ANEXO I: Contrato de tratamiento de datos entre Igenomix Spain Lab SLU en calidad de encargado del tratamiento y el Cliente, en calidad de responsable del tratamiento ubicado dentro de la UE/el EEE

SECCIÓN I

Cláusula 1 Finalidad y ámbito de aplicación

a) La finalidad del presente Contrato de tratamiento de datos, basado en las cláusulas contractuales tipo[1] (en lo sucesivo, «pliego de cláusulas») es garantizar que se cumpla el **artículo 28, apartados 3 y 4, del 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**.

b) Los responsables y encargados del tratamiento enumerados en el anexo I han dado su consentimiento a vincularse por el presente pliego de cláusulas a fin de garantizar el cumplimiento del artículo 28, apartados 3 y 4, del Reglamento (UE) 2016/679 y/o del artículo 29, apartados 3 y 4, del Reglamento (UE) 2018/1725.

c) El presente pliego de cláusulas se aplica al tratamiento de datos personales especificado en el anexo II.

d) Los anexos I a IV forman parte del pliego.

e) El presente pliego de cláusulas se entiende sin perjuicio de las obligaciones a las que esté sujeto el responsable en virtud del Reglamento (UE) 2016/679 y/o del Reglamento (UE) 2018/1725.

f) El presente pliego de cláusulas no garantiza por sí mismo el cumplimiento de las obligaciones relativas a las transferencias internacionales contempladas en el capítulo V del Reglamento (UE) 2016/679 y/o del Reglamento (UE) 2018/1725.

Cláusula 2 Invariabilidad del pliego de cláusulas

a) Las partes se comprometen a no modificar el pliego de cláusulas, excepto para añadir o actualizar información en los anexos.

b) Esto no es óbice para que las partes incluyan en un contrato más amplio las cláusulas contractuales tipo que contiene el presente pliego, ni para que añadan otras cláusulas o garantías adicionales siempre que no contradigan, directa o indirectamente, el pliego de cláusulas ni perjudiquen los derechos o libertades fundamentales de los interesados.

Cláusula 3 Interpretación

a) Cuando en el presente pliego de cláusulas se utilizan términos definidos en el Reglamento (UE) 2016/679 o en el Reglamento (UE) 2018/1725, respectivamente, se entiende que tienen el mismo significado que en el Reglamento correspondiente.

b) El presente pliego de cláusulas deberá leerse e interpretarse con arreglo a las disposiciones del Reglamento (UE) 2016/679 o del Reglamento (UE) 2018/1725, respectivamente.

c) No se podrán realizar interpretaciones del presente pliego de cláusulas que entren en conflicto con los derechos y obligaciones establecidos en el Reglamento (UE) 2016/679 o que perjudiquen los derechos o libertades fundamentales de los interesados.

Cláusula 4 Jerarquía

En caso de contradicción entre el presente pliego de cláusulas y las disposiciones de acuerdos conexos entre las partes que estuvieren en vigor en el momento en que se pactare o comenzare a aplicarse el presente pliego de cláusulas, prevalecerá el presente pliego de cláusulas.

Cláusula 5 Cláusula de incorporación

a) Cualquier entidad que no sea parte en el presente pliego de cláusulas podrá, previo consentimiento de todas las partes, adherirse al presente pliego de cláusulas en cualquier momento, ya sea como responsable o como encargado, cumplimentando los anexos y firmando el anexo I.

b) Una vez se hayan cumplimentado y firmado los anexos a que se refiere la letra a), la entidad que se adhiera será tratada como parte en el presente pliego de cláusulas y tendrá los derechos y obligaciones de un responsable o encargado, según la categoría en la que se haya inscrito en el anexo I.

c) La entidad que se adhiera no adquirirá derechos y obligaciones del presente pliego de cláusulas derivados del período anterior a la adhesión.

SECCIÓN II – OBLIGACIONES DE LAS PARTES

Cláusula 6 Descripción del tratamiento o tratamientos

En el anexo II se especifican los pormenores de las operaciones de tratamiento y, en particular, las categorías de datos personales y los fines para los que se tratan los datos personales por cuenta del responsable.

