

- **Expediente N.º: EXP202413235**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 8 de agosto de 2024, se presentó reclamación ante la Agencia Española de Protección de Datos contra **TRAK HEALTH SOLUTIONS, S.L.** con NIF **B02943348** (en adelante, TRAK HEALTH).

Los motivos en que basa la reclamación son los siguientes:

La parte reclamante manifiesta que la plataforma TRAK HEALTH destinada a la prestación de servicios de rehabilitación y tratamiento de fisioterapia online, condiciona el acceso pleno a sus funcionalidades a la aceptación, por parte del usuario, de la grabación de su imagen personal, lo que considera podría implicar un trato desigual o potencialmente discriminatorio respecto de aquellos usuarios que rechacen dicha grabación, al verse privados de la posibilidad acceder al tratamiento de rehabilitación completo.

Asimismo, señala una posible deficiencia en la obtención del consentimiento, en la medida en que, a su juicio, no se garantiza que este sea explícito y específico para el tratamiento de categorías especiales de datos personales.

Igualmente, considera que la información proporcionada a los usuarios sobre el uso de sus datos no es clara ni transparente, al no informar de la eventual utilización de las grabaciones con fines de entrenamiento de los sistemas de inteligencia artificial.

Por último, indica que la plataforma no incorpora advertencias ni recomendaciones dirigidas a los usuarios para evitar la posible captación de datos personales sensibles en el entorno doméstico, durante la grabación de las sesiones de rehabilitación.

Junto a su escrito aporta diversa documentación entre la que destaca:

- Documento “Ventanas_aplicacion” que comprende:
 - o Captura de pantalla de la “*VENTANA DE TÉRMINOS Y CONDICIONES PARA PODER USAR LA APLICACIÓN!*” de TRAK HEALTH.
 - o Captura de pantalla de una ventana emergente de una plataforma digital de ejercicios, en la que se informa al usuario de que, antes de empezar la actividad, va a realizar 3 ejercicios. Asimismo, se le plantea la posibilidad de activar un sistema de asistencia basado en IA, mediante la opción “¡Claro!

- Ejercitarme con IA*", o rechazar tal asistencia mediante la opción "No, gracias. Lo haré sin apoyo de la IA".
- Documento "*POLITICA_DE_PRIVACIDAD*" en el que se reproduce la Política de Privacidad de TRAK HEALTH SOLUTIONS, S.L.

SEGUNDO: Con fecha 22 de agosto de 2024, se da traslado a esta Agencia, desde la Autoridad Catalana de Protección de Datos, de la reclamación previamente descrita, presentada también, por la parte reclamante, en el registro electrónico de dicha autoridad.

TERCERO: Con fecha 8 de noviembre de 2024, de conformidad con el artículo 65 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 admitió a trámite la reclamación presentada.

CUARTO: 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.

Al objeto de investigar la ocurrencia de los hechos descritos, se realizó requerimiento de información a TRAK HEALTH con fecha 16/08/2025.

Con fecha 11/09/2025 la parte reclamada presentó escrito de contestación a dicho requerimiento de la que se extraen los siguientes aspectos:

- TRAK ofrece servicios de telerehabilitación, que ofrece para aquellos clientes que consientan y de manera opcional, retroalimentación realizada por IA. Para ello, será necesario que el cliente opte por activar la cámara de su dispositivo.
- La plataforma es utilizable sin cámara, manteniendo la prestación asistencial básica.
- Las grabaciones no son descargables, se accede a ellas mediante URL firmadas de corta duración y no se reutilizan para entrenar modelos o IA. (Se documenta en la EIPD y en el RAT que se acompañan).
- Se adjunta el Registro de Actividades del Tratamiento con la ficha específica del tratamiento al que se refiere la reclamación (identificación de finalidades, categorías de datos —incluidos datos de salud—, colectivos, destinatarios, plazos de conservación y medidas).
- Se identifica como base de legitimación el artículo 6.1 b) y el artículo 9.2 h) del RGPD para el tratamiento de categorías especiales de datos. No obstante, para la activación opcional de la cámara de vídeo se señalan los artículos 6.1 a) y 9.2 a) del RGPD separado del alta/uso general y registrando prueba de consentimiento. Se aportan textos informativos y evidencias de interfaz/flujo de consentimiento. (Anexo A2 y A3).

