Contrato de tratamiento de datos

Contrato TD

entre

_____

_____

_____

_____

_____

_____

Página(s) web de Jimdo:

- **El responsable del contrato** / El usuario de Jimdo -

-

y

Jimdo GmbH
Stresemannstr. 375
22761 Hamburg
Germany

-

El **encargado del contrato** / "***Jimdo***"

-

Preámbulo

El responsable del tratamiento sabe que Jimdo ofrece sus servicios a una gran cantidad de clientes. Por ello, el presente contrato limita la posibilidad del responsable del tratamiento de dar instrucciones adicionales que perjudiquen a los servicios que Jimdo presta a otros clientes o usuarios. Jimdo no podría operar si tuviera en cuenta una gran cantidad de instrucciones de los clientes.

1. Disposiciones generales

1.1. Además de prestar sus servicios al cliente, Jimdo también procesa datos personales por encargo del cliente. Por voluntad de las partes, este contrato contiene el encargo escrito del tratamiento de datos por encargo en virtud del § 11 de la Ley alemana de protección de datos (BDSG, por sus siglas en alemán) y el contrato en virtud del Art. 28 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos - RGPD), y regula los derechos y obligaciones de las partes en relación con el tratamiento de datos.

1.2. Cuando en este contrato se emplee el término “tratamiento de datos” o “tratamiento” (de datos), se hará referencia a la definición de “tratamiento” en virtud del Art. 4, punto 2 del RGPD.

1.3. Cuando en el presente contrato se haga mención de la BDSG (Ley alemana de protección de datos), las menciones solo se tendrán en cuenta hasta el 24/5/2018. A partir del 25/5/2018, las menciones harán siempre referencia al RGPD en este contrato.

2. Objeto del contrato

2.1. Jimdo presta un servicio en línea con el que los usuarios de Jimdo, en calidad de clientes, pueden crear y gestionar una página web de Jimdo por sí mismos. El servicio prestado permite a los usuarios ajustar el diseño de sus páginas de Jimdo con autonomía, configurar contenidos propios y gestionar una tienda. Por lo demás, el objeto del encargo se desprende de la relación contractual principal celebrada entre las partes. Esta se basa en las CGC de Jimdo, que se integran de manera efectiva en la relación contractual entre las partes.

2.2. El presente contrato para el tratamiento de datos por encargo completa las CGC de Jimdo.

2.3. Los siguientes tipos de datos suelen ser objeto del tratamiento:

- Datos de clientes del cliente
  - Nombre, dirección
  - Datos de pedidos
  - en caso de una tienda de Jimdo: Datos de pagos (sin embargo, estos solo los almacenará el encargado del tratamiento de pagos)

- Datos de uso de los visitantes de la página web de Jimdo del cliente
  - Jimdo utiliza varios servicios de análisis de uso (por ejemplo, Google Analytics) para elaborar estadísticas para los usuarios de Jimdo, como por ejemplo, el cliente; pero también para evaluar y optimizar las ofertas de Jimdo periódicamente.

- Datos de contenido que los visitantes de las páginas web del responsable del tratamiento publican en las mismas (por ejemplo, en comentarios, libros de visitas y formularios).

- Datos de comunicación o mensajes de correo electrónico que se envían a través del encargado del tratamiento de correo electrónico Rackspace Limited. Cuando una página web de Jimdo nos comunica una cuenta de correo electrónico o un redireccionamiento de correo electrónico, Jimdo le entregará una cuenta de Rackspace Limited para usuarios de Jimdo. Rackspace Limited se ocupará de enviar y administrar correos electrónicos por encargo de Jimdo.

Los tipos de datos indicados con anterioridad son datos que suelen tratarse cuando se utilizan servicios de Jimdo. Los tipos de datos pueden variar dependiendo de los servicios de Jimdo utilizados por el responsable del tratamiento y pueden ser ampliados si Jimdo lo considera oportuno. Si los tipos de datos difieren de la lista indicada con anterioridad, los tipos de datos específicos se estipularán en un anexo separado al presente contrato. En ese caso, el responsable del tratamiento puede ponerse en contacto con Jimdo (privacy@jimdo.com) y enumerar los tipos de datos que difieren o solicitar un anexo separado. Jimdo procurará que siempre se cumplan las bases jurídicas aplicables al recabado, al tratamiento y al uso de datos personales, siempre y cuando ello recaiga en el alcance de la responsabilidad de Jimdo. El responsable del tratamiento es el único responsable de comprobar que está autorizado a tratar datos de contenido (por ejemplo, de formularios empleados por el cliente) u otros datos cuyo tratamiento ha iniciado el propio responsable del tratamiento en el contexto del uso de sus páginas web.

2.4. Afectados por el tratamiento de datos:

- Clientes del cliente
- Interesados o visitantes de la página web del cliente
- Empleados del cliente

3. Derechos, derechos de instrucción y obligaciones del cliente

3.1. El responsable del tratamiento es el responsable, en virtud del Art. 4, punto 7 del RGPD, de tratar datos por encargo del proveedor. Conforme a la cláusula 4, apartado 5, el encargado del tratamiento tiene derecho a advertir al responsable del tratamiento en caso de que, en su opinión, el objeto del encargo o de una instrucción concreta sea un tratamiento de datos no autorizado por las leyes. En caso de que el encargado del tratamiento pueda alegar que un tratamiento por instrucción del responsable del tratamiento puede acarrear la responsabilidad del encargado del tratamiento en virtud del Art. 82 del RGPD, el encargado del tratamiento se reserva el derecho a suspender el tratamiento hasta que se aclare la cuestión de la responsabilidad entre las partes.

3.2. Como responsable, el responsable del tratamiento es el encargado de salvaguardar los derechos de los afectados. Deberán tenerse en cuenta los derechos de los afectados frente al cliente. El encargado del tratamiento informará al responsable del tratamiento inmediatamente en caso de que los afectados ejerzan sus derechos frente al responsable del tratamiento y ello afecte directamente al cliente.

3.3. El responsable del tratamiento puede impartir instrucciones adicionales a Jimdo en relación con el tratamiento de datos personales. El responsable del tratamiento puede dar dichas instrucciones, principalmente, en su área de administración, a través de la configuración de los servicios. Por ejemplo, puede configurar los análisis web. El resto de instrucciones adicionales deberá enviarse en formato textual (por ejemplo, por correo electrónico) a Jimdo. A continuación, Jimdo comprobará la viabilidad de las instrucciones teniendo en cuenta los intereses y la operabilidad de los servicios de Jimdo para todos los clientes, y le comunicará al responsable del tratamiento los costes de la instrucción concreta. Después de una declaración de aceptación de costes, se llevará a cabo la instrucción impartida. Ello no afecta a las disposiciones relativas a una posible remuneración de gastos adicionales que surjan de instrucciones adicionales del responsable del tratamiento al proveedor.

3.4. El responsable del tratamiento puede nombrar personas autorizadas para dar instrucciones en el área de administración de su página de Jimdo o publicar su dirección de correo electrónico. En caso de que cambien las personas autorizadas para dar instrucciones del cliente, el responsable del tratamiento se lo comunicará al encargado del tratamiento en formato textual o modificando las direcciones de correo electrónico publicadas en el área de administración de Jimdo.

3.5. El responsable del tratamiento informará al encargado del tratamiento de inmediato en caso de que constate errores o irregularidades en relación con el tratamiento de datos personales por parte del proveedor.

