ANEXO III

CONTRATO DE ENCARGO DE TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

De una parte, Jordi Surrallés Calonge como responsable de los tratamientos de protección de datos de la FUNDACIÓ INSTITUT DE RECERCA DE L'HOSPITAL DE LA SANTA CREU I SANT PAU (en adelante, "IR SANT PAU o RESPONSABLE") con NIF nº G-60136934 y domicilio social en Carrer Sant Quintí, número 77-79, 08041 Barcelona, y en ejercicio de las funciones que le confiere el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD), y la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD)

Y de otra parte PREVENCONTROL, S.A., con NIF nº ESA62071097 y domicilio social en la calle Sant Pau, 25, de Terrassa (08221), representada en este acto por D. Joaquim Ruiz Bosch actúa en su calidad de Apoderado de la sociedad, en virtud de poder conferido por acuerdo del Consejo de Administración de PREVENCONTROL, S.A. de fecha 19 de junio de 2024, elevado a público el mismo día ante el Notario de Barcelona D. Pedro Ángel Casado Martín, bajo el número 1293 de su protocolo, cuya inscripción en el Registro Mercantil se halla vigente y cuyas facultades no han sido revocadas ni en adelante "Encargado de tratamiento").

Ambas partes se reconocen recíprocamente la capacidad legal necesaria para obligarse de común acuerdo y

MANIFIESTAN

1. Que el RESPONSABLE, de acuerdo con las competencias que tiene atribuidas, le corresponde la realización de la Prevención de Riesgos Laborales y ha contratado los servicios del ENCARGADO consistentes en la prestación del: "*Servei d'assessoria i consultoria en Prevenció de Riscos Laborals així com la disponibilitat d'una plataforma de formació i una plataforma de gestió de la prevenció per a l'Institut de Recerca Sant Pau, segons característiques tècniques i condicions definides en el Plec de Prescripcions Tècniques, per garantir el nivell de prestació requerida per l'Institut de Recerca Sant Pau*", con la duración que consta descrita en el expediente de licitación LICIR 25/17 y el contrato de prestación de servicios (en adelante, los "servicios").

2. Que los datos relativos a la aptitud médica de las personas trabajadoras, obtenidos en el marco de la vigilancia de la salud, constituyen datos de salud en los términos establecidos en el artículo 9.1 del Reglamento (UE) 2016/679 (RGPD) y en el Considerando 35 del mismo. En relación con dichos datos, PREVENCONTROL actúa como responsable del tratamiento, conforme a lo dispuesto en el artículo 4.7 del RGPD, al determinar los fines y medios del tratamiento, incluida la realización de reconocimientos médicos y la emisión del juicio clínico correspondiente. En consecuencia, el tratamiento de esta información queda excluido del objeto del presente contrato, que se limita exclusivamente a las actividades en las que PREVENCONTROL actúa como encargado del tratamiento por cuenta del cliente

3. Dado que la ejecución del contrato mencionado por parte de PREVENCONTROL, S.A implica el tratamiento de datos personales de los que es responsable IR SANT PAU, PREVENCONTROL, S.A., tendrá la condición de encargada del tratamiento, de conformidad con el RGPD y la LOPDGDD.

4. Que, el ENCARGADO dispone de la capacidad y los recursos necesarios para garantizar que ofrece suficientes garantías para aplicar medidas técnicas y organizativas apropiadas para cumplir con lo que establece la normativa vigente y proteger los derechos de los interesados, por lo cual ambas partes convienen suscribir el presente contrato de encargo de tratamiento de datos de carácter personal en relación con el contrato mencionado, en los términos establecidos en los artículos 28 del RGPD y 33 de la LOPDGDD y con sujeción a las siguientes:

CLÁUSULAS

1. Objeto, naturaleza y finalidad del encargo

Mediante el presente contrato de encargo, se habilita al encargado del tratamiento para tratar, por cuenta de IR SANT PAU, los datos de carácter personal necesarios para la prestación del servicio de asesoría y consultoría en Prevención de Riesgos Laborales.

El tratamiento consistirá en la prestación de asesoramiento especializado, así como en el suministro de una plataforma de formación y una plataforma de gestión de la prevención en materia de Prevención de Riesgos Laborales.

2. Tipo de datos personales y categoría de interesados

Para ejecutar las prestaciones derivadas objeto del presente contrato de encargo, el responsable coloca a disposición del encargado la siguiente información:

- Tipo de datos personales a los que tendrá acceso el ENCARGADO: nombre, apellido, formación, perfil profesional, información sobre la aptitud para desarrollar el puesto de trabajo de cada uno de los trabajadores.
- Categorías de interesados: empleados del RESPONSABLE
- Operaciones de tratamiento autorizadas: acceso, recogida, conservación, consulta, supresión, registro y destrucción.