Cláusula 7 Obligaciones de las partes

7.1. Instrucciones

a) El encargado tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, salvo que esté obligado a ello en virtud del Derecho de la Unión o del Estado miembro que se aplique al encargado. En tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público. El responsable también podrá dar instrucciones ulteriores en cualquier momento del período de tratamiento de los datos personales. Dichas instrucciones deberán estar siempre documentadas.

b) El encargado informará inmediatamente al responsable si las instrucciones dadas por el responsable infringen, a juicio del encargado, el Reglamento (UE) 2016/679 o las disposiciones aplicables del Derecho de la Unión o de los Estados miembros en materia de protección de datos.

7.2. Limitación de la finalidad

El encargado tratará los datos personales únicamente para los fines específicos del tratamiento indicados en el anexo II, salvo cuando siga instrucciones adicionales del responsable.

7.3. Duración del tratamiento de datos personales

El tratamiento por parte del encargado solo se realizará durante el período especificado en el anexo II.

[1] Cláusulas contractuales tipo para responsables y encargados dentro de la UE/el EEE (europa.eu)

7.4. Seguridad del tratamiento

a) El encargado aplicará, como mínimo, las medidas técnicas y organizativas especificadas en el anexo III para garantizar la seguridad de los datos personales. Una de estas medidas podrá consistir en la protección contra violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados a dichos datos («violación de la seguridad de los datos personales»). A la hora de determinar un nivel adecuado de seguridad, las partes tendrán debidamente en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, y los riesgos que entraña el tratamiento para los interesados.

b) El encargado solo concederá acceso a los datos personales tratados a los miembros de su personal en la medida en que sea estrictamente necesario para la ejecución, la gestión y el seguimiento del contrato. El encargado garantizará que las personas autorizadas para tratar los datos personales recibidos se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.

7.5. Datos sensibles

Si el tratamiento afecta a datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos o 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, o datos relativos a condenas e infracciones penales («datos sensibles»), el encargado aplicará restricciones específicas y/o garantías adicionales.

7.6. Documentación y cumplimiento

a) Las partes deberán poder demostrar el cumplimiento del presente pliego de cláusulas.

b) El encargado resolverá con presteza y de forma adecuada las consultas del responsable relacionadas con el tratamiento con arreglo al presente pliego de cláusulas.

c) El encargado pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones contempladas en el presente pliego de cláusulas y que deriven directamente del Reglamento (UE) 2016/679. A instancia del responsable, el encargado permitirá y contribuirá a la realización de auditorías de las actividades de tratamiento cubiertas por el presente pliego de cláusulas, a intervalos razonables o si existen indicios de incumplimiento. Al decidir si se realiza un examen o una auditoría, el responsable podrá tener en cuenta las certificaciones pertinentes que obren en poder del encargado.

d) El responsable podrá optar por realizar la auditoría por sí mismo o autorizar a un auditor independiente. Las auditorías también podrán consistir en inspecciones de los locales o instalaciones físicas del encargado y, cuando proceda, realizarse con un preaviso razonable.

e) Las partes pondrán a disposición de las autoridades de control competentes, a instancia de estas, la información a que se refiere la presente cláusula y, en particular, los resultados de las auditorías.

7.7. Recurso a subencargados

a) **AUTORIZACIÓN GENERAL POR ESCRITO: El encargado cuenta con una autorización general del responsable para contratar a subencargados que figuren en la lista del anexo IV.** El encargado informará al responsable específicamente y por escrito de las adiciones o sustituciones de subencargados previstas en dicha lista con al menos 15 días de antelación, de modo que el responsable tenga tiempo suficiente para formular objeción a tales cambios antes de que se contrate al subencargado o subencargados de que se trate. El encargado del tratamiento proporcionará al responsable la información necesaria para que pueda ejercer su derecho a formular objeción.