3.6. En caso de que el responsable del tratamiento tenga una obligación de información a terceros en virtud de los Arts. 33 y 34 del RGPD u otras obligaciones legales de comunicación, el responsable del tratamiento será el responsable de su cumplimiento.

4. Obligaciones generales del proveedor

4.1. El encargado del tratamiento tratará datos personales exclusivamente en el marco de los acuerdos pactados o en cumplimiento de las instrucciones adicionales impartidas por el cliente, de haberlas. De ello se excluyen las normas legales que, en su caso, obligan al encargado del tratamiento a llevar a cabo un tratamiento distinto. En ese caso, el encargado del tratamiento le comunicará al responsable del tratamiento dichas exigencias legales antes del tratamiento, siempre y cuando el Derecho aplicable no prohíba dicha comunicación en aras del interés público. Por lo demás, el objeto, el tipo y el alcance del tratamiento de datos toman como base exclusivamente el presente contrato o las instrucciones del cliente. El encargado del tratamiento tiene prohibido llevar a cabo un tratamiento de datos que difiera de lo aquí estipulado, salvo que el responsable del tratamiento lo haya aceptado por escrito.

4.2. Jimdo procurará que el tratamiento de datos se limite al marco de la prestación de servicios conforme al contrato principal en su ámbito de responsabilidad, que incluye a los subcontratistas conforme a la Cláusula 6 del presente Contrato, de conformidad con las disposiciones del presente Contrato.

4.3. Jimdo está obligada a que el tratamiento de datos, en caso de que difiera de la cláusula 4.1, se produzca por encargo directo del cliente, solo en Estados miembros de la Unión Europea (UE) o del Espacio Económico Europeo (EEE) o, en caso de que el tratamiento de datos se produzca en un tercer país, a adoptar las disposiciones que permitan un tratamiento válido conforme al Art. 46 del RGPD.

4.4. Jimdo está obligada a que su empresa y sus procesos operativos funcionen de forma que los datos que trata por encargo del responsable del tratamiento tengan la suficiente seguridad y estén protegidos contra el acceso no autorizado de terceros. Si Jimdo acomete cambios significativos para la seguridad de los datos en su organización del tratamiento de datos por encargo, se lo comunicará al responsable del tratamiento previamente.

4.5. Jimdo informará al responsable del tratamiento inmediatamente en caso de que una instrucción impartida por el cliente, en su criterio, incumpla normativas legales. El encargado del tratamiento tiene derecho a suspender la instrucción afectada hasta que el responsable del tratamiento la confirme o la modifique. En caso de que el encargado del tratamiento pueda alegar que un tratamiento por instrucción del responsable del tratamiento puede acarrear la responsabilidad del encargado del tratamiento en virtud del Art. 82 del RGPD, el encargado del tratamiento se reserva el derecho a suspender el tratamiento hasta que se aclare la cuestión de la responsabilidad entre las partes.

4.6. El tratamiento de datos por encargo del responsable del tratamiento fuera de los Estados en los que opera el encargado del tratamiento o sus subcontratistas solo está autorizado con el consentimiento escrito del cliente. El tratamiento de datos en nombre del responsable del tratamiento en viviendas particulares solo está autorizado con el consentimiento escrito del responsable del tratamiento en cada caso concreto.

4.7. Jimdo tratará los datos que trate por encargo del responsable del tratamiento separados del resto de datos. No es obligatorio que se produzca una separación física. Jimdo identificará adecuadamente los datos que trate por encargo del cliente. En caso de que los datos se traten con distintos fines, Jimdo identificará los datos con su fin específico.

4.8. Jimdo puede (aunque no está obligado a ello) comunicarle al responsable del tratamiento la(s) persona(s) autorizadas a recibir instrucciones del cliente. En caso de que cambien las personas autorizadas a recibir instrucciones de la empresa del proveedor, el encargado del tratamiento se lo comunicará al responsable del tratamiento por escrito.

5. Responsable de protección de datos del proveedor

Jimdo ha nombrado a un responsable de protección de datos externo conforme al Art. 37 del RGPD. Se trata de:

B³ | Informationstechnologie Andreas Bethke
Papenbergallee 34
25548 Kellinghusen
Alemania
Correo electrónico: privacy@jimdo.com

6. Obligaciones de notificación del proveedor

6.1. Jimdo está obligada a comunicarle al responsable del tratamiento inmediatamente todos los incumplimientos de las normativas de protección de datos o de los acuerdos contractuales o de las instrucciones impartidas por el cliente, cuando estos se hayan producido durante el tratamiento de datos por parte de ella u otras personas que se ocupan del tratamiento. Lo mismo se aplicará a la violación de la protección de datos personales que el encargado del tratamiento trata por encargo del cliente.

6.2. Por añadidura, Jimdo informará al responsable del tratamiento inmediatamente en caso de que una autoridad supervisora en virtud del Art. 58 del RGPD actúe contra Jimdo y ello pueda conllevar una auditoría del tratamiento que Jimdo lleva a cabo por encargo del cliente.

6.3. Jimdo es consciente de que el responsable del tratamiento puede tener una obligación de notificación conforme a los Arts. 33 y 34 del RGPD, que contempla una notificación a la autoridad supervisora en el plazo de 72 horas tras la puesta en conocimiento. El encargado del tratamiento ayudará al responsable del tratamiento a cumplir con sus obligaciones de notificación. En concreto, el encargado del tratamiento comunicará por escrito (fax o correo electrónico) al responsable del tratamiento todo acceso no autorizado a los datos personales que trata por encargo del responsable del tratamiento de inmediato, en un plazo máximo de 48 horas desde que tenga conocimiento del acceso. La notificación del encargado del tratamiento al responsable del tratamiento debe contener, sobre todo, la siguiente información:

- una descripción del tipo de violación de la protección de datos personales, en la medida de lo posible indicando las categorías y la cifra aproximada de personas afectadas, las categorías afectadas y la cifra aproximada de paquetes de datos personales afectados;

- una descripción de las medidas adoptadas o propuestas por el encargado del tratamiento para subsanar la violación de la protección de datos personales y, en su caso, las medidas adoptadas para la mitigación de posibles consecuencias adversas.

7. Obligación de participación activa del proveedor

7.1. Jimdo ayudará al responsable del tratamiento a cumplir su obligación de responder a las solicitudes relacionadas con el ejercicio de los derechos de los afectados en virtud de los Arts. 12-23 del RGPD. Se aplicará lo estipulado en la Cláusula 11 del presente contrato.

7.2. Cuando el responsable del tratamiento deba elaborar listas de procedimientos o listas de actividades de tratamiento, Jimdo deberá colaborar activamente. Deberá comunicarle al responsable del tratamiento los datos necesarios en cada caso de forma apropiada.

7.3. El encargado del tratamiento ayudará al cliente, teniendo en cuenta el tipo de tratamiento y la información que obre en su poder, a la hora de cumplir las obligaciones estipuladas en los Arts. 32-36 del RGPD.

8. Facultades de supervisión

8.1. Para que el responsable del tratamiento pueda ejercer sus derechos y obligaciones de supervisión antes y durante la relación contractual, Jimdo le proporcionará al cliente, previa solicitud, un informe de los encargados externos de la protección de datos de Jimdo en cuanto a las medidas técnicas y organizativas adoptadas en Jimdo y en los centros informáticos utilizados por Jimdo. Dicho informe se actualizará, como máximo, cada 24 meses.