3. Duración

La vigencia del presente contrato de encargo queda vinculada a la duración del contrato principal suscrito, derivado del proceso de licitación LICIR 25/17. Dicha vigencia se extenderá hasta la finalización de dicho contrato, incluyendo sus posibles prórrogas o modificaciones debidamente formalizadas.

4. Obligaciones y derechos del RESPONSABLE

El RESPONSABLE garantiza que los datos facilitados al ENCARGADO se han obtenido lícitamente y que son adecuados, pertinentes y limitados a los fines del tratamiento.

El RESPONSABLE pondrá a disposición del ENCARGADO los datos a los que se refiere la cláusula segunda de este contrato para ejecutar las prestaciones objeto del encargo.

El RESPONSABLE tiene derecho a obtener del ENCARGADO toda la información que considere necesaria relativa a los datos y tratamientos descritos en la cláusula segunda, a fin de poder cumplir con sus obligaciones como RESPONSABLE.

El RESPONSABLE velará, antes y durante todo el tratamiento, para que el ENCARGADO cumpla la normativa en materia de protección de datos.

El RESPONSABLE tiene derecho a obtener la asistencia del ENCARGADO para atender las solicitudes e inspecciones de cualquier autoridad de control cuando los tratamientos objeto de aquellas sean los que lleva a cabo el ENCARGADO.

El RESPONSABLE tiene derecho a ser compensado por el ENCARGADO por los daños y perjuicios que sufra como consecuencia del incumplimiento de las obligaciones del ENCARGADO o de sus subcontratistas. El RESPONSABLE advierte al ENCARGADO que, si determina por su cuenta los fines y los medios del tratamiento, será considerado responsable del tratamiento y estará sujeto a cumplir las disposiciones de la normativa vigente aplicables como tal.

Corresponde al RESPONSABLE facilitar el derecho de información en el momento de la recogida de los datos.

5. Obligaciones y derechos del ENCARGADO

El ENCARGADO se obliga a respetar todas las obligaciones que pudieran corresponderle como encargado del tratamiento conforme lo dispuesto en la normativa vigente y cualquier otra disposición o regulación que le fuera igualmente aplicable.

El ENCARGADO tratará los datos únicamente de acuerdo con las instrucciones documentadas del responsable del tratamiento. Si el ENCARGADO del tratamiento considera que alguna de las instrucciones del responsable infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, deberá informar inmediatamente al RESPONSABLE

El ENCARGADO no destinará, aplicará o utilizará los datos a los que tenga acceso para un fin distinto al encargo o que suponga el incumplimiento de este contrato.

El ENCARGADO pondrá a disposición del RESPONSABLE la información necesaria para demostrar el cumplimiento del contrato, permitiendo las inspecciones y auditorías necesarias para evaluar el tratamiento.

El ENCARGADO mantendrá el deber de secreto respecto de los datos personales a los que haya tenido acceso en virtud del presente acuerdo, incluso después de finalizada su relación contractual con el RESPONSABLE.

El ENCARGADO también deberá asistir al responsable a garantizar el cumplimiento de las siguientes obligaciones, teniendo en cuenta la naturaleza del tratamiento y la información de la que disponga:

a) La obligación de realizar una evaluación de impacto de las operaciones de tratamiento en la protección de datos personales, cuando sea probable que un determinado tratamiento suponga un alto riesgo para los derechos y libertades de las personas físicas.

b) La obligación de consultar a la autoridad de control antes de iniciar el tratamiento, cuando la evaluación de impacto relativa a la protección de datos evidencie que el tratamiento comporta un alto riesgo si el responsable no adopta las medidas necesarias para mitigarlo.

c) La obligación de garantizar que los datos personales sean exactos y estén actualizados.

En caso de que el ENCARGADO participe en la recogida de datos por cuenta del RESPONSABLE, será este último quien determine previamente el contenido y formato de la cláusula informativa que deba ser entregada a los interesados. El ENCARGADO colaborará en su entrega, en la puesta a disposición de dicha información en nombre del RESPONSABLE si así se acuerda.