b) Cuando el encargado contrate a un subencargado para llevar a cabo actividades de tratamiento específicas (por cuenta del responsable), lo hará por medio de un contrato que imponga al subencargado, en esencia, las mismas obligaciones en materia de protección de datos que las impuestas al encargado en virtud del presente pliego de cláusulas. El encargado se asegurará de que el subencargado cumpla las obligaciones a las que esté sujeto en virtud del presente pliego de cláusulas y del Reglamento (UE) 2016/679.

c) El encargado proporcionará al responsable, a instancia de este, una copia del contrato con el subencargado y de cualquier modificación posterior del mismo. En la medida en que sea necesario para proteger secretos comerciales u otro tipo de información confidencial, como datos personales, el encargado podrá expurgar el texto del contrato antes de compartir la copia.

d) El encargado seguirá siendo plenamente responsable ante el responsable del cumplimiento de las obligaciones que imponga al subencargado su contrato con el encargado. El encargado notificará al responsable los incumplimientos por parte del subencargado de las obligaciones que le atribuya dicho contrato.

e) El encargado pactará con el subencargado una cláusula de tercero beneficiario en virtud de la cual, en caso de que el encargado desaparezca de facto, cese de existir jurídicamente o sea insolvente, el responsable tendrá derecho a rescindir el contrato del subencargado y ordenar a este que suprima o devuelva los datos personales.

7.8. Transferencias internacionales

a) Las transferencias de datos a un tercer país o a una organización internacional por parte del encargado solo podrán realizarse siguiendo instrucciones documentadas del responsable o en virtud de una exigencia expresa del Derecho de la Unión o del Estado miembro al que esté sujeto el encargado; se llevarán a cabo de conformidad con el capítulo V del Reglamento (UE) 2016/679.

b) El responsable se aviene a que, cuando el encargado recurra a un subencargado de conformidad con la cláusula 7.7 para llevar a cabo actividades de tratamiento específicas (por cuenta del responsable) y dichas actividades conlleven una transferencia de datos personales en el sentido del capítulo V del Reglamento (UE) 2016/679, el encargado y el subencargado puedan garantizar el cumplimiento del capítulo V del Reglamento (UE) 2016/679 utilizando cláusulas contractuales tipo adoptadas por la Comisión, con arreglo al artículo 46, apartado 2, del Reglamento (UE) 2016/679, siempre que se cumplan las condiciones para la utilización de dichas cláusulas contractuales tipo.

Cláusula 8 Ayuda al responsable del tratamiento

a) El encargado notificará con presteza al responsable las solicitudes que reciba del interesado. No responderá a dicha solicitud por sí mismo, a menos que el responsable le haya autorizado a hacerlo.

b) El encargado ayudará al responsable a cumplir sus obligaciones al responder a las solicitudes de ejercicio de derechos de los interesados teniendo en cuenta la naturaleza del tratamiento. En el cumplimiento

de las obligaciones que le atribuyen las letras a) y b), el encargado cumplirá las instrucciones del responsable.

c) Además de la obligación del encargado de ayudar al responsable en virtud de la cláusula 8, letra b), el encargado también ayudará al responsable a garantizar el cumplimiento de las obligaciones siguientes teniendo en cuenta la naturaleza del tratamiento y la información de que disponga el encargado:

1) la obligación de realizar una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales («evaluación de impacto») cuando sea probable que un tipo de tratamiento suponga un alto riesgo para los derechos y libertades de las personas físicas;

2) la obligación de consultar a las autoridades de control competentes antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo;

3) la obligación de garantizar que los datos personales sean exactos y estén actualizados, informando sin demora al responsable si el encargado descubre que los datos personales que está tratando son inexactos o han quedado obsoletos;

4) las obligaciones contempladas en el artículo 32 del Reglamento (UE) 2016/679.

d) Las partes establecerán en el anexo III medidas técnicas y organizativas apropiadas que obliguen al encargado a ayudar al responsable a aplicar la presente cláusula, así como el objeto y el alcance de la ayuda requerida.