8.2. Si tiene preguntas, el responsable del tratamiento puede ponerse en contacto con los encargados externos de la protección de datos de Jimdo.

8.3. El responsable del tratamiento tiene derecho a comprobar en cualquier momento que Jimdo está cumpliendo las normativas de protección de datos o las disposiciones contractuales acordadas entre las partes o las instrucciones del responsable del tratamiento en el alcance necesario.

8.4. Jimdo está obligada a informar al responsable del tratamiento en caso de que ello sea necesario para la realización de las comprobaciones en virtud del apartado 8.3.

8.5. El responsable del tratamiento puede exigir una comprobación visual de los datos tratados por Jimdo por encargo del cliente, así como de los sistemas y programas de tratamiento de datos empleados.

8.6. Con previo aviso comunicado con un plazo razonable (mínimo diez días laborables), el responsable del tratamiento puede realizar una auditoría en virtud del apartado 8.5 en las instalaciones de la empresa Jimdo GmbH, en los horarios comerciales habituales. Al hacerlo, el responsable del tratamiento procurará que las auditorías se limiten al alcance necesario para no perturbar de manera desproporcionada los procesos operativos del encargado del tratamiento con sus comprobaciones. En principio, los gastos de una inspección se limitan a un día por año natural para el proveedor. El responsable del tratamiento está obligado a tratar con confidencialidad la información confidencial interna del encargado del tratamiento adquirida en el marco de dichas comprobaciones o por otros motivos, sobre todo los detalles relativos a las medidas técnicas y organizativas, a no revelarlas a terceros ni hacerlas accesibles a terceros, siempre y cuando ello no se produzca con los fines de los servicios contratados entre el responsable del tratamiento y el proveedor.

8.7. En caso de que las autoridades supervisoras tomen medidas contra el responsable del tratamiento en virtud del Art. 58 del RGPD, sobre todo en materia de obligaciones de información y auditoría, Jimdo estará obligada a comunicarle al responsable del tratamiento la información necesaria y a facilitarles a las autoridades supervisoras competentes auditorías físicas. El responsable del tratamiento deberá informar al encargado del tratamiento de las medidas previstas en este sentido.

8.8. El responsable del tratamiento tiene derecho a realizar las auditorías por medio de auditores nombrados por él por escrito como mínimo diez días antes de cada auditoría concreta, siempre y cuando el encargado del tratamiento consienta dicha auditoría externa. El encargado del tratamiento no se negará a otorgar su consentimiento sin motivos. El encargado del tratamiento tiene derecho a rechazar al auditor, sobre todo, si el auditor tiene una relación de competencia con el proveedor. Los auditores externos están obligados a celebrar un contrato de confidencialidad escrito con el encargado del tratamiento y solo podrán llevar a cabo la auditoría cuando lo hayan firmado. Todo ello no afecta a las facultades de inspección del cliente.

9. Subcontratistas

9.1. Para prestar sus servicios a los usuarios de su empresa, Jimdo puede contratar subcontratistas para llevar a cabo labores que también pueden abarcar el tratamiento de datos personales. Jimdo enumerará todos los subcontratistas que ya han sido contratados a la firma del contrato en el "Anexo 1" del mismo. El cambio de subcontratistas o la contratación de nuevos subcontratistas está permitida según las condiciones estipuladas en el apartado 9.4.

9.2. Jimdo debe seleccionar a los subcontratistas diligentemente y comprobar, antes de su contratación, que pueda cumplir los acuerdos celebrados entre el responsable del tratamiento y Jimdo. Sobre todo, Jimdo debe comprobar antes de contratarlos y a lo largo de la duración del contrato, que los subcontratistas hayan adoptado las medidas técnicas y organizativas necesarias para la protección de datos personales en virtud del Art. 32 del RGPD. Jimdo documentará los resultados de dichas comprobaciones y se los comunicará al responsable del tratamiento previa solicitud.

9.3. Jimdo está obligada a obtener una confirmación del subcontratista de que este ha nombrado a un delegado de protección de datos en su empresa conforme al Art. 37 del RGPD. En caso de que el subcontratista no haya nombrado a un delegado de protección de datos, Jimdo deberá advertir de ello al responsable del tratamiento y aportar información que demuestre que el subcontratista no está obligado por ley a nombrar a un delegado de protección de datos. Jimdo deberá garantizar que las normas estipuladas en el presente contrato también sean aplicables a los subcontratistas. Jimdo deberá comprobar el cumplimiento de estas obligaciones periódicamente.

9.4. En caso de que se prevea un cambio de subcontratista o la contratación de un nuevo subcontratista, Jimdo deberá informar al responsable del tratamiento por escrito con la suficiente antelación, como muy tarde cuatro semanas antes del cambio o la nueva contratación ("Información"). El responsable del tratamiento tiene derecho a oponerse al cambio o a la nueva contratación de un subcontratista indicando los motivos por escrito en el plazo de tres semanas a partir de la recepción de la "Información". El responsable del tratamiento podrá cancelar su oposición en cualquier momento por escrito. En caso de oposición, el encargado del tratamiento podrá rescindir la relación contractual con el responsable del tratamiento en un plazo mínimo de 14 días antes de que finalice un mes natural. A la hora de fijar el plazo de rescisión, el encargado del tratamiento tendrá en cuenta los intereses del responsable del tratamiento en una medida razonable. Si el responsable del tratamiento no se opone en el plazo de tres semanas tras la recepción de la "Información", se considerará que el responsable del tratamiento ha aceptado el cambio o la nueva contratación del subcontratista en cuestión.

9.5. Jimdo debe garantizar que las disposiciones acordados en el presente contrato y las instrucciones adicionales del cliente, de haberlas, también sean aplicables a los subcontratistas. Jimdo deberá comprobar el cumplimiento de estas obligaciones periódicamente.

9.6. Jimdo debe celebrar con el subcontratista un contrato de tratamiento de datos por encargo que cumpla los requisitos del Art. 28 del RGPD. Además, Jimdo deberá acordar con el subcontratista las mismas obligaciones de protección de datos que han fijado el responsable del tratamiento y Jimdo. Deberá entregarse al responsable del tratamiento un duplicado del contrato de tratamiento de datos por encargo si este lo solicita.

9.7. Sobre todo, Jimdo está obligado a garantizar por medio de normas contractuales que las facultades de supervisión (Cláusula 8 del presente contrato) del responsable del tratamiento y de las autoridades supervisoras también se apliquen al subcontratista y que se acuerden derechos de inspección con el responsable del tratamiento y las autoridades supervisoras. Además, deberá acordarse por contrato que el subcontratista permita dichas inspecciones y posibles auditorías físicas.

9.8. Los servicios de terceros que el encargado del tratamiento utilice como meros servicios adicionales para ejercer su actividad comercial no se considerarán subcontratas en los términos de los párrafos 9.1 - 9.7. Entre ellos se incluyen, por ejemplo, los servicios de limpieza, los servicios de comunicación

sin una relación concreta con los servicios que el encargado del tratamiento presta al cliente, los servicios postales y de mensajería, los servicios de transporte y los servicios de vigilancia. En lo relativo a los servicios adicionales prestados por terceros, el encargado del tratamiento también está obligado a procurar que se adopten las medidas preventivas técnicas y organizativas necesarias para garantizar la protección de los datos personales. El mantenimiento de los sistemas informáticos o las aplicaciones constituyen una subcontrata y un tratamiento por encargo sujeto a consentimiento en virtud del Art. 28 del RGPD, en caso de que el mantenimiento y la inspección afecte a sistemas informáticos que también se utilizan en relación con la prestación de servicios al responsable del tratamiento y en cuyo mantenimiento se puede acceder a datos personales que se tratan por encargo del cliente.