El ENCARGADO devolverá al RESPONSABLE del tratamiento los datos de carácter personal y, en su caso, los soportes en los que consten, una vez finalizada la prestación. Esta devolución incluirá el borrado de los datos existentes en los sistemas del ENCARGADO, salvo aquellos que deban conservarse debidamente bloqueados por exigencias legales o mientras puedan derivarse responsabilidades relacionadas con la prestación.

El ENCARGADO en el caso de uso de servidores, comunicará el lugar en el que estarán ubicados y desde donde se prestarán los servicios asociados a estos, así como cualquier cambio significativo que pueda afectar al cumplimiento de la normativa aplicable en materia de protección de datos.

6. Personal autorizado para realizar el tratamiento

El ENCARGADO limitará el acceso a los datos personales tratados a los miembros de su personal en la medida en que sea estrictamente necesario para la ejecución, gestión y seguimiento del encargo y garantiza que el personal autorizado para realizar el tratamiento se ha comprometido de forma expresa y por escrito a respetar la confidencialidad de los datos o que está sujeto a una obligación legal de confidencialidad de naturaleza estatutaria, así como a cumplir con las medidas de seguridad correspondientes, de las cuales deberán ser informadas debidamente.

Mantendrá a disposición del RESPONSABLE la documentación que acredite su cumplimiento.

El ENCARGADO tomará medidas para garantizar que cualquier persona que actúe bajo su autoridad y tenga acceso a datos personales sólo pueda tratarlos siguiendo las instrucciones del RESPONSABLE o esté obligada a ello en virtud de la legislación vigente.

El ENCARGADO garantiza que el personal autorizado para realizar el tratamiento ha recibido la formación necesaria para asegurar que no se pondrá en riesgo la protección de datos personales.

7. Medidas de seguridad

El ENCARGADO manifiesta estar al corriente en lo que concierne a las obligaciones derivadas de la normativa de protección de datos, especialmente en lo que se refiere a la implantación de las medidas de seguridad para las diferentes categorías de datos y de tratamiento establecidas en el artículo 32 del GDPR.

El ENCARGADO garantiza que se implementarán adecuadamente dichas medidas de seguridad y ayudará al RESPONSABLE a cumplir las obligaciones establecidas en los artículos 32 a 36 del GDPR, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del ENCARGADO. El RESPONSABLE realizará un análisis de los posibles riesgos derivados del tratamiento para determinar las medidas de seguridad apropiadas para garantizar la seguridad de la información tratada y los derechos de los interesados y, si determinara que existen riesgos, trasladará al ENCARGADO un informe con la evaluación de impacto para que proceda a la implementación de medidas adecuadas para evitarlos o mitigarlos.

Se adjunta al presente Anexo un listado con las medidas de seguridad específicas aplicadas por parte del ENCARGADO.

El ENCARGADO, por su parte, deberá analizar los posibles riesgos y otras circunstancias que puedan incidir en la seguridad que le sean atribuibles, debiendo informar, si los hubiere, al RESPONSABLE para evaluar su impacto.

De todas formas, el ENCARGADO garantiza que, teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, implementará medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que entrañe el tratamiento, que en su caso incluya, entre otros:

- Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

- Restaurar la disponibilidad y el acceso a datos de forma rápida en caso de incidente físico o técnico.

- Procedimientos de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas
para garantizar la seguridad del tratamiento.

- Seudonimizar y cifrar los datos personales, si aplica.

El ENCARGADO informa, así mismo, que tiene contratado a un Delegado de Protección de datos, cuyos datos se facilitan a continuación:

DESPATX D'ADVOCATS BADIA S.L.P
Sr. Andreu Alonso
aalonso@badia-adv.cm
93.788.56.33 www.badia-adv.com

8. Violación de la seguridad

En el supuesto de violación de la seguridad de los datos personales, el encargado debe colaborar con el responsable y ayudarle a cumplir las obligaciones que le atribuye el RGPD, de la siguiente manera:

1. Cuando se trate de una violación de seguridad de datos personales tratados por el responsable, el encargado debe asistir al responsable en las siguientes acciones:

   a) Notificar la violación de seguridad de los datos personales a la autoridad de control sin dilación indebida desde que tenga conocimiento, si procede.

   b) Preparar toda la información relevante para documentar y comunicar el incidente, incluyendo como mínimo:

   - Descripción de la naturaleza de los datos personales, incluidas, cuando sea posible, las categorías y el número aproximado de interesados afectados, así como las categorías y el número aproximado de registros de datos personales afectados.
   - Descripción de las posibles consecuencias de la violación de seguridad de los datos personales.
   - Descripción de las medidas adoptadas o propuestas para remediar la violación de seguridad de los datos personales, incluidas, si procede, las medidas para mitigar los posibles efectos negativos.