Cláusula 9 Notificación de violaciones de la seguridad de los datos personales

En caso de violación de la seguridad de los datos personales, el encargado colaborará con el responsable y le ayudará a cumplir las obligaciones que le atribuyen los artículos 33 y 34 del Reglamento (UE) 2016/679, en su caso, teniendo en cuenta la naturaleza del tratamiento y la información de que disponga el encargado.

9.1. Violación de la seguridad de datos personales tratados por el responsable

En caso de violación de la seguridad de los datos personales en relación con los datos tratados por el responsable, el encargado ayudará al responsable en lo siguiente.

a) Notificar la violación de la seguridad de los datos personales a las autoridades de control competentes sin dilación indebida una vez tenga constancia de ella, si procede (a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas).

b) Recabar la información siguiente, que, de conformidad con el artículo 33, apartado 3, del Reglamento (UE) 2016/679, deberá figurar en la notificación del responsable, que debe incluir como mínimo:

1) la naturaleza de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

2) las consecuencias probables de la violación de la seguridad de los datos personales;

3) las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Cuando y en la medida en que no se pueda proporcionar toda la información al mismo tiempo, en la notificación inicial se proporcionará la información de que se disponga en ese momento y, a medida que se vaya recabando, la información adicional se irá proporcionando sin dilación indebida.

c) Cumplir, con arreglo al artículo 34 del Reglamento (UE) 2016/679, la obligación de comunicar sin dilación indebida al interesado la violación de la seguridad de los datos personales cuando sea probable que la violación de la seguridad entrañe un alto riesgo para los derechos y libertades de las personas físicas.

9.2. Violación de la seguridad de datos personales tratados por el encargado

En caso de violación de la seguridad de datos personales tratados por el encargado, este lo notificará al responsable sin dilación indebida una vez que el encargado tenga constancia de ella. Dicha notificación deberá incluir como mínimo:

a) una descripción de la naturaleza de la violación de la seguridad (inclusive, cuando sea posible, las categorías y el número aproximado de interesados y de registros de datos afectados);

b) los datos de un punto de contacto en el que pueda obtenerse más información sobre la violación de la seguridad de los datos personales;

c) sus consecuencias probables y las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad, incluyendo las medidas adoptadas para mitigar los posibles efectos negativos.

Cuando y en la medida en que no se pueda proporcionar toda la información al mismo tiempo, en la notificación inicial se proporcionará la información de que se disponga en ese momento y, a medida que se vaya recabando, la información adicional se irá proporcionando sin dilación indebida.

Las partes establecerán en el anexo III los demás elementos que deberá aportar el encargado cuando ayude al responsable a cumplir las obligaciones que le atribuyen los **artículos 33 y 34 del Reglamento (UE) 2016/679**.

SECCIÓN III: DISPOSICIONES FINALES

Cláusula 10 Incumplimiento de las cláusulas y resolución del contrato

a) Sin perjuicio de lo dispuesto en el Reglamento (UE) 2016/679, en caso de que el encargado del tratamiento incumpla las obligaciones que le atribuye el presente pliego de cláusulas, el responsable podrá ordenar al encargado que suspenda el tratamiento de datos personales hasta que este vuelva a dar cumplimiento al presente pliego de cláusulas, o resolver el contrato. El encargado informará con presteza al responsable en caso de que no pueda dar cumplimiento al presente pliego de cláusulas por cualquier motivo.

b) El responsable estará facultado para resolver el contrato en lo que se refiera al tratamiento de datos personales en virtud del presente pliego de cláusulas cuando:

1) el tratamiento de datos personales por parte del encargado haya sido suspendido por el responsable con arreglo a la letra

a) y no se vuelva a dar cumplimiento al presente pliego de cláusulas en un plazo razonable y, en cualquier caso, en un plazo de un mes a contar desde la suspensión;

2) el encargado incumpla de manera sustancial o persistente el presente pliego de cláusulas o las obligaciones que le atribuye el Reglamento (UE) 2016/679;