10. Obligación de confidencialidad

10.1. A la hora de tratar datos por encargo del cliente, Jimdo está obligado a tratar con confidencialidad los datos que recibe o de los que tiene conocimiento en el marco del encargo.

10.2. Jimdo garantiza que conoce las normativas de protección de datos aplicables y que está familiarizado con su aplicación. Jimdo también garantiza que informa a los empleados que se ocupan de estas labores acerca de las disposiciones de protección de datos aplicables a los mismos y les obliga a tratarlos con confidencialidad en virtud del RGPD y del secreto informático en virtud del § 53 de la Ley alemana de protección de datos (nueva).

10.3. Si este lo solicita, se debe demostrar al responsable del tratamiento la obligación de los empleados en los términos del párrafo 2.

11. Ejercicio de derechos de los afectados

11.1. El responsable del tratamiento es el único responsable del ejercicio de derechos de los afectados. Los derechos de los afectados deben ejercerse frente al cliente. Jimdo está obligada a ayudar al responsable del tratamiento a cumplir su obligación de tramitar solicitudes de los afectados conforme a los Arts. 12-23 del RGPD, siempre y cuando el responsable del tratamiento no pueda satisfacer las reclamaciones sin la participación activa de la empresa Jimdo GmbH. Al hacerlo, Jimdo deberá prestar especial atención a que la información necesaria se entregue al responsable del tratamiento lo antes posible para que este pueda cumplir, sobre todo, las obligaciones que estipula el Art. 12, sec. 3 del RGPD.

11.2. En caso de que el responsable del tratamiento necesite la participación activa del encargado del tratamiento para posibilitar el ejercicio de los derechos de los afectados (sobre todo de información, rectificación, bloqueo o eliminación), el encargado del tratamiento adoptará las medidas necesarias conforme a las instrucciones del cliente. En la medida de lo posible, el encargado del tratamiento ayudará al responsable del tratamiento a cumplir su obligación de responder a las solicitudes de ejercicio de derechos de los afectados adoptando medidas técnicas y organizativas adecuadas.

11.3. Ello no afectará a las normas relativas a una posible remuneración por gastos adicionales derivados de la participación activa del encargado del tratamiento en relación con el ejercicio de derechos de los afectados del cliente.

12. Obligaciones de confidencialidad

12.1. Las dos partes están obligadas a tratar con confidencialidad toda la información relacionada con la ejecución del presente contrato sin limitaciones temporales y a utilizarla exclusivamente para la ejecución del contrato. Ninguna de las partes tiene derecho a utilizar dicha información, total o parcialmente, con fines ajenos a los aquí estipulados ni a poner dicha información a disposición de terceros.

12.2. La obligación que antecede no se aplicará si una de las partes puede demostrar que ha recibido información de terceros sin estar obligado a tratarla con confidencialidad o que es de conocimiento público.

13. Remuneración

13.1. La remuneración del encargado del tratamiento se acordará por separado.

14. Medidas técnicas y organizativas para garantizar la seguridad de los datos

14.1. Jimdo se compromete frente al responsable del tratamiento a adoptar las medidas técnicas y organizativas necesarias para cumplir las normativas de protección de datos aplicables. Ello incluye, principalmente, las normas estipuladas en el Art. 32 del RGPD.

14.2. El estado de la técnica y las medidas organizativas existentes en el momento de celebrar el contrato se adjuntan como Anexo 2 al presente contrato. Las partes están de acuerdo en que será necesario realizar modificaciones en las medidas técnicas y organizativas para adaptarse a la coyuntura técnica y jurídica. Jimdo acordará previamente con el responsable del tratamiento las modificaciones sustanciales que puedan afectar a la integridad, a la confidencialidad o a la disponibilidad de los datos personales. Jimdo podrá implantar medidas que conlleven meramente cambios técnicos y organizativos insignificantes y que no afecten negativamente a la integridad, a la confidencialidad y a la disponibilidad de los datos personales sin el consentimiento previo del cliente. El responsable del tratamiento puede exigir, una vez al año o en ocasiones justificadas, un informe actual sobre las medidas técnicas y organizativas adoptadas por Jimdo.

14.3. Jimdo comprobará, periódicamente y cuando las circunstancias lo exijan, la eficacia de las medidas técnicas y organizativas adoptadas. En caso de que exista una necesidad de optimización o modificación, Jimdo informará al cliente.

15. Duración del encargo

15.1. El contrato comenzará con su firma y seguirá vigente mientras lo haga el contrato principal preexistente entre las partes, relativo al uso de los servicios del proveedor. Puede rescindirse con un plazo de un mes antes de que finalice la duración correspondiente. La rescisión debe producirse por escrito.

15.2. El responsable del tratamiento puede rescindir el contrato en cualquier momento, sin cumplir plazo alguno, en caso de que Jimdo GmbH incumpla gravemente las normativas de protección de datos aplicables o las obligaciones del presente contrato, en caso de que Jimdo no pueda ejecutar una instrucción del responsable del tratamiento o en caso de que Jimdo niegue el acceso al responsable del tratamiento o a las autoridades supervisoras competentes de manera que incumpla el contrato.

16. Finalización

16.1. Tras la finalización del contrato, Jimdo deberá, según prefiera el cliente, devolverle a este o eliminar todos los documentos, los datos y los resultados derivados de su tratamiento y uso que obren en su poder en relación con el encargo contratado. La eliminación deberá documentarse debidamente. Ello no afectará a las posibles obligaciones legales de conservación de datos u otras obligaciones de bloqueo de los mismos. Por cuanto respecta a los soportes de datos, deberán destruirse en caso de que el responsable del tratamiento desee la eliminación, respetando como mínimo el nivel de seguridad 3 de la norma DIN 66399; deberá demostrarse la destrucción frente al responsable del tratamiento tal y como estipula el nivel de seguridad de la norma DIN 66399.

16.2. El responsable del tratamiento tiene derecho a supervisar la devolución y la eliminación completa de los datos conforme al contrato por parte del proveedor. Ello puede producirse en forma de visualización física de las instalaciones de tratamiento de datos en la empresa del proveedor. El responsable del tratamiento deberá anunciar la inspección física con un plazo razonable.

17. Derecho de retención

17.1. Las partes acuerdan renunciar al derecho de retención del encargado del tratamiento en virtud del Art. 273 del Código Civil alemán por cuanto respecta a los datos tratados y los correspondientes soportes de datos.

18. Disposiciones finales

18.1. En caso de que la propiedad que el responsable del tratamiento tiene depositada en el encargado del tratamiento se vea amenazada por acciones de terceros (por ejemplo, por embargo o confiscación), por un procedimiento concursal o por otros eventos, el encargado del tratamiento deberá informar al responsable del tratamiento de inmediato. El encargado del tratamiento informará de inmediato al acreedor de que se trata de datos tratados por encargo.

18.2. Todo acuerdo adicional deberá celebrarse por escrito.

18.3. En caso de que partes del presente contrato sean inválidas, ello no afectará a la validez del resto de disposiciones del contrato.