Si no es posible facilitar la información de forma simultánea, y en la medida en que no lo sea, se deberá proporcionar de forma gradual sin dilación indebida.

   c) Comunicar la violación de seguridad de los datos personales al interesado sin dilación indebida desde que tenga conocimiento, si procede.

2. Cuando se trate de una violación de seguridad de datos personales tratados por el ENCARGADO:

Este deberá informar al responsable del tratamiento, sin dilación indebida y en todo caso antes de 24 horas desde que tenga conocimiento, sobre las violaciones de seguridad de los datos personales bajo su responsabilidad de las que tenga constancia, junto con toda la información relevante para documentar y comunicar el incidente, por correo electrónico a la dirección indicada en la cláusula novena de este contrato de encargo.

Si se dispone de ella deberá facilitarse, como mínimo, la información especificada en el apartado b) del punto 1 y, adicionalmente, el nombre y los datos de una persona de contacto en la que se pueda obtener más información.

Si no es posible facilitar la información de forma simultánea, y en la medida en que no lo sea, esta se deberá proporcionar de forma gradual sin dilación indebida.

9. Comunicación de los datos a terceros

El ENCARGADO no podrá comunicar los datos a otros destinatarios, salvo que hubiera obtenido una autorización previa y por escrito del RESPONSABLE y se den los supuestos legalmente admisibles; la cual, de existir, se anexará al presente contrato.

El ENCARGADO podrá comunicar datos personales a otros encargados del tratamiento del mismo RESPONSABLE, siempre de conformidad con las instrucciones del RESPONSABLE. En tal caso, este último deberá identificar previamente y por escrito la entidad a la que se comunicarán los datos, la finalidad, los datos objeto de comunicación y las medidas de seguridad que deberán aplicarse.

La comunicación de los datos a Autoridades públicas en el ejercicio de sus funciones públicas no son consideradas comunicaciones de datos, por lo que no se precisará de la autorización del RESPONSABLE si dichas transmisiones son necesarias para alcanzar la finalidad del encargo.

Las comunicaciones dirigidas al RESPONSABLE de tratamiento se enviarán a: Carrer Sant Quintí, 77-79, 08041 Barcelona y correo electrónico: dpo_ir@santpau.cat

Las comunicaciones dirigidas al ENCARGADO de tratamiento se enviarán a: Carrer Sant Pau, 25, 08221 - Terrassa y correo electrónico:lopd_rv@prevencontrol.com

10. Transferencias internacionales de datos

El ENCARGADO no podrá realizar transferencias de datos a terceros países u organizaciones internacionales no establecidos en la UE, salvo que hubiera obtenido una autorización previa y por escrito del RESPONSABLE; la cual, de existir, se anexará al presente contrato.

11. Subcontratación del tratamiento de datos

Se pueden subcontratar algunos de los tratamientos de datos previstos en el objeto de este encargo. El RESPONSABLE autoriza expresamente al ENCARGADO a la contratación de servicios de hosting y auxiliares a la siguiente empresa, quién se ha obligado a las mismas condiciones y requisitos de tratamiento de datos que constan en el presente Contrato con el ENCARGADO:

Turing Projects
S.L. CIF:
B66276072
Carrer Castanyers, 3
08461 Sant Esteve de
Palautordera. Barcelona
Tel.: +

Para subcontratar con otras empresas el ENCARGADO deberá comunicarse previamente y por escrito al responsable, con una antelación de un mes. Deberán indicarse los tratamientos que se pretende subcontratar e identificarse de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición dentro del plazo establecido.

El subcontratista, que también tiene la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el ENCARGADO y las instrucciones que dicte el RESPONSABLE. Corresponde al ENCARGADO inicial regular la nueva relación, de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad...) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. Si el subencargado incumple dichas condiciones, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo relativo al cumplimiento de las obligaciones

En todo caso, el RESPONSABLE *deberá estar informado de* toda la cadena de subcontratación.

12. Derechos de los interesados

El ENCARGADO asistirá al RESPONSABLE del tratamiento en la respuesta al ejercicio de los siguientes derechos:

1. Acceso, rectificación, supresión y oposición.
2. Limitación del tratamiento.
3. Portabilidad de los datos.
4. A no ser objeto de decisiones individuales automatizadas (incluida la elaboración de perfiles).

Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento o a no ser objeto de decisiones individuales automatizadas ante el encargado del tratamiento, este deberá comunicarlo por correo electrónico a la dirección indicada en la cláusula octava de este contrato de encargo. La comunicación deberá realizarse sin dilación indebida desde la recepción de la solicitud por el ENCARGADO y, en la medida de lo posible, en un plazo máximo de tres días laborables, junto con, en su caso, cualquier otra información que pueda ser relevante para resolver la solicitud.

13. Responsabilidad

Conforme el artículo 82 del RGPD, el RESPONSABLE que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto en el RGPD. El ENCARGADO únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del RGPD dirigidas específicamente al ENCARGADO o haya actuado al margen o en contra de las instrucciones legales del RESPONSABLE. Del mismo modo el RESPONSABLE o ENCARGADO estará exento de responsabilidad si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios. En el caso de que el RESPONSABLE y el ENCARGADO hayan participado en la misma operación de tratamiento y sean, con arreglo al citado artículo, responsables de cualquier daño o perjuicio causado por dicho tratamiento, cada RESPONSABLE o ENCARGADO será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado.

14. Fin de la prestación de servicio

Una vez finalice la prestación de servicios objeto de este contrato, si el ENCARGADO hubiera almacenado datos personales, deberá suprimirlos o devolverlos a elección del RESPONSABLE, incluidas las copias existentes. El ENCARGADO deberá emitir a un certificado de destrucción o devolución si así lo exige el RESPONSABLE.

No procederá la supresión de datos cuando se requiera su conservación por una obligación legal, en cuyo caso el ENCARGADO procederá a la custodia de los mismos bloqueando los datos y limitando su tratamiento en tanto que pudieran derivarse responsabilidades de su relación con el RESPONSABLE.

El ENCARGADO mantendrá el deber de secreto y confidencialidad de los datos incluso después de finalizar la relación objeto de este contrato.

15. Modificación del contrato de encargo

Este contrato de encargo de tratamiento de datos personales podrá modificarse de forma expresa y de mutuo acuerdo entre las partes, mediante la firma de la correspondiente adenda

Y para que conste a los efectos oportunos, en prueba de conformidad de las partes, firman el presente contrato, por duplicado, en el lugar y la fecha indicados en el encabezamiento.

Por FUNDACIÓ INSTITUT DE RECERCA DE L'HOSPITAL DE LA SANTA CREU I SANT PAU

JORDI SURRALLES (R: G60136934)

Firmado digitalmente por JORDI SURRALLES (R: G60136934)
Fecha: 2025.07.16 10:51:30 +02'00'

Jordi Surrallés Calonge
Responsable de Tratamiento

Por PREVENCONTROL, SA

JOAQUIN RUIZ (R: A62071097)

Firmado digitalmen
JOAQUIN RUIZ (R
DN: JOAQUIN RUIZ (R:
A62 c=
PRE SA, email=
comptabilitat@prevencontrol.net
Fecha: 2025.07.16 09:55:30 +02'00'

Joaquín Ruiz Bosch
Encargado de Tratamiento

ANEXO I. MEDIDAS DE SEGURIDAD APLICADAS POR EL ENCARGADO

Preámbulo

El presente anexo recoge las medidas técnicas y organizativas de seguridad aplicables por parte de PREVENCONTROL, en su condición de encargado del tratamiento, de conformidad con el artículo 28.3.c) del Reglamento (UE) 2016/679 (RGPD).

Este anexo tiene carácter genérico y transversal, dado que el contrato comprende varios servicios de distinta naturaleza. Por ello, se incluyen a continuación medidas aplicables a todas aquellas capas de servicio en las que PREVENCONTROL actúa como encargado del tratamiento, que son:

- Servicio de prevención de riesgos laborales (salvo vigilancia de la salud).
- Servicio de consultoría en PRL.
- Plataforma eLearning.
- Licencia SaaS de la plataforma SmartOSH.

Queda expresamente excluida del ámbito de este anexo la vigilancia de la salud, ya que el tratamiento de los datos de salud derivados de esta actividad se realiza bajo la responsabilidad directa del personal sanitario, sin intervención de PREVENCONTROL como encargado del tratamiento.

Las partes podrán acordar, durante la ejecución del contrato, medidas de seguridad específicas y complementarias para determinadas actuaciones o capas del servicio, en función del riesgo, la sensibilidad de los datos tratados y el alcance de la intervención de PREVENCONTROL.

1. Principios generales

PREVENCONTROL aplica un modelo de seguridad de la información basado en los siguientes principios:

- Confidencialidad, integridad y disponibilidad de los datos.
- Minimización y limitación del tratamiento de los datos personales.
- Prevención y respuesta ante incidentes de seguridad.