3) el encargado incumpla una resolución vinculante de un órgano jurisdiccional competente o de las autoridades de control competentes en relación con las obligaciones que les atribuye el presente pliego de cláusulas, el Reglamento (UE) 2016/679.

c) El encargado estará facultado para resolver el contrato en lo que se refiera al tratamiento de datos personales en virtud del presente pliego de cláusulas cuando, tras haber informado al responsable de que sus instrucciones infringen los requisitos jurídicos exigidos por la cláusula 7.1, letra b), el responsable insiste en que se sigan dichas instrucciones.

d) Tras la resolución del contrato, el encargado suprimirá, a petición del responsable, todos los datos personales tratados por cuenta del responsable y acreditará al responsable que lo ha hecho, o devolverá todos los datos personales al responsable y suprimirá las copias existentes, a menos que el Derecho de la Unión o de los Estados miembros exija el almacenamiento de los datos personales. Hasta que se destruyan o devuelvan los datos, el encargado seguirá garantizando el cumplimiento con el presente pliego de cláusulas.

***

ANEXO I: LISTA DE PARTES

Responsable(s): EL CLIENTE DE LOS SERVICIOS DE IGX

En nombre del Responsable, las instrucciones al Encargado pueden proceder de:

a) El Médico que solicita la prueba
b) El responsable de protección de datos/gerente del responsable del tratamiento
c) Otras personas en función de lo acordado entre las partes

Persona de contacto: el responsable del tratamiento tiene la responsabilidad de facilitar al Encargado información sobre su persona de contacto

Firma y fecha de adhesión: El presente pliego de cláusulas forma parte integrante de las Condiciones Generales de los servicios genéticos de Igenomix. Así pues, las partes aceptan que al firmar el contrato correspondiente a las Condiciones Generales, firman también el presente pliego de cláusulas.

Encargado(s): IGENOMIX SPAIN LAB, S.L.U. sociedad constituida y organizada de conformidad con las leyes de España, Dirección: Calle Narcís Monturiol 11B, Edificio Europark, Parque Tecnológico de Paterna (46980), Valencia, España.

Nombre, cargo y datos de la persona de contacto: Data Protection Officer [Encargado de protección de datos] /privacy@igenomix.com

En nombre del Responsable, las instrucciones al Encargado pueden dirigirse a:

a) El correspondiente director de pruebas de Igenomix
b) El servicio de atención al cliente de Igenomix
c) El Data Protection Officer [Encargado de protección de datos

Firma y fecha de adhesión: El presente pliego de cláusulas forma parte integrante de las Condiciones Generales de los servicios genéticos de Igenomix. Así pues, las partes aceptan que al firmar el contrato correspondiente a las Condiciones Generales, firman también el presente pliego de cláusulas.

ANEXO II: DESCRIPCIÓN DEL TRATAMIENTO

1. ***Categorías de interesados cuyos datos personales se tratan***
   Pacientes del responsable del tratamiento
   Personal pertinente del responsable del tratamiento
2. ***Categorías de datos personales tratados***
   Sobre los pacientes:

a) Datos identificativos (nombre, fecha de nacimiento, teléfono, dirección de correo electrónico)
b) Datos sanitarios recogidos en los formularios TRF
c) Datos genéticos recogidos en los formularios TRF
d) Resultados de los análisis de las muestras biológicas de los pacientes
e) Otros datos que puedan ser necesarios para una prueba específica

Sobre el personal:

i. Nombre
ii. Dirección de correo electrónico
iii. Nombre de usuario y contraseña

3. ***Datos sensibles tratados (si procede) y restricciones o garantías aplicadas que tengan plenamente en cuenta la naturaleza de los datos y los riesgos que entrañan, como, por ejemplo, la limitación estricta de la finalidad, restricciones de acceso (incluido el acceso exclusivo del personal que haya hecho un curso especializado), un registro del acceso a los datos, restricciones a transferencias ulteriores o medidas de seguridad adicionales.***

a) limitación estricta de la finalidad
b) restricciones de acceso (incluido el acceso exclusivo del personal que haya seguido una formación especializada)
c) mantenimiento de un registro de acceso a los datos

4. ***Naturaleza del tratamiento***

El encargado del tratamiento realizará el análisis de la prueba genética en nombre del responsable del tratamiento en

función de la prueba genética solicitada por el responsable del tratamiento. Posible anonimización de datos personales con fines de investigación.