18.4. En caso de divergencias entre una traducción y el original, prevalecerá la formulación en idioma alemán.

19. Firma

_____ _____

Lugar, fecha - El Responsable del tratamiento -

Hamburg, 11.05.2018 - El **encargado del tratamiento**/Jimdo -

Matthias Henze

(CEO)

Dennis Manzke

(Head of Finance and Administration)

_____

Lugar, fecha

Anexo 1 - Subcontratistas

Para el tratamiento de datos por encargo del cliente, el encargado del tratamiento utiliza servicios de terceros que tratan datos por encargo del encargado del tratamiento (“subcontratistas”).

Infraestructura / plataforma técnica			
Mandrill	Newsletters y notificaciones.	Mailchimp by The Rocket Science Group, LLC, 675 Ponce de Leon Ave NE, Suite 5000, Atlanta, GA 30308, USA	Opt-Out im Newsletter,https://mailchimp.com/legal/privacy/
SendGrid	Newsletters y notificaciones.	SendGrid Inc., 1801 California St #500, Denver, CO 80202, USA	https://sendgrid.com/policies/privacy/
Google Tag Manager	La herramienta Tag Manager es un dominio sin cookies y no recopila información de identificación personal. La herramienta activa otras etiquetas, que pueden recopilar datos".	Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	https://www.google.com/analytics/tag-manager/use-policy/
Google Analytics	Herramienta para el análisis web.	Google LLC, 1600, Amphitheatre Parkway, Mountain View, CA 94043, USA	Browser Plugin, Opt-Out https://tools.google.com/dlpage/gaoptout?hl=en/
Adobe Image Editor	Edición de imágenes en el menú del usuario	Adobe Systems Incorporated, 345 Park Avenue, San Jose, CA 95110-2704, USA	http://www.adobe.com/privacy.html
Firebase	Firebase es una base datos en tiempo real que utilizamos para el almacenamiento e intercambio de datos en tiempo real (por ejemplo, para nuestras aplicaciones). Todos los datos de los usuarios son anonimizados antes de su transferencia a Firebase.	Firebase is a Google subsidiary and is based in San Francisco (CA), USA.	https://www.firebase.com/terms/privacy-policy.html
Sipgate	Edición de imágenes.	sipgate GmbH Gladbacher Straße 74 40219 Düsseldorf Deutschland	https://www.sipgate.de/datenschutz.html
Rackspace	Aplicación web para la gestión de servicios de correo y cuentas de correo electrónico.	Rackspace US Inc., Rackspace, 1 Fanatical Place, City of Windcrest, San Antonio, TX 78218, USA	https://www.rackspace.com/de-de/information/legal/privacystatement
SiftScience	Herramienta para la detección de fraude.	Sift Science, Inc., 123 Mission Street, 20th Floor, San Francisco, CA 94105	https://siftscience.com/service-privacy
Stripe	Plataforma de pagos.	Stripe Inc.,185 Berry Street, Suite 550, San Francisco, CA 94107, USA	https://stripe.com/de/privacy
Global Collect	Plataforma de pagos.	Global Collect Service B.V., Planetenweg 43 - 59, 2132 HM Hoofddorp, NL	http://www.globalcollect.com/Privacy

Zuora	Gestión de suscripciones.	Zuora Inc., 3050 S. Delaware Street, Suite 301, San Mateo, CA 94403, USA	https://www.zuora.com/privacy-statement/
Add This	Servicio para añadir páginas web a favoritos.	AddThis Inc., Oracle America Inc.,1595 Spring Hill Rd, Suite 300, Vienna, VA 22182, USA	http://www.addthis.com/privacy https://www.oracle.com/legal/privacy/index.html
fabric.io	Informes sobre incidencias.	Fabric is a Google Inc. subsidiary and is based in San Francisco (CA), USA.	https://fabric.io/terms?locale=en-us&utm_campaign=fabric-marketing&utm_medium=natural
InternetX	Gestión de dominios.	InterNetX GmbH, Maximilianstr. 6, 93047 Regensburg, Germany	https://www.internetx.com/rechtliches/datenschutz/
RankingCoach	Asistente para el posicionamiento en motores de búsqueda.	rankingCoach GmbH, Brügelmannstrasse 3, 50679 Köln, Germany	https://www.rankingcoach.com/en-us/privacy-policy
status.io	Página de estado con información actualizada sobre la accesibilidad y la funcionalidad de nuestro sistema	T3CH.com LLC, 19 N. County Line Road, Jackson, NJ 08527, USA	https://status.io/privacy
Paypal	encargado del tratamiento de pagos	PayPal (Europe) S.à r.l. et Cie, S.C.A., 22-24 Boulevard Royal, 2449 Luxembourg	https://www.paypal.com/de/webapps/mpp/ua/privacy-full?locale.x=de_DE
wpengine	Sistema de gestión de contenidos para blogs.	WP Engine Irongate House, 22-30 Duke's Place London, EC3A 7LP United Kingdom	https://wpengine.com/legal/privacy/
Fastly Inc.	Entrega de contenidos	Fastly, Inc., General Counsel, 475 Brannan St, Suite 300, San Francisco, CA 94107, USA	https://www.fastly.com/privacy
Disqus	Sistema de comentarios.	DISQUS, Inc., 301 Howard St, Floor 3, San Francisco, California 94105, USA	https://help.disqus.com/terms-and-policies/disqus-privacy-policy
G-Suite	Uso de los sistemas de productividad de Google con el sistema de correo electrónico Jimdo"	Un producto de Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	https://policies.google.com/privacy?hl=de
Twyla	Sistema de soporte de chat	Twyla GmbH, Winterfeldtstraße 21, 10781 Berlin, Germany	https://www.twylahelps.com/
Zendesk	Sistema de tickets para el soporte al usuario.	Zendesk, Inc., 1019 Market Street, San Francisco, CA 94103, USA	https://www.zendesk.de/company/customers-partners/#privacy-policy
Launchdarkly	Usamos los Feature Flags of LaunchDarkly para nuestro Internal Flighting-Systeme	Catamorphic, Co. ("LaunchDarkly"), 405 14th Street, Oakland, CA 94612, USA	https://launchdarkly.com/policies/privacy/
Facebook Login	Tecnología Single-Sign-On	Facebook Inc., 1 Hacker Way, Menlo Park, CA 94025, USA	https://www.facebook.com/about/privacy/
Google Plus Login	Tecnología Single-Sign-On	Un producto de Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	https://www.google.de/intl/de/policies/privacy/
Youtube	Función de inserción de Youtube para mostrar y reproducir videos del proveedor" "Youtube"	Un producto de Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	https://www.google.de/intl/de/policies/privacy
Prefinery	Herramienta para la adquisición de clientes y publicaciones de productos	Prefinery, 1108 Lavaca Street, Suite 110-318, Austin, TX 78701, USA	https://www.prefinery.com/privacy
Redis	encargado del tratamiento de banco de datos	Redislabs, 700 E El Camino Real Suite 250, Mountain View, CA 94040	https://redislabs.com/privacy/