2. Certificaciones

Las infraestructuras utilizadas por PREVENCONTROL para la prestación de los servicios (plataforma SmartOSH) cuentan con las siguientes certificaciones:

- ISO/IEC 27001: sistema de gestión de la seguridad de la información.
- ENS (Esquema Nacional de Seguridad) en nivel básico o medio, según el servicio.

3. Medidas técnicas y organizativas

PREVENCONTROL aplica, entre otras, las siguientes medidas:

- Control de acceso lógico mediante autenticación robusta (usuario y contraseña segura, y en su caso, segundo factor).
- Gestión de roles y permisos, garantizando el principio de mínimo privilegio.
- Copias de seguridad periódicas, con política de retención definida.
- Cifrado de datos en tránsito, mediante protocolos seguros (TLS).
- Cifrado de datos en reposo, en entornos que así lo requieran.
- Registro de actividad (logs) de acciones realizadas por administradores y usuarios.
- Protocolo interno de gestión de incidentes, incluyendo la notificación al responsable dentro de los plazos legales en caso de violación de seguridad.
- Auditorías y revisiones periódicas de la seguridad de los sistemas.
- Formación continua del personal con acceso a datos personales, en materia de protección de datos y seguridad de la información.

4. Subencargados del tratamiento

Los proveedores utilizados por PREVENCONTROL (incluidos los de alojamiento y mantenimiento de la plataforma SmartOSH) son seleccionados mediante un procedimiento de evaluación de riesgos y homologación, y están vinculados contractualmente conforme a lo dispuesto en el artículo 28 del RGPD.

5. Evaluación y mejora continua

Las medidas descritas podrán ser objeto de revisión, adaptación o ampliación por parte de las partes, especialmente a medida que se vayan desarrollando los distintos servicios o funcionalidades del contrato. PREVENCONTROL se compromete a colaborar con el responsable del tratamiento para garantizar, en todo momento, un nivel de seguridad adecuado al riesgo.

Preven Control

S H E Ed.

Badia)advocats

CERTIFICADO DE ADECUACIÓN A LA NORMATIVA DE PROTECCIÓN DE DATOS

Andreu Alonso Juan-Muns, en representación de **DESPATX D'ADVOCATS BADIA SLP**, con NIF B64020209 y domicilio fiscal situado en Plaça Vella, 7. 1r 08221 Terrassa (Barcelona), como empresa consultora de privacidad de PREVENCONTROL SA, con NIF A62071097 y domicilio fiscal situado en CARRER SANT PAU, 25 - 08221 TERRASSA (Barcelona) de TERRASSA, con contrato vigente de asesoramiento, adaptación, mantenimiento y actualización a las normativas de privacidad que les afecten,

CERTIFICA

Que la empresa PREVENCONTROL SA ha recibido información suficiente y adecuada para adaptarse, mantenerse y actualizarse al Reglamento (UE) 2016/679, de 27 de abril (GDPR), y a la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD), y para transmitirla al personal autorizado para el tratamiento de datos personales y a los encargados del tratamiento.

Que PREVENCONTROL SA recibe asesoramiento de esta consultora para el cumplimiento de todas las disposiciones de las normativas aplicables para el tratamiento de los datos personales de su responsabilidad, y manifiestamente con los principios descritos en el artículo 5 del GDPR, por los que los datos personales son tratados de manera lícita, leal y transparente en relación con el interesado y son adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

Que PREVENCONTROL SA ha implementado políticas técnicas y organizativas apropiadas para aplicar las medidas de seguridad que establece el GDPR para proteger los derechos y libertades de los interesados y les ha facilitado la información adecuada para que puedan ejercerlos.

Terrassa, 31 de marzo de 2023

NOMBRE ALONSO JUAN-MUNS ANDREU - NIF

Firmado digitalmente por NOMBRE ALONSO JUAN-MUNS ANDREU

Fecha: 2023.03.31 10:56:24 +02'00'

Firmado: Andreu Alonso Juan-Muns

PREVENCONTROL SA

INFORME DE LA POLÍTICA DE SEGURIDAD (TRATAMIENTOS ESPECÍFICOS)

1. Identificación de la organización Responsable del tratamiento

De conformidad con lo dispuesto en el Reglamento (UE) 2016/679 de 27 de abril de 2016 (GDPR), la organización Responsable del tratamiento es quién determina los fines y los medios del tratamiento de datos personales (Ficheros).