Etapas: 1) recogida de muestras 2)introducción de datos en el sistema ERP/LIMS de IGX 3) análisis de datos en la propia empresa, o en otra filial de IGX o por un tercero 4) el equipo de diagnóstico genera el informe 5) emisión del informe final al responsable del tratamiento a través del sistema ERP/LIMS de IGX 6) Potencial anonimización de los datos.

5. Finalidad(es) del tratamiento de los datos personales por cuenta del responsable del tratamiento

a) Los datos personales son tratados por el encargado del tratamiento en nombre del responsable del tratamiento para cumplir los servicios genéticos que el responsable, como cliente, encargó al encargado como proveedor de servicios.

b) El encargado no puede utilizar los datos personales recibidos del responsable para ningún otro fin y sólo de acuerdo con las instrucciones del responsable.

c) El encargado del tratamiento podrá anonimizar los datos personales de modo que no puedan ser atribuidos, directa o indirectamente, a ninguna persona. El encargado podrá utilizar los datos totalmente anonimizados con fines de investigación científica.

6. Duración del tratamiento

El tratamiento continuará mientras el responsable del tratamiento comparta los datos personales con el encargado del tratamiento con el fin de prestar los servicios que el responsable del tratamiento ha encargado al encargado del tratamiento y durante los periodos de conservación mencionados en el apartado 7 siguiente.

7. Supresión o devolución de datos personales

Cuando los datos ya no sean útiles o necesarios para los fines para los que fueron recogidos y tratados, o cuando se hayan cumplido y agotado dichos fines, los datos personales deberán ser suprimidos, siempre que no sea necesario bloquearlos para responder de posibles responsabilidades nacidas del tratamiento de datos personales y por el plazo de prescripción de dichas responsabilidades previsto en el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento.

En caso de tratamiento por parte de (sub)encargados, especifíquese también el objeto, la naturaleza y la duración del tratamiento

Para algunas pruebas, el encargado del tratamiento utiliza uno de los subencargados del tratamiento mencionados en el anexo 4 para la realización de las pruebas genéticas.

8. Para la transferencias a (sub)encargados, se aplican las siguientes medidas:

Pseudonimización de los datos transmitidos a los subencargados;

Control de acceso a los datos para que únicamente acceda a ellos quien estrictamente tenga la necesidad de conocerlos;

9. Descripción de las medidas de seguridad técnicas y organizativas concretas que aplicará el encargado del tratamiento para brindar asistencia al responsable:

a. El encargado del tratamiento podrá compartir el informe de las pruebas genéticas directamente con el paciente en un correo electrónico cifrado, una vez verificada la identidad de éste.

b. El encargado del tratamiento podrá revelar los datos en bruto del análisis de pruebas genéticas al responsable del tratamiento y al paciente previa solicitud y abono de los honorarios correspondientes.

ANEXO III: MEDIDAS TÉCNICAS Y ORGANIZATIVAS, EN ESPECIAL MEDIDAS TÉCNICAS Y ORGANIZATIVAS PARA GARANTIZAR LA SEGURIDAD DE LOS DATOS

Descripción de las medidas de seguridad técnicas y organizativas aplicadas por los encargados del tratamiento (inclusive las certificaciones pertinentes) para garantizar un nivel adecuado de seguridad, teniendo en cuenta la naturaleza, el alcance, el contexto y la finalidad del tratamiento, así como los riesgos para los derechos y libertades de las personas físicas.

