- **Expediente N.º: EXP202414199**

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 Agencia Española de Protección de Datos ha tenido conocimiento a través de diligencia de que el **INSTITUTO BIOTECNOLÓGICO EN MEDICINA INTEGRATIVA Y TERAPIAS AVANZADAS P&G, S.L.** con NIF ***B93656536*** (en adelante, el Instituto), podría haber vulnerado la normativa de protección de datos al haber accedido personal no sanitario a sus bases de datos que contienen la documentación clínica de los pacientes (diagnóstico, tratamiento y solicitudes de análisis proteómico). La información conocida hace referencia a 1.434 accesos a las bases de datos del Instituto entre los días 30/04/2019 y 17/05/2024.

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 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:

El Instituto es una empresa creada en Málaga en 2018 que presta servicios de análisis proteómicos de perfiles moleculares que participan en la fisiopatología de enfermedades neoplásicas, autoinmunes, neurodegenerativas, inflamatorias e infecciosas y también de prevención y test celulares, dentro del campo de colaboración con distintos Hospitales, Laboratorios, Universidades, entidades públicas y privadas tanto de carácter nacional como internacional. Aportan copia de diversos acuerdos de colaboración y de investigación con diversas entidades.

Manifiestan que toda la actividad desarrollada por la entidad se centra exclusivamente dentro del campo de análisis proteómico en tanto las entidades colaboradoras ceden las muestras para su análisis y la entidad brinda el perfil molecular del paciente, y que el trabajo se centra en el análisis y estudio realizado de la muestra, recalcando además que dicho estudio e investigación ha sido y es objeto de distintos premios al ser precursora en la investigación, pero en ningún caso realizan diagnósticos a pacientes, ni realizan medicamentos, y que la entidad lleva a cabo su actividad exclusivamente en el análisis de la muestra y envío del resultado al facultativo, entidad o laboratorio, siendo el facultativo o laboratorio quien lleva todos los controles preceptivos de consentimiento informado y protección de datos previos respecto a sus pacientes, que la entidad desconoce.

Cuentan con la autorización del Comité de Ética de la Investigación con medicamentos. Aportan copia de certificado emitido por el Comité de Ética de la Investigación con Medicamentos Provincial de Málaga, de la Consejería de Salud y Consumo de la Junta de Andalucía, como DOC Nº 10.

En cuanto al número de empleados de la entidad, manifiesta el Instituto que, aparte del bioquímico fundador y representante legal, cuenta con cuatro empleados: un Inmunólogo y responsable facultativo, un bioquímico, una biotecnóloga y un técnico. Aportan copia del organigrama de la plantilla como DOC Nº 11.

En cuanto al acceso a la aplicación por parte de su personal no sanitario, manifiesta el Instituto que colabora con clínicas y médicos sin tener contacto directo con el paciente. El procedimiento se inicia con petición en soporte papel con nombre, apellidos, edad y el diagnóstico o hipótesis de diagnóstico del paciente, así como la clínica o médico que solicita la analítica. Una vez recibida se procede a eliminar el soporte papel de la petición se elimina mediante una destructora de papel y se procede a automatizar los datos.

La automatización se lleva a cabo, en un PC con contraseña, mediante la introducción de los datos en un Excel cifrado, donde se cambia la contraseña con una frecuencia de seis meses y en el que se introducen los mismos datos aportados con anterioridad más un código identificativo de entrada requerido a efectos administrativos para la emisión de una factura. En este Excel se encuentran pseudonimizados todos los titulares de las muestras que se han llevado a cabo.

Solo tres de los empleados pueden acceder al Excel cifrado, siendo la contraseña desconocida para los que no lo necesitan por sus funciones. Cada uno de los empleados dispone de un usuario con contraseña, y según el cargo que tengan dentro de la empresa pueden acceder a determinados documentos por carpetas, garantizando la seguridad y confidencialidad de los datos. En las muestras biológicas que recibe la entidad no se maneja ADN, ya que sólo se trabaja únicamente con plasma.

En octubre de 2024 se ha contratado a una empresa especializada en la protección de datos, quienes están ayudando a establecer los protocolos necesarios y el software adecuado a sus tratamientos; también se ha comunicado el Delegado de Protección de Datos a la AEPD.

En cuanto al procedimiento de la entrega de los resultados a los pacientes o clínicas solicitantes, una vez analizada la muestra, se procede a enviar los resultados a la clínica o médico correspondiente, introduciéndolo manualmente en las plataformas de gestión de cada requirente, con las claves que estos aportan.