Nombre fiscal	PREVENCONTROL SA
Marca comercial	PREVENCONTROL
Actividad	PREVENCIÓN DE RIESGOS LABORALES Y VIGILANCIA DE LA SALUD
Dirección	CARRER SANT PAU, 25 - 08221 TERRASSA (Barcelona)
Teléfono	902112124
E-mail	lopd_pc@prevencontrol.net
DPO	DESPATX D'ADVOCATS BADIA SLP aalonso@badia-adv.com

2. Identificación de los Ficheros de datos personales

Un fichero es un conjunto estructurado de datos personales accesibles con arreglo a criterios determinados y susceptibles de tratamiento para un fin específico.

Fichero	Descripción	Tipo	Sistema	Categoría
INFORMES MÉDICOS	Gestión administrativa de datos de salud para dar curso a expedientes por interés del interesado. Incluye bajas laborales, partes de accidentes, certificados de salud, etc.	Responsable	Mixto	ESPECIAL
VIGILANCIA DE LA SALUD	Gestión de revisiones médicas	Responsable	Mixto	ESPECIAL
SERVICIOS DE ASESORÍA LABORAL (SALUD)	Servicios laborales para empresas. Contratación, nóminas, despidos, etc. Incluyen datos de salud de partes de accidentes o bajas laborales .	Encargado	Mixto	ESPECIAL
SERVICIOS MÉDICOS A EMPRESAS	Servicios médicos prestados a centros de salud, geriátricos, reconocimientos médicos, vigilancia de la salud, clubs deportivos, etc.	Encargado	Mixto	ESPECIAL
CONTACTOS (SALUD)	Comunicación, información y gestión sobre productos y servicios. Incluye contactos web y redes sociales con información sensible (datos de salud)	Responsable	Mixto	ESPECIAL
REVISIONES MÉDICAS	Gestión de revisiones médicas	Responsable	Mixto	ESPECIAL
HISTORIAL CLÍNICO	Gestión y administración de datos de salud	Responsable	Mixto	ESPECIAL

3. Política de seguridad relativa a la protección de datos

La Organización ha implementado las siguientes medidas de protección de datos:

1. Protección de datos desde el diseño y por defecto.
2. Análisis de los riesgos del tratamiento.
3. Evaluación de impacto relativa a la protección de datos.

4. Medidas específicas de protección de datos.

3.1. Protección de datos desde el diseño y por defecto

De conformidad con el artículo 25 del Reglamento (UE) 2016/679 de 27 de abril de 2016 (GDPR), la protección de datos desde el diseño y por defecto se basa en la implementación de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que entraña el tratamiento teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, alcance, contexto y fines del tratamiento.

El Responsable del tratamiento ha aplicado desde el diseño y por defecto las siguientes medidas de seguridad:

Categorías de datos básicos

- **Finalidad del tratamiento:**
  - Se tratan los datos para fines determinados, explícitos y legítimos.
  - No se tratarán los datos posteriormente de manera incompatible con dichos fines.
- **Minimización de datos:**
  - Se obtienen únicamente los datos adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- **Exactitud de datos**
  - Se han adoptado mecanismos adecuados para actualizar los datos.
- **Confidencialidad del tratamiento:**
  - Se han suscrito acuerdos de confidencialidad con el personal autorizado.
  - Se han suscrito contratos de protección de datos con:
    - los encargados del tratamiento.
    - los corresponsables del tratamiento.
    - los destinatarios de datos.
- **Integridad y seguridad de los datos:**
  - Se han implementado mecanismos de identificación y autenticación para controlar el acceso a los sitemas informáticos mediante contraseñas cifradas y seguras con un mínimo de 8 caracteres, que deben incluir mayúsculas, minúsculas y dígitos.
  - Se han aplicado medidas de seguridad en el mobiliario y departamentos que contienen datos personales para restringir el acceso a personas no autorizadas y evitar que los datos sean accesibles a un número indeterminado de personas sin la intervención humana.
  - Se han adoptado medidas adecuadas para garantizar permanentemente:
    - la integridad y seguridad física de los datos.
    - la disponibilidad y resiliencia de los sistemas de tratamiento.
    - la restauración de datos mediante copias de respaldo.
    - la supresión efectiva de los datos o la seudonimización de los mismos.
  - Existe un protocolo para actuar ante las brechas de seguridad detectadas y, en el caso de producirse una violación de datos, proceder a activar los mecanismos necesarios para mitigar los riesgos que afecten los derechos y libertades de los interesados, así como los procedimientos para la notificación de la misma a la autoridad de control y la comunicación a los interesados si fuese necesario.
- **Derechos del interesado:**
  - Se han organizado los datos de manera que posibilite el ejercicio de los derechos del interesado.
  - Existe un protocolo de actuación para resolver sin dilación las solicitudes de derechos recibidas.

