciberataques se han vuelto cada vez más sofisticados, buscando los ciberdelincuentes nuevas formas y métodos de penetrar en los sistemas, elaborar malware más complejos y novedoso, etc, y que por ello han establecido las medidas que indica en su escrito de alegaciones para reforzar la seguridad.

A este respecto, debe recordarse que la vulnerabilidad detectada y aprovechada por terceros para acceder a datos personales de forma ilegítima no se debió tanto a un ataque sofisticado, sino más bien a una negligencia ***(…)***, y que la CONSEJERÍA lo justifica argumentando que fue debido a un error humano y a consecuencia de razones de extrema urgencia y necesidad.

No obstante, esta Agencia valora positivamente la adopción de nuevas medidas que redunden en una mayor seguridad en lo que al tratamiento de datos personales se refiere y que ayuden a prevenir, en un futuro, incidentes como el que se sustancia en el presente procedimiento.

Por todo lo expuesto, se desestiman las alegaciones aducidas.

IV
Artículo 5.1.f) del RGPD

El artículo 5.1.f) "*Principios relativos al tratamiento*" del RGPD establece:

"*1. Los datos personales serán:*
(…)

> *f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).*"

El principio de seguridad de los datos requiere la aplicación de medidas técnicas u organizativas apropiadas que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, tratamiento o acceso no autorizado o ilícito. En este sentido, las medidas de seguridad son claves a la hora de garantizar el derecho fundamental a la protección de datos. No es posible la existencia del derecho fundamental a la protección de datos si no se garantizan la confidencialidad, la integridad y la disponibilidad de los mismos.

De ahí que la seguridad y la confidencialidad de los datos personales se consideren esenciales para evitar que los interesados sufran efectos negativos. Por ello, deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, especialmente para impedir el acceso o uso no autorizados de dichos datos y del equipo o sistema utilizados en el tratamiento.

En definitiva, es el responsable del tratamiento el que tiene la obligación de integrar las garantías necesarias en el tratamiento, con la finalidad de, en virtud del principio de responsabilidad proactiva, cumplir y ser capaz de demostrar el cumplimiento, al mismo tiempo que respeta el derecho fundamental a la protección de datos.

En el presente caso, se ha vulnerado el principio de confidencialidad pues ha quedado acreditado que se produjeron accesos indebidos por terceros no autorizados a datos personales de ciudadanos en la aplicación Web de la CONSEJERÍA para la obtención del Certificado Digital Covid, debido todo ello a un error en el proceso de autenticación del usuario. Se pudo acceder, entre otros, a datos tales como Nombre y apellidos, NIF, fecha de nacimiento, teléfono(s) de contacto, CIPA y datos relacionados con la administración de la vacuna para la Covid. La CONSEJERÍA justifica el incidente en un error humano y a consecuencia de razones de extrema urgencia y necesidad.

Ello supone una vulneración de la obligación de garantizar la confidencialidad de los datos, poniendo de manifiesto un incumplimiento de la obligación de tratarlos de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito.

Por todo lo expuesto y de conformidad con las evidencias de las que se dispone se considera que los hechos conocidos son constitutivos de una infracción, imputable a la CONSEJERÍA, por vulneración del artículo 5.1.f) del RGPD.

V

Tipificación de la infracción del artículo 5.1.f) del RGPD

De confirmarse, la citada infracción del artículo 5.1.f) del RGPD podría suponer la comisión de las infracciones tipificadas en el artículo 83.5 del RGPD que bajo la rúbrica "*Condiciones generales para la imposición de multas administrativas*" dispone:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9; (…)"

A este respecto, la LOPDGDD, en su artículo 71 "*Infracciones*" establece que *"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica*".

A efectos del plazo de prescripción, el artículo 72 "*Infracciones consideradas muy graves*" de la LOPDGDD indica:

"1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679. (…)"

VI
Sanción por la infracción del artículo 5.1.f) del RGPD

Sin perjuicio de lo dispuesto en el artículo 83.5 del RGPD, el citado artículo dispone en su apartado 7 lo siguiente:

"7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro".

Por su parte, el artículo 77 "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*" de la LOPDGDD dispone lo siguiente:

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.
(…)

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar

serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.
Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo. (…)"

Por tanto, confirmada la citada infracción del artículo 5.1.f) del RGPD, corresponde sancionar con APERCIBIMIENTO a la CONSEJERÍA.

VII
Artículo 32 del RGPD

El Artículo 32 "*Seguridad del tratamiento*" del RGPD establece:

"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".