Confidencialidad, integridad, disponibilidad y resistencia de los sistemas y servicios de tratamiento

1. Los empleados u otras personas que trabajan en el Encargado del tratamiento como afiliado del Grupo Vitrolife www.vitrolifegroup.com están sujetos a acuerdos de confidencialidad
2. Existen procedimientos que garantizan que las personas que tienen acceso a los datos personales disponen de una cuenta de acceso individual
3. El acceso a los datos personales se registrará
4. Los datos personales almacenados son objeto de copias de seguridad automáticas periódicas.
5. Se aplicarán procedimientos, políticas y planes para garantizar la integridad y disponibilidad permanentes, por ejemplo, un plan de continuidad de la actividad y de recuperación en caso de catástrofe que incluya un calendario
6. Plan de copias de seguridad para mantener copias de seguridad de los recursos de la empresa.

- Copia de seguridad diaria del mainframe con un tiempo de retención de 30 días.
- Copia de seguridad trimestral del mainframe con retención durante tres trimestres.
- Copia de seguridad anual del mainframe con retención durante 2 años.

7. Las copias de seguridad están protegidas mediante seguridad física o cifrado AES de 256 bits
8. Sistema de monitorización de accesos no autorizados (o intentos de acceso) a los dispositivos y sistemas del Grupo Vitrolife, por ejemplo, un cortafuegos.

Seguridad de los datos

9. Protección de punto final en ordenadores, portátiles y servidores.
10. Tráfico y comportamiento del punto final mediante alertas de protección del punto final.
11. La supervisión de los dispositivos (hardware y software) se mantiene actualizada, incluida la activación de la actualización automática en los dispositivos para los sistemas operativos instalados actualmente
12. Tráfico de red a través de cortafuegos.
13. Procedimiento definido de violación de datos personales e incidentes de datos.
14. Parches críticos automatizados y actualizaciones de aplicaciones críticas definidas.
15. Detección de comportamientos y patrones desviados.
16. Detección de anomalías con escaneo continuo y alertas sobre el dispositivo, servicio y aplicaciones gestionadas y el comportamiento del usuario.
17. Cobertura de vulnerabilidades recién descubiertas.

Identificación y autorización de los usuarios

18. Sólo podrán acceder a los datos personales las personas identificadas y autorizadas mediante el registro del acceso a los datos personales para su trazabilidad
19. Política de contraseñas que garantice que sólo las personas identificadas y autorizadas tengan acceso a los datos personales.
20. Todos los datos y dispositivos estarán protegidos por una contraseña segura, autenticación multifactor (MFA) u otras configuraciones de seguridad
21. Acceso restringido al ordenador local.
22. Limitar y controlar el uso de programas de utilidades privilegiadas o cualquier software que requiera privilegios administrativos para ejecutarse
23. El acceso sólo se concede previa aprobación del responsable más cercano y del responsable de TI.
24. Sincronización de archivos offline encriptados en discos duros locales
25. Análisis de seguridad continuo con externalización central y socios de cooperación.

Protección de datos durante la transmisión y el almacenamiento

26. Durante la transmisión y el almacenamiento se utiliza el cifrado AES de 256 bits
27. Los servidores que almacenan datos personales almacenados electrónicamente se encuentran en las instalaciones
28. Deben existir copias de seguridad automáticas (cuando los datos se almacenan electrónicamente)
29. Los documentos físicos se almacenan en los locales del encargado del tratamiento (salvo acuerdo en contrario con el responsable del tratamiento)
30. Los documentos físicos se almacenan en condiciones no expuestas a incendios, robos, etc.
31. Sólo acceden a los datos personales almacenados las personas identificadas y autorizadas, y el acceso debe quedar registrado El acceso requiere una contraseña, MFA (o una tarjeta llave si los datos se almacenan físicamente en armarios).