sentry.io	Informes sobre incidencias.	Un producto de Functional Software, Inc., 132 Hawthorne St, San Francisco, CA 94107	https://sentry.io/privacy
Name.com	Gestión de dominios.	Name.com Inc., 414 14th Street #200, Denver, Colorado 80202, USA	http://www.name.com/media/policies/privacy-policy.pdf
Amazon Web Services	DNS, código Javascript, archivos de hoja de estilo	Amazon Web Services, Germany GmbH, Krausenstr. 38, 10117 Berlin, Germany	https://aws.amazon.com/de/privacy/?nc1=f_pr
Herramientas internas:			
Jira	Resolución de problemas y documentación	Atlassian, 55 Broadway Floot 17&25 New York, NY 10006 USA	https://www.atlassian.com/legal/privacy-policy
Slack	Solución de comunicaciones internas	436 Lafayette Street, 1008 Western Ave #401, Seattle, WA 98104	https://slack.com/intl/de-de/privacy-policy
Trello	Herramienta interna de planificación y comunicaciones	Atlassian, 55 Broadway Floot 17&25 New York, NY 10006 USA	https://trello.com/privacy
Tableau	Herramienta para el análisis de datos y registros de datos	Tableau Germany GmbH, An der Welle 4, 60322 Frankfurt am Main, Germany	https://www.tableau.com/de-de/privacy
Github	Servicio en línea para proyectos de desarrollo de software	Github, 88 Colin P Kelly Jr St, San Francisco, CA 94107, USA	https://help.github.com/articles/github-privacy-statement/
Microsoft	Uso interno de Microsoft Office y Skype	Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA	https://privacy.microsoft.com/en-us/privacystatement
Hootsuite	Herramienta de redes sociales	Hootsuite Media Inc. 5, East 8th Avenue, Vancouver BC, Canada V5T 1R6	https://hootsuite.com/de/legal/privacy
Performance und Marketing:			
Facebook Pixel & Custom Audiences	En el caso de consentimiento explícito, esto puede rastrear el comportamiento de los usuarios después de haber visto o hecho clic en un anuncio de Facebook. Este proceso está diseñado para evaluar la efectividad de los anuncios de Facebook con fines estadísticos y de investigación de mercado y puede ayudar a optimizar los esfuerzos publicitarios futuros.	Facebook Inc., 1 Hacker Way, Menlo Park, CA 94025, USA	https://www.facebook.com/about/privacy/
Hotjar	Optimización de conversión	Hotjar Ltd., Level 2, St Julian's Business Centre, 3, Elia Zammit Street, St Julian's STJ 1000, Malta	https://www.hotjar.com/legal/compliance/opt-out
Taboola	Plataforma de recomendación de contenido	Taboola, Inc., 28 West 23rd Street, 5th Floor, New York, NY 10010, USA	https://www.taboola.com/privacy-policy

Tv-Squared	Este sitio web utiliza TVSquared para el análisis estadístico del tráfico de los visitantes en relación con la publicidad televisiva	TV Squared Limited, Codebase, Argyle House, 3 Lady Lawson St, Edinburgh, EH3 9DR	http://tvsquared.com/privacy-policy/
bunchbox	Herramienta de optimización del sitio para la implementación de pruebas A / B y análisis multivariables	app.bunchbox.co, Peaks & Pies GmbH, Raboisen 30, 20095 Hamburg, Deutschland	http://peaksandpies.com
smartly.io	Herramienta para campañas publicitarias para Facebook e Instagram	SMARTLY.IO SOLUTIONS OY, Elielinaukio 2 G, 00100 Helsinki, Finland	https://cdn2.hubspot.net/hubfs/1570479/Privacy%20Policy/Smartly.io%20Privacy%20Policy.pdf
Zoho	Base de datos de promociones de Jimdo Pages	Zoho Corp B.V., Hoogoorddreef 15, 1101BA, Amsterdam, NL	https://www.zoho.eu/privacy.html
Fullstory	Fullstory registra el comportamiento de los usuarios en nuestro sitio web. Las grabaciones de los visitantes permiten que Jimdo los analice y luego mejore la experiencia del visitante. Fullstory almacena y recopila datos de forma anónima mediante cookies. Seguimiento (es decir, la recopilación de datos generados por la cookie) y relacionado con el uso del sitio web) se puede desactivar en cualquier momento. Siga las instrucciones en https://www.fullstory.com/optout.	Fullstory Inc., 818 Marietta Street, Atlanta, GA 30318, USA	https://www.fullstory.com/legal/privacy/
Surveymonkey	Para encuestas usamos los servicios de SurveyMonkey	SurveyMonkey Europe UC, 2 Shelbourne Buildings, Second Floor, Shelbourne Rd, Ballsbridge, Dublin 4, Ireland	https://de.surveymonkey.com/mp/policy/privacy-policy/
Trustpilot	Opiniones de los usuarios	Trustpilot A/S, Pilestræde 58, 5, 1112 Kopenhagen, Dänemark – de.trustpilot.com	http://legal.trustpilot.de/end-user-privacy-terms
Bing	Mercadeo en línea (Ad Words)	Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA	http://choice.microsoft.com/de-de/opt-out

Anexo 2 - Medidas técnicas y organizativas del proveedor

El encargado del tratamiento adopta las siguientes medidas técnicas y organizativas para garantizar la seguridad de los datos en virtud del Art. 32 del RGPD.

El encargado del tratamiento (encargado del tratamiento del contrato de tratamiento de datos por encargo) debe adoptar las medidas técnicas y organizativas necesarias para el tratamiento por encargo teniendo en cuenta el estado de la técnica, los costes de implementación, el tipo, el alcance, las circunstancias y los fines del tratamiento, así como la probabilidad y la gravedad de los peligros a los que se exponen los bienes jurídicos de las personas afectadas debido al tratamiento, para garantizar un nivel de protección adecuado al riesgo a la hora de tratar (por encargo) datos personales.

Las siguientes medidas, que se corresponden con el catálogo del § 64 del RGPD (2017), son medidas necesarias en el marco del tratamiento por encargo. Por motivos de seguridad, a continuación se indica únicamente una descripción general.

1. Confidencialidad

1.1 Controles de acceso

Se han adoptado las siguientes medidas para impedir un acceso no autorizado a las instalaciones de tratamiento de datos con las que se tratan o utilizan datos personales (controles de acceso):

- Las oficinas de Jimdo GmbH se encuentran en un edificio de oficinas de Hamburgo y los accesos a las oficinas de Jimdo GmbH están cerrados día y noche. Solo tienen acceso al edificio de oficinas los arrendadores y los arrendatarios de las oficinas. Las oficinas y las instalaciones comerciales de Jimdo están aseguradas por medio de un sistema de cierre electrónico. Solo las personas autorizadas tienen la llave electrónica necesaria. Por lo general, en las oficinas de Jimdo no se almacenan datos personales por encargo del cliente. Todos los sistemas informáticos empleados en relación con el encargo se ubican en centros informáticos que Jimdo utiliza.
- Jimdo procura que solo se utilicen centros informáticos que cumplan los requisitos de seguridad de datos vigentes en la República Federal de Alemania.
- Los centros informáticos utilizados por Jimdo están certificado conforme a ISO 27001 y cuentan con mecanismos y medidas de control de acceso suficientemente equipados. El centro informático utilizado para los datos del responsable del tratamiento cumple las exigencias del estándar Tier 3.
- La entrega de llaves y la gestión de llaves se basa en un proceso definido que regula la concesión y la retirada de autorizaciones de acceso a las salas tanto al comienzo de una relación laboral como a su fin.
- Las autorizaciones de acceso no se otorgan a los empleados hasta que no lo solicitan los superiores o el departamento de Recursos Humanos. A la hora de conceder autorizaciones se tiene en cuenta el principio de necesidad.
- Los visitantes no obtienen un acceso a las oficinas hasta que la recepción abre la puerta. La recepción tiene la puerta de entrada a la vista y procura que todo visitante se registre en la recepción.
- Todo visitante se registra en un libro de visitas y, a continuación, el recepcionista le acompaña hasta la persona con la que tiene previsto reunirse. Los empleados de Jimdo supervisan constantemente el acceso de los visitantes. Hay normas para el personal externo y el acompañamiento de invitados.

