Acuerdo de Tratamiento de Datos (ATD)

Data Processing Agreement (DPA)

1. Preámbulo aufinity Group GmbH (en adelante, «el Encargado del tratamiento») procesa datos personales en nombre del Cliente (en adelante, «el Responsable del tratamiento») de conformidad con el Art. 28 del Reglamento General de Protección de Datos (en adelante, «RGPD») y en cumplimiento de sus obligaciones contractuales de conformidad con sus Condiciones Generales y las respectivas Órdenes de Pedido suscritas (en adelante, conjuntamente, el «Acuerdo Principal»). El presente Acuerdo de Tratamiento de Datos (en lo sucesivo, «ATD») especifica las obligaciones de protección de datos de las Partes en relación con el Acuerdo Principal.	**1. Preamble** The aufinity Group GmbH (hereinafter "Processor") processes personal data on behalf of the Client (hereinafter "Controller") in accordance with Art. 28 of the General Data Protection Regulation (hereinafter "GDPR") and in fulfillment of its contractual obligations in accordance with its General Terms and Conditions and the respective Order Forms concluded (hereinafter together "Main Agreement"). This Data Processing Agreement (hereinafter "DPA") specifies the data protection obligations of the Parties in connection with the Main Agreement.
2. Ámbito del tratamiento 2.1. El objeto y la duración, la naturaleza y los fines del tratamiento, el tipo de datos personales y las categorías de interesados figuran en el **Anexo 1**. 2.2. La vigencia del presente ATD se basa en la del Acuerdo Principal. El derecho a una rescisión extraordinaria no se ve afectado por ello.	**2. Scope of the Processing** 2.1. The subject matter and duration, nature and purposes of the processing, the type of personal data and the categories of data subjects are set out in **Annex 1**. 2.2. The term of this DPA is based on the term of the Main Agreement. The right to extraordinary termination remains unaffected by this.

3. Autoridad de instrucción 3.1. El Encargado del tratamiento trata los datos personales exclusivamente con arreglo a las instrucciones del Responsable del tratamiento. Las instrucciones se establecen en la presente ATD y pueden ser modificadas, completadas o sustituidas por el Responsable mediante instrucciones individuales en forma de texto. Tanto el Responsable como el Encargado del tratamiento deben documentar las instrucciones del Responsable. 3.2. Si el Responsable del tratamiento emite instrucciones individuales que van más allá del alcance de los servicios acordados contractualmente, los costes resultantes correrán a cargo del Responsable del tratamiento, a menos que sean necesarios para evitar o subsanar infracciones legales en el ámbito de responsabilidad del Encargado del tratamiento. 3.3. Cuando la