El artículo 32 no establece medidas de seguridad estáticas, sino que corresponderá al responsable determinar aquellas medidas de seguridad que son necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales, por lo tanto, un mismo tratamiento de datos puede implicar medidas de seguridad distintas en función de las especificidades concretas en las que tiene lugar dicho tratamiento de datos.

En consonancia con estas previsiones, el Considerando 75 del RGPD establece: Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados.

Asimismo, el Considerando 83 del RGPD establece: 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 definitiva, el primer paso para determinar las medidas de seguridad será la evaluación del riesgo. Una vez evaluado será necesario determinar las medidas de seguridad encaminadas para reducir o eliminar los riesgos para el tratamiento de los datos.

El principio de seguridad de los datos requiere la aplicación de medidas técnicas u organizativas apropiadas en el tratamiento de los datos personales para proteger dichos datos contra el acceso, uso, modificación, difusión, pérdida, destrucción o daño accidental, no autorizado o ilícito. En este sentido, las medidas de seguridad son claves a la hora de garantizar el derecho fundamental a la protección de datos. No es posible la existencia del derecho fundamental a la protección de datos si no es posible garantizar la confidencialidad, la integridad y la disponibilidad de estos.

No debe olvidarse que, de conformidad con el artículo 32.1 del RGPD, las medidas técnicas y organizativas a aplicar para garantizar un nivel de seguridad adecuado al riesgo deben tener en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

En este sentido, procede señalar que la actividad de la CONSEJERÍA conlleva el tratamiento de datos personales de miles de ciudadanos, incluidos datos de salud (categoría especial de datos).

Por ello, derivado de la actividad a la que se dedica y de los datos personales que trata, está obligada realizar un análisis de los riesgos y una implantación de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo de su actividad para los derechos y libertades de las personas, teniendo en cuenta especialmente que su actividad conlleva tratar datos de salud.

(…)

En este sentido, procede recordar que el responsable está obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas. (Considerando 74)

Por tanto, de todo lo anterior se deduce una falta de la debida diligencia tanto en el cumplimiento de las medidas de seguridad adecuadas al riesgo del tratamiento, así como en la supervisión o comprobación de su observancia y de la idoneidad de las mismas.

De conformidad con las evidencias de las que se dispone, se considera que los hechos conocidos son constitutivos de una infracción, imputable a la CONSEJERÍA, por vulneración del artículo 32 del RGPD.

VIII

Tipificación de la infracción del artículo 32 del RGPD

De confirmarse, la citada infracción del artículo 32 del RGPD podría suponer la comisión de las infracciones tipificadas en el artículo 83.4 del RGPD que bajo la rúbrica **"***Condiciones generales para la imposición de multas administrativas*" dispone:

"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; (…)"

A este respecto, la LOPDGDD, en su artículo 71 "*Infracciones*" establece que: "*Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica*".

A efectos del plazo de prescripción, el artículo 73 *"Infracciones consideradas graves*" de la LOPDGDD indica:

"*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:*

f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.

IX

Sanción por la infracción del artículo 32 del RGPD

Sin perjuicio de lo dispuesto en el artículo 83.5 del RGPD, el citado artículo dispone en su apartado 7 lo siguiente:

"7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro".

Por su parte, el artículo 77 "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*" de la LOPDGDD dispone lo siguiente:

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

a) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará

resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.
(…)

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.
Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo. (…)"

Por tanto, confirmada la citada infracción del artículo 32 del RGPD, corresponde sancionar con APERCIBIMIENTO a la CONSEJERÍA.

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 CONSEJERÍA DE SANIDAD DE LA COMUNIDAD DE MADRID, DIRECCIÓN GENERAL DE SALUD PÚBLICA, con NIF S7800001E, por una infracción del Artículo 5.1.f) del RGPD, tipificada en el Artículo 83.5 del RGPD, una sanción de APERCIBIMIENTO.

SEGUNDO: IMPONER a CONSEJERÍA DE SANIDAD DE LA COMUNIDAD DE MADRID, DIRECCIÓN GENERAL DE SALUD PÚBLICA, con NIF S7800001E, por una infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD, una sanción de APERCIBIMIENTO.

TERCERO: NOTIFICAR la presente resolución a CONSEJERÍA DE SANIDAD DE LA COMUNIDAD DE MADRID, DIRECCIÓN GENERAL DE SALUD PÚBLICA, con NIF S7800001E

CUARTO: COMUNICAR la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

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. 48.6 de la LOPDGDD, 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.

938-181022

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