- Las entradas y ventanas de las oficinas de Jimdo GmbH están protegidas por una instalación de alarma. Esta puede activarse y desactivarse manualmente. Independientemente de ello, la instalación de alarma se activa automáticamente todos los días a las 21 horas.

1.2 Controles de acceso

Se han adoptado las siguientes medidas para impedir el uso de los sistemas de tratamiento de datos (ordenadores) por terceros no autorizados:

- Para obtener un acceso a los sistemas informáticos, los usuarios deben disponer de la correspondiente autorización de acceso. Para ello, los administradores conceden las correspondientes autorizaciones de usuario. Pero eso solo se produce cuando el supervisor del empleado en cuestión los solicita. La solicitud puede presentarse a través del departamento de Recursos Humanos.
- En ese caso, el usuario obtiene un nombre de usuario y una contraseña inicial que deberá cambiar la primera vez que inicie sesión. Las normas aplicables a las contraseñan incluyen una longitud mínima de 8 caracteres; además, la contraseña debe contar con mayúsculas y minúsculas, cifras y caracteres especiales.
- Las contraseñas se cambian cada 90 días. La única excepción son las contraseñas que disponen de una longitud mínima de 32 caracteres. En ese caso, no se recomienda un cambio de contraseña automático.
- Se guarda un historial de contraseñas. De esta forma, se garantiza que las últimas 10 contraseñas no puedan volver a utilizarse.
- Se registran los intentos fallidos de inicio de sesión. En caso de que se introduzca la contraseña erróneamente tres veces, se bloquea la cuenta de usuario en cuestión.
- Los accesos remotos a los sistemas informáticos de Jimdo GmbH siempre se producen a través de conexiones cifradas.
- Los servidores de Jimdo GmbH cuentan con un sistema de prevención de intrusiones. Todos los sistemas de servidores y clientes disponen de software antivirus, con el que se garantiza una actualización diaria de las firmas de virus.
- Todos los servidores están protegidos con un cortafuegos que se mantiene constantemente y se amplía con actualizaciones y parches.
- El acceso de servidores y clientes a Internet y el acceso a estos sistemas a través de Internet también está protegido por cortafuegos. De esta forma, se garantiza que solo estén habilitados los puertos necesarios para la comunicación. El resto de puertos está debidamente bloqueado.
- Todos los empleados tienen la orden de bloquear sus sistemas informáticos cuando los abandonan.
- Por lo general, las contraseñas se guardan cifradas.

1.3 Controles de acceso

Se han adoptado las siguientes medidas que garantizan que el personal autorizado para el uso de un sistema de tratamiento de datos solo pueda acceder a los datos para los que tiene autorización de acceso, y que los datos personales no se puedan leer, copiar, modificar o eliminar sin autorización durante el tratamiento, el uso y después del almacenamiento.
El responsable del tratamiento es el responsable de someter a un control de acceso adecuado los datos en los discos de almacenamiento/espacio web que se le cede contractualmente mientras dure el contrato; sobre todo, deberá garantizar que solo accedan a los mismos terceros autorizados (por ejemplo, agencias web, administradores).

- Las autorizaciones para los sistemas informáticos y aplicaciones de Jimdo GmbH las crean exclusivamente los administradores.
- Por lo general, las autorizaciones se conceden en base al principio “need to know”. Por ello, solo obtendrán un derecho de acceso a datos, bases de datos o aplicaciones las personas que mantengan y procesen dichos datos, aplicaciones o bases de datos o participen en su desarrollo.

- El requisito para ello es que un superior del empleado solicite la autorización para este. La solicitud también puede presentarla el “Office Team”.
- Se registrarán todos los accesos a los sistemas informáticos para detectar e impedir los usos no autorizados.
- Existe un programa de autorización basado en roles con la posibilidad de realizar una concesión diferenciada de autorizaciones de acceso, lo cual garantiza que los empleados obtengan derechos de acceso a las aplicaciones y los datos únicamente en función de su ámbito de actividad y, en su caso, del proyecto en el que participan.
- La destrucción de los soportes de datos y documentos en papel se producirá a través de un encargado del tratamiento de servicios que garantice una destrucción que cumpla las exigencias de la norma DIN 66399.
- Todos los empleados de Jimdo GmbH tienen la orden de depositar toda la información que contenga datos personales o información sobre proyectos en los contenedores designados para la destrucción.
- Por lo general, los empleados tienen prohibido instalar software no autorizado en los sistemas informáticos.
- Todos los sistemas de servidores y clientes se actualizan periódicamente con actualizaciones de seguridad.

1.4 Separación

Las siguientes medidas garantizan que puedan tratarse los datos por separado en función de los distintos fines para los que han sido recabados:

- Todos los sistemas informáticos que Jimdo utiliza para el responsable del tratamiento disponen de una separación lógica de clientes que garantiza una separación de los datos respecto a los datos que se tratan con otros fines.
- Se produce un tratamiento o almacenamiento separado de los datos que tienen distintos fines de tratamiento.
- Los empleados del departamento de Técnica (Administración), Soporte, Administración de dominios y Contabilidad de clientes han creado un sistema de autorizaciones con autorizaciones de acceso escalonadas.
- El responsable del tratamiento es el responsable de la separación de los datos personales en los discos de almacenamiento y los sistemas modulares que se le ceden.

1.5 Seudonimización y cifrado

Las siguientes medidas garantizan que el tratamiento de datos personales se produzca de manera que los datos, sin añadir información adicional, ya no se puedan asignar a una persona afectada específica, siempre y cuando dicha información adicional se almacene por separado y se adopten las medidas técnicas y organizativas necesarias.

- El responsable del tratamiento es el responsable de la seudonimización de los datos personales en los sistemas modulares o en el espacio web que se le cede, siempre y cuando las leyes lo exijan.
- El responsable del tratamiento es el responsable de cifrar mediante técnicas adecuadas (software) los datos de los sistemas modulares o el espacio de almacenamiento que se le cede por contrato a lo largo de la duración del mismo.
- Por lo general, el acceso administrativo a los sistemas de servidores se producirá a través de conexiones cifradas.
- Además, los datos de los sistemas de servidores y clientes se almacenarán en soportes de datos cifrados. Con estos fines se emplean sistemas de cifrado de discos duros.