- En relación con el derecho de supresión y los plazos de conservación (5 años según la página web) se cuenta con un procedimiento para el bloqueo de los datos, del que se aporta copia. Además, se aporta copia del Mapa de ciclo de vida y 'finalización' de la EIPD.
- Consta copia de EIPD incluyendo: análisis de necesidad y proporcionalidad, matriz de riesgos, medidas técnicas y organizativas, y decisión de no proceder a consulta previa al no existir riesgo residual alto no mitigable
- Por otra parte, se aporta extracto de política de privacidad/capas informativas que reflejan la no reutilización de grabaciones para entrenar IA y la opcionalidad de la cámara.

FUNDAMENTOS DE DERECHO

I

Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del RGPD confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 de la 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

Licitud del tratamiento

El artículo 6.1 del RGPD establece las condiciones que deben cumplirse para que el tratamiento de datos personales sea lícito:

"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

- a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;*
- b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;*
- c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;*
- d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;*
- e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;*
- f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del*



interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones. [...]”.

III

Tratamiento de datos de categoría especial

Por su parte, el artículo 9.1 del RGPD, bajo la rúbrica “*Tratamiento de categorías especiales de datos personales*”, determina:

“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.

En su apartado 2, el citado precepto, establece las excepciones que deben concurrir para que pueda llevarse a cabo su tratamiento, entre otras:

“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.”

IV

Conclusión

En el presente caso, la parte reclamada presta servicios de rehabilitación online, ofreciendo de manera opcional la posibilidad de recibir correcciones a través de un sistema de IA. Para ello, será necesario la activación de la cámara del dispositivo de los pacientes.

La reclamación presentada ante la AEPD señalaba, en lo que interesa a la normativa en materia de protección de datos, deficiencias en la manera de recabar el consentimiento de datos de salud, deficiencias en la información sobre el tratamiento, así como supuestas deficiencias relacionadas con la conservación de los datos y la recogida de datos excesivos.

No obstante, durante las actuaciones previas de investigación no se han obtenido indicios racionales suficientes de la existencia de una infracción en el ámbito competencial de la AEPD por cuanto que, de acuerdo con lo indicado por la parte reclamada, el tratamiento de datos personales derivado de su actividad se sustenta en en la ejecución de la relación contractual establecida con el usuario para la prestación asistencial básica de servicios de rehabilitación, al amparo del artículo 6.1.b) del RGPD, en relación con la excepción prevista en el artículo 9.2.h) del mismo texto legal para los datos de salud. Sobre esta base el reclamante puede acceder y utilizar la plataforma en su modalidad básica, sin necesidad de activar la cámara ni las funcionalidades de la IA para lo cual, en el momento del acceso, se habilita un mecanismo que permite aceptar expresamente las funcionalidades adicionales.

En lo que respecta a prestaciones adicionales, como la grabación de las sesiones del usuario en la plataforma y la opcional y consentida asistencia mediante IA, TRAK

HEALTH articula a través de su página web un mecanismo específico de aceptación que permite al interesado prestar su consentimiento explícito, conforme a los artículos 6.1.a) y 9.2.a) del RGPD, en la medida en que se trata de funcionalidades opcionales que no resultan necesarias para la prestación asistencial básica

Por otro lado, según la documentación que obra en el expediente, la grabación de las sesiones de los pacientes se encuentra sometida a un régimen de acceso restringido, limitado exclusivamente al profesional sanitario asignado, con la finalidad de supervisar la evolución del paciente, sin que se hayan recabado indicios de que las grabaciones se destinen finalidades distintas de las indicadas.

Tampoco constan indicios racionales suficientes sobre la captación de datos excesivos o imposibilidad del ejercicio del derecho de supresión como señalaba la parte reclamante.

A este respecto, debe destacarse que en el ámbito administrativo sancionador son de aplicación, con alguna matización, pero sin excepciones, los principios inspiradores del orden penal, teniendo plena virtualidad el principio de presunción de inocencia, que debe regir sin excepciones en el ordenamiento sancionador y ha de ser respetado en la imposición de cualesquiera sanciones.

El Tribunal Constitucional en Sentencia 76/1990, considera que el derecho a la presunción de inocencia comporta

“que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio”.

De acuerdo con este planteamiento, el artículo 53.2 de la LPACAP, establece que, en el caso de procedimientos administrativos de naturaleza sancionadora, los presuntos responsables tendrán los siguientes derechos:

“b) A la presunción de no existencia de responsabilidad administrativa mientras no se demuestre lo contrario.”

Como ha precisado el Tribunal Supremo en Sentencia de 26 de octubre de 1998, la vigencia del principio de presunción de inocencia

“no se opone a que la convicción judicial en un proceso pueda formarse sobre la base de una prueba indiciaria, pero para que esta prueba pueda desvirtuar dicha presunción debe satisfacer las siguientes exigencias constitucionales: los indicios han de estar plenamente probados – no puede tratarse de meras sospechas – y tiene que explicitar el razonamiento en virtud del cual, partiendo de los indicios probados, ha llegado a la conclusión de que el imputado realizó la conducta infractora, pues, de otro modo, ni la subsunción estaría fundada en Derecho ni habría manera de determinar si el proceso deductivo es arbitrario, irracional o absurdo, es decir, si se ha vulnerado el derecho a la presunción de inocencia al estimar que la actividad probatoria pueda entenderse de cargo.”

Así las cosas, se debe distinguir la verdadera prueba de indicios de las meras sospechas o conjeturas. El Tribunal Constitucional ha manifestado en su Sentencia 24/1997 que

“los criterios para distinguir entre pruebas indiciarias capaces de desvirtuar la presunción de inocencia y las simples sospechas se apoyan en que: a) La prueba indiciaria ha de partir de hechos plenamente probados. b) Los hechos constitutivos de delito deben deducirse de esos indicios (hechos completamente probados) a través de un proceso mental razonado y acorde con las reglas del criterio humano, explicitado en la sentencia condenatoria (SSTC 174/1985, 175/1985, 229/1988, 107/1989, 384/1993 y 206/1994, entre otras).”

En definitiva, el principio de presunción de inocencia impide imputar una infracción administrativa cuando no se haya obtenido y constatado una prueba de cargo que acredite los hechos que motivan la imputación o la intervención en los mismos del presunto infractor.

Estrechamente vinculado al principio de presunción de inocencia, se encuentra el principio *in dubio pro reo*, del que la Sentencia del Tribunal Constitucional de 20/02/1989 indica que *“Nuestra doctrina y jurisprudencia penal han venido sosteniendo que, aunque ambos puedan considerarse como manifestaciones de un genérico favor rei, existe una diferencia sustancial entre el derecho a la presunción de inocencia, que desenvuelve su eficacia cuando existe una falta absoluta de pruebas o cuando las practicadas no reúnen las garantías procesales y el principio jurisprudencial in dubio pro reo que pertenece al momento de la valoración o apreciación probatoria, y que ha de juzgar cuando, concurre aquella actividad probatoria indispensable, exista una duda racional sobre la real concurrencia de los elementos objetivos y subjetivos que integran el tipo penal de que se trate.”*

De acuerdo con este principio, aplicable también al ámbito del derecho administrativo sancionador, la carga de la prueba recae en la administración, señalándose que, en caso de duda sobre los hechos o la responsabilidad del investigado/imputado debe realizarse la interpretación más favorable al presunto infractor.

En el presente caso, como se ha expuesto, no se han encontrado indicios racionales suficientes que permitiesen imputar a TRACK la comisión de infracciones de la normativa de protección de datos personales, por lo que no cabe estimar enervado el derecho a la presunción de inocencia que le ampara.

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, 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 **TRAK HEALTH SOLUTIONS, S.L.** y a la parte reclamante.

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