Categorías especiales de datos (incluye datos penales)

- **Medidas adicionales de seguridad**
  - Se han aplicado métodos para la seudonimización o cifrado de datos personales.
  - Se han implementado mecanismos de identificación y autenticación para controlar el acceso a los sitemas informáticos mediante contraseñas cifradas y seguras con un mínimo de 12 caracteres, que deben incluir mayúsculas, minúsculas, dígitos y símbolos.

- Para limitar el acceso a información que contiene categorías especiales de datos, se han aplicado las siguientes medidas de seguridad:
  - datos automatizados: autenticación adicional para acceder a ficheros o aplicaciones informáticas.
  - datos no automatizados: cierres con llave aplicados al mobiliario o departamentos.
- Se han adoptado mecanismos para impedir intentos reiterados de acceso no autorizados.
- Se han implementado mecanismos efectivos que impidan el acceso a la información contenida en los soportes móviles y trasladables fuera de la empresa.
- Se han implementado procesos de verificación, evaluación y valoración de las medidas de seguridad adoptadas.

Tratamientos con un alto riesgo para los derechos y libertades de los interesados

- **Evaluación de impacto**
  - Se han implementado medidas adecuadas para la aplicación de los resultados de la evaluación de impacto.

Transferencias internacionales de datos

- **Medidas adicionales de seguridad**
  - Se ha comprobado que las garantías de protección de datos en las cuales se basa la transmisión de datos son legítimas y vigentes.
  - En los contratos con los encargados de tratamiento autorizados para realizar transferencias internacionales de datos se especifica que deberán seguir las instrucciones del Responsable para efectuarlas.

Elaboración automatizada de perfiles

- **Medidas adicionales de seguridad**
  - Se han analizado los riesgos que atañen al tratamiento para evaluar el impacto sobre la protección de datos y se ha determinado que no existen tales riesgos debido a que las decisiones que puedan ser tomadas no pueden producir efectos jurídicos o de algún otro modo que afecten significativamente al interesado.
  - Se han tomado las medidas oportunas para que si en un futuro las decisiones que puedan ser tomadas puedan producir algún efecto jurídico como los detallados en el párrafo anterior, se aplique el protocolo para tratamientos con alto riesgo llevando a cabo una evaluación de impacto relativa a la protección de datos.

3.2 Análisis de los riesgos del tratamiento

De conformidad con el artículo 32 del Reglamento (UE) 2016/679 de 27 de abril de 2016 (GDPR), se ha analizado el nivel de seguridad a implantar en la Organización para garantizar la protección de datos, teniendo en cuenta los altos riesgos que pueda tener el tratamiento para los derechos y libertades de los interesados, como consecuencia de:

- La destrucción accidental o ilícita de datos.
- La pérdida, alteración o comunicación no autorizada.
- El acceso a los datos cuando sean transmitidos, conservados u objeto de algún otro tipo de tratamiento.

Teniendo en cuenta las operaciones de tratamiento realizadas se ha determinado que existe la probabilidad de altos riesgos, por lo que, además de las medidas establecidas en la protección de datos desde el diseño y por defecto, también

se aplican las medidas dispuestas en la evaluación de impacto.

3.3 Evaluación de impacto relativa a la protección de datos

De conformidad con el artículo 35 del Reglamento (UE) 2016/679 de 27 de abril de 2016 (GDPR), el Responsable del tratamiento ha realizado una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales con el fin de establecer los riesgos para los derechos y libertades de los interesados sujetos a tratamiento y aplicar las medidas de seguridad adecuadas para mitigar dichos riesgos.

Se ha previsto revisar la evaluación de impacto siempre que se prevean cambios en los riesgos del tratamiento o, si no fuera el caso, en un máximo de 2 años.

3.4 Medidas específicas de protección de datos.

El Responsable del tratamiento dispone de los siguientes informes reglamentarios para garantizar la protección de datos:

- Registro de las actividades del tratamiento (conforme el artículo 30 del GDPR).
- Protocolo para dar curso al ejercicio de los derechos del interesado (conforme los artículos 13 a 23 del GDPR).
- Protocolo para resolver las violaciones de la seguridad (conforme los artículos 33 y 34 del GDPR).