2. Integridad

2.1 Control de introducción de datos

Con las siguientes medidas se puede comprobar y determinar a posteriori *si se introducen, modifican o eliminan datos personales en los sistemas de tratamiento de datos y quién lleva a cabo dichas acciones:*

- La introducción, modificación y eliminación de datos se registrará en las bases de datos.
- El responsable del tratamiento es el responsable de introducir los datos personales, de haberlos, en los sistemas modulares que se le ceden por contrato a lo largo de la duración del mismo y de contratar únicamente terceros adecuados a estos fines (por ejemplo, agencias web, administradores). Por lo general, los empleados del encargado del tratamiento no podrán acceder a dichos datos ni introducir, modificar o eliminar datos.
- Por tanto, normalmente es el responsable del tratamiento el que trata los datos personales, de manera que los encargados del tratamiento no puedan comprobar y determinar *a posteriori* qué datos personales introduce o modifica el cliente, en qué momento y en qué sistema de tratamiento automático.
- En el ejercicio de su actividad, el encargado del tratamiento solo llevará a cabo un registro de dichos datos y dichas modificaciones en caso de que se le imparta una instrucción adicional por escrito y fuera del área de administración de la página web, y lo hará en un alcance adecuado, documentando la hora y las personas que introducen los datos.
- En caso de que el encargado del tratamiento (Jimdo) deba eliminar información por motivos legales o bloquear el acceso a la misma (por ejemplo, en caso de uso por parte de clientes en los sistemas informáticos de servicios telemáticos o de comunicación electrónica de terceros), se llevará a cabo un registro del bloqueo o la eliminación de contenidos. Los datos de los registros se almacenarán y contendrán la identificación del empleado. La eliminación se producirá automáticamente cuando finalice el contrato y se llevará a cabo un registro de la misma.

2.2 Control de transmisión de datos

Las siguientes medidas garantizan que los datos personales no puedan leerlos, copiarlos, modificarlos o eliminarlos personas no autorizadas durante su transmisión electrónica o durante su transporte o almacenamiento en soportes de datos, y que pueda verificarse y determinarse a qué órganos pueden transmitirse o se han transmitido datos personales utilizando instalaciones de transmisión de datos.

- Para administrar los servidores se emplearán únicamente conexiones cifradas. Por lo general, no se producirá una transmisión de datos del cliente. La única excepción son los casos en los que Jimdo esté obligada a entregar datos por exigencias legales o por orden judicial.
- Por lo demás, la transmisión de datos que se almacenen en los sistemas informáticos de Jimdo por encargo del responsable del tratamiento solo se producirá en el contexto de las actividades previstas por el responsable del tratamiento en relación con su presencia en Internet (acceso a las páginas web por parte de visitantes de las páginas web) en el alcance técnico necesario en cada caso.
- La confidencialidad de la transmisión de datos personales se garantiza por medio de cifrados SSL/TSL a través de las páginas web del encargado del tratamiento.
- Todos los empleados que trabajen en un proyecto del responsable del tratamiento obtendrán formación en cuanto al uso autorizado de datos y las modalidades de transmisión de datos.
- En la medida de lo posible, los datos se transmitirán cifrados a su receptor.
- Los empleados de Jimdo GmbH tienen prohibido utilizar soportes de datos privados en los proyectos de los clientes.
- Los empleados de Jimdo GmbH obtienen formación periódica en materia de protección de datos. Todos los empleados están obligados a tratar los datos personales con confidencialidad.

- Por lo demás, el responsable del tratamiento es el responsable de que los datos de los sistemas modulares o espacios de almacenamiento que se le ceden por contrato se sometan a un control de transporte adecuado y técnicas de cifrado apropiadas a lo largo de la duración del contrato.

3. Disponibilidad y resistencia

Las siguientes medidas garantizan que los sistemas de tratamiento de los datos empleados funcionen siempre sin complicaciones y que los datos personales estén protegidos contra una destrucción o una pérdida accidentales.

- Los centros informáticos que emplea Jimdo disponen del siguiente suministro de energía ininterrumpido (SEI), aire acondicionado en las salas de servidores, dispositivos de supervisión de la temperatura y la humedad en las salas de servidores, alarmas de incendio y humos, sistemas de alarma y seguridad.
- Hay un sistema antiincendios y un sistema de alarma temprana exhaustivos. Los datos de los sistemas de servidores de Jimdo GmbH se aseguran incrementalmente cada día y “por completo” una vez a la semana. Lo medios de aseguramiento se aplican de manera cifrada en un lugar separado físicamente.
- La reproducción de copias de seguridad se prueba con regularidad.
- Los sistemas informáticos disponen de un suministro de energía ininterrumpido. En la sala de servidores hay una alarma antiincendios y un sistema de extinción de CO2. Todos los sistemas de servidores se someten a una monitorización que, en caso de avería, envía una notificación inmediata al administrador.
- En la empresa Jimdo GmbH hay un plan de emergencias que también incluye un plan de reinicio.
- Los datos de los sistemas de servidores de Jimdo GmbH se aseguran incrementalmente a diario y “por completo” una vez a la semana. Lo medios de aseguramiento se aplican de manera cifrada en un lugar separado físicamente.
- La reproducción de copias de seguridad se prueba con regularidad.
- Los sistemas informáticos disponen de un suministro de energía ininterrumpido. En la sala de servidores hay una alarma antiincendios y un sistema de extinción de CO2. Todos los sistemas de servidores se someten a una monitorización que, en caso de avería, envía una notificación inmediata al administrador.

4. Procedimientos de comprobación, valoración y evaluación periódicas

Objetivo de la garantía: procedimientos de comprobación, valoración y evaluación periódicas de la eficacia de las medidas técnicas y organizativas para garantizar un tratamiento que proteja los datos.

4.1 Gestión de la protección de datos

- Jimdo cuenta con un núcleo consolidado de empleados técnicos de larga duración con experiencia y destrezas técnicas en materia de seguridad de datos.
- Los empleados obtienen formación periódica.
- En Jimdo GmbH se implementa una gestión de la seguridad de datos. Hay una normativa de protección y seguridad de datos y directrices con las que se garantiza la implantación de los objetivos de la normativa.
- Hay un equipo de protección de datos y seguridad informática (DST) que planifica, implanta, evalúa y modifica las medidas en materia de protección y seguridad de datos.
- Las directrices se evalúan y se modifican periódicamente en cuanto a su eficacia.
- Sobre todo, se garantiza que todos los empleados sepan reconocer las incidencias relacionadas con la protección de datos y notificarlas inmediatamente al DST. Este investigará la incidencia de

inmediato. En caso de que se vean afectados datos tratados por encargo del cliente, se procurará informar al mismo inmediatamente acerca del tipo y el alcance de la incidencia.

- En el tratamiento de datos con fines propios, en caso de que se den los requisitos del Art. 33 del RGPD, se notificará a la autoridad supervisora en el plazo de 72 horas desde que se tenga conocimiento de la incidencia.

4.2 Controles contratados (subcontratación de terceros)

Las siguientes medidas garantizan que los datos personales que se tratan por encargo solo puedan tratarse conforme a las instrucciones del cliente.

- Jimdo GmbH cuenta con un delegado de protección de datos en su empresa.
- En caso de contratación de proveedores de servicios externos, se celebrará un contrato de tratamiento por encargo conforme a las leyes de protección de datos aplicables, previa auditoría del delegado de protección de datos de Jimdo GmbH. Los proveedores también serán supervisados periódicamente durante la relación contractual.

4.3 Protección de datos mediante instalaciones técnicas y configuraciones previas que favorezcan la protección de datos

- En Jimdo GmbH, a la hora de desarrollar software, se procura cumplir el principio de necesidad en relación con las interfaces de usuario. Por ello, por ejemplo, los campos de los formularios y las pantallas pueden configurarse con flexibilidad. De este modo, pueden crearse campos obligatorios o desactivarse campos.
- El software de Jimdo GmbH soporta el control de entradas por medio de un Audit-Trail flexible y ajustable que permite un almacenamiento inalterable de las modificaciones efectuadas en los datos y permisos de usuarios.
- Los permisos para acceder a los datos o aplicaciones pueden fijarse de manera flexible y granular.

- Proveedor/Jimdo -