Si el centro requirente no tiene plataforma, se procede a la entrega de los resultados, bien directamente al médico y a la clínica, o exclusivamente al médico. La entrega de los resultados se hace vía mail, en el que se adjunta un documento con el nombre, apellido, el número de identificador y una tabla que contiene parámetros y factores de riesgo que se observan en la investigación. Estos documentos van cifrados, procediéndose a comunicar por whatsapp o por vía telefónica la contraseña del documento. Se indica por una vía distinta al mail para garantizar una mayor seguridad.

Estos informes médicos son enviados exclusivamente por la Dirección del Instituto.

En cuanto a la responsabilidad del tratamiento de datos personales efectuado por el personal no sanitario, en primer lugar, todos los empleados han firmado el documento de compromiso de confidencialidad; en segundo lugar, la Dirección ha procedido a elaborar perfiles al resto de empleados que limita el acceso a los contenidos en función del puesto que ocupa cada uno.

Cada uno de los empleados tiene un usuario de acceso con contraseña, estando cifradas las carpetas con datos personales, evitando así una pérdida de confidencialidad de los datos. Se trata de personal no estrictamente sanitario pero cualificado y especializado en los estudios biomédicos (bioquímico, biotecnóloga, etc.). Además durante el proceso de estudios y generación de resultados de las muestras, resulta imprescindible el trabajo en equipo en la misma sala de las 4 trabajadores implicados.

Como DOC nº15 se aportan el compromiso de confidencialidad y Protección de datos firmados por el bioquímico, la biotecnóloga y el técnico, dos de ellos con fecha 6 de noviembre de 2024 y el tercero el 4 de diciembre de 2024, especificándose en ello las responsabilidades en caso de incumplimiento.

En cuanto al Análisis de Riesgo elaborado sobre los tratamientos de datos de salud, disponen de un Registro de Actividades, un Procedimiento de atención al Ejercicio de Derechos, otro de gestión de Brechas de Seguridad, y unos listados con Plazos de conservación de documentos, que ponen a disposición de la AEPD si fuese necesario.

Aportan como DOC nº 13 el análisis de Riesgo y EIPD, de fecha 14/10/2024. En el documento se define el Riesgo Inherente como la probabilidad por el impacto, valorándose entre 1 y 4 la probabilidad, e igualmente entre 1 y 4 el impacto. Se identifica como máximo (4x4 igual a 16) el Riesgo Inherente en la “gestión y control sanitario, historial clínico”.

Se realiza en el documento un análisis de los riesgos en los que se identifican especialmente, riesgos asociados a los accesos no autorizados a datos personales, con sus soluciones pertinentes, proponiendo una serie de medidas, relacionadas, en especial, con el control de acceso.

Concluye el documento *que “Las medidas correctoras propuestas son suficientes para reducir el riesgo inherente a un riesgo residual aceptable. El plazo de implantación de las acciones es de 3 a 6 meses, para la implementación de las mismas. En el plazo de 9 meses a un año, se verificará que dichas acciones se encuentran implantadas, y si no, se deberá apremiar al Responsable, o analizar la posibilidad de incluir otras medidas de control adicionales o sustitutivas que permitan reducir el nivel de riesgo.”*

Aportan el Documento de Políticas de Seguridad, como DOC n.º 14.

Finalmente, manifiesta el Instituto su voluntad e interés de cumplir de forma escrupulosa con toda la normativa y aporta información sobre los nuevos protocolos y medidas para su cumplimiento, empezando por la designación de un DPO, ante la AEPD, del que aportan copia, habiendo contratado con fecha 17/03/2025 a una empresa especializada en informática para adoptar las medidas de seguridad necesarias para para una mayor seguridad confidencialidad de los datos específicamente, (…). (DOC Nº2 copia del contrato).

Aportan copia del documento “Manual para empleados” de la entidad (DOC Nº4), sobre Protección de Datos, que incluye un anexo I de confidencialidad y propiedad intelectual e industrial donde se informa de las normas de seguridad y protección de datos y Anexo II con detalle de las medidas de seguridad que incluyen disposiciones sobre datos en papel en proceso de revisión o tramitación, contraseñas, destrucción, equipos, soportes de almacenamiento, terminales móviles, uso de Internet y uso de correo electrónico entre otras. Se incluyen otros anexos con contenido especifico sobre normas de chats, o teletrabajo así como “*las Buenas Prácticas del CCN-CERT”* sobre el uso del correo electrónico para el envío de datos sensibles (BP/02) y referencias a normas relevantes de acceso a la Historia Clínica por parte de personal no sanitario.