Seguridad física de los lugares en los que se tratan datos personales

32. Sólo las personas identificadas y autorizadas tienen acceso a los locales en los que se procesan y/o almacenan los datos personales
33. Las oficinas, armarios, ordenadores portátiles, etc. que contengan datos personales deben estar protegidos, por ejemplo, mediante una cerradura o un código de acceso. Los datos personales deben guardarse bajo llave después de las horas de trabajo
34. La(s) sala(s) de servidores, incluidos los equipos, cables, etc., deben estar protegidos con medidas físicas suficientes

Detección de amenazas, vulnerabilidad y gestión de incidentes

35. Identificación de los dispositivos conectados a la red.
36. Agentes de evaluación de riesgos: para identificar vulnerabilidades en la aplicación o servicio del dispositivo.

37. Escaneo continuo de vulnerabilidades: de dispositivo, aplicación y servicios.
38. Revisión de seguridad de terceros y prueba de penetración.
39. Marco de gobernanza informática para hacer cumplir las normas de seguridad a proveedores, contratistas y otros no empleados (por ejemplo, acuerdos de confidencialidad, protección de datos, etc.).
40. Procedimiento definido de violación de datos personales e incidentes de datos.
41. El análisis posterior a los incidentes conduce a una mejora continua del marco y los procedimientos.

Organización

42. Departamento de TI centralizado con plena responsabilidad sobre las aplicaciones comunes del Grupo y todos los equipos de TI propiedad del entorno de TI del Grupo o conectados a él.
43. El director de TI del Grupo Vitrolife aprueba todas las aplicaciones, servicios e implementación de equipos y su conexión con el entorno de TI.
44. La seguridad de TI es gestionada, aprobada y establecida por el departamento de TI del Grupo Vitrolife.

Políticas para empleados

45. Formación de concienciación para todos los empleados y otras personas que trabajen con tratamiento de datos que cubra la seguridad informática y/o el tratamiento de datos (concienciación sobre la privacidad).
46. Existe una política documentada de contraseñas seguras a disposición de los usuarios.

Trabajo a distancia

47. Los dispositivos, software, etc. utilizados para el trabajo a distancia están protegidos de la misma forma y se aplican las mismas medidas que para el procesamiento que tiene lugar en las instalaciones del Grupo Vitrolife.

Continuidad del negocio y plan de recuperación de desastres

48. El Encargado del tratamiento dispondrá de un plan de continuidad de la actividad y de recuperación en caso de catástrofe que incluya un calendario.
49. El Encargado del tratamiento dispondrá de un plan de acción y un procedimiento de comunicación en caso de violación de la seguridad de los datos y/o de un incidente que afecte a la continuidad de la actividad.

ANEXO IV: LISTA DE SUBENCARGADOS DEL TRATAMIENTO

El responsable del tratamiento ha autorizado al encargado del tratamiento a contratar subencargados de la siguiente lista de subencargados:

Nombre del subencargado	Información de contacto	Objeto	Base jurídica para la transferencia de datos
ABACID 2007, SL	C/ Oña, 28050 Madrid. CIF / NIF: B-85194199 Teléfono: (+34) 917 567 878 Correo electrónico: atencionalcliente@mail.abacid.es Correo electrónico	Realizar cierta parte de las pruebas solicitadas por el cliente (Cariotipo)	Contrato de encargado del tratamiento

	DPD: **dpo@mail.abacid.es** Sitio web: **www.abacid.es**		
BLUE HEALTHCARE, S.L.,	Avenida de Alberto Alcocer, 7, 28036 Madrid	Ofrecer asesoramiento genético posterior	Contrato de encargado del tratamiento
Igenomix FZ, LLC	26th Street, Building 40 - Unit 501 & 502, Dubai HealtCare City, Dubái, EAU privacy@igenomix.com	Realizar las pruebas solicitadas por el cliente (CGT Bank, CGT Plus, CGT Exome y CGT One – subcontratado parcialmente)	Contrato de transferencia de datos del Grupo
IGENOMIX ITALIA S.R.L. a	Italia Via Enrico Fermi 1, Marostica (36063), Vicenza, Italia	Realizar las pruebas solicitadas por el cliente (CGT Essential)	Contrato de transferencia de datos del Grupo