Por último, aportan también certificado de formación impartida a los empleados sobre protección de datos.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 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 Presidencia 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
Tratamiento de categorías especiales de datos personales

El artículo 9 del RGPD, que regula el tratamiento de categorías especiales de datos personales, establece lo siguiente:

"1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:
a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión o de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional;

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud."

III

Seguridad del tratamiento

El artículo 32 del RGPD estipula lo siguiente:

"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."

IV
Integridad y confidencialidad

La letra f) del artículo 5.1 del RGPD propugna:

"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»)."

V
Conclusión

La presentas actuaciones de investigación se iniciaron a resultas de la piesta en conocimiento de esta AEPD de información de que pudieran haberse producido accesos por parte de personal no médico a información objeto de tratamiento por el Instituto.
Las actuaciones previas de investigación concluyen que el Instituto centra su actividad dentro del campo de análisis proteómicos sin diagnósticos a pacientes y que su labor se centra en el análisis de muestras que previamente han sido enviadas por los centros sanitarios u otras entidades y que cuenta en su plantilla con personal cualificado, especialista en los estudios biomédicos y adecuado para llevar a cabo las investigaciones y para el control integral del proceso ya que en otro caso se podría alterar el resultado de las pruebas realizadas.

En el Instituto solo tres empleados tienen acceso a los datos pseudonimizados de los pacientes, que se encuentran en un Excel cifrado con contraseña. Los resultados se comunican al médico solicitante vía email con documento cifrado, remitiendo la contraseña del documento por otra vía distinta

El Instituto ha realizado un Análisis de Riesgos y Evaluación de Impacto de Protección de Datos, identificando riesgos asociados a los accesos no autorizados a datos personales, estableciendo medidas correctoras específicas para mitigar este grupo de

riesgos, proponiendo a su vez también un conjunto de medidas específicas para el tratamiento de diagnóstico molecular y estudios médicos, que incluyen controles de acceso y perfiles de usuarios, cifrado, y formación de empleados entre otros.

También aporta el Instituto los compromisos de confidencialidad suscritos por los tres empleados no sanitarios (el bioquímico, la biotecnóloga y el técnico), en los que consta que la obligación de confidencialidad debe mantenerse aún después de concluida la relación laboral, y mencionándose responsabilidades en caso de incumplimiento.

La información recibida por la AEPD se centra exclusivamente en el número absoluto de accesos a la base de datos del Instituto (aprox. 1.500 accesos en 5 años) por parte del personal no sanitario, sin que haya aportado evidencias de los accesos por personal no sanitario a la información clínica de pacientes, ni aclarado cómo han obtenido la información en detalle de los accesos de las entidades con el número exacto por periodos temporales, por personal de perfil no sanitario.

Esta cifra absoluta de accesos no permite, por sí sola, sacar conclusión alguna sobre el grado de cumplimiento por parte del Instituto del RGPD y ante la falta de evidencias adicionales, y tiene por ello el carácter de mera sospecha inespecífica y genérica de posibles irregularidades, cuya veracidad y fundamento no quedan confirmados por la actividad previa de investigación de la AEPD.

Para que esta Agencia pueda apreciar la existencia de una infracción del RGPD, es imprescindible que concurran dos elementos esenciales: por un lado, que se haya producido un tratamiento de datos personales; y, por otro, que dicho tratamiento resulte ilícito por carecer de base jurídica, infringir principios del RGPD o vulnerar derechos del interesado, entre otras obligaciones del responsable del tratamiento. La responsabilidad debe ser atribuible a una persona física o jurídica identificada que actúe como responsable o encargado del tratamiento.

La información y abundante documentación aportada por el Instituto parecen estar alineadas con los principios y garantías previstos en el RGPD para el tratamiento de datos de salud en el ámbito de la investigación médica.

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.

Todo ello sin perjuicio de las posibles actuaciones posteriores que esta Agencia pudiera llevar a cabo, aplicando los poderes de investigación y correctivos que ostenta.

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

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a **INSTITUTO BIOTECNOLÓGICO EN MEDICINA INTEGRATIVA Y TERAPIAS AVANZADAS P&G, S.L.**

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública. La publicación se realizará 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 Presidencia 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.

940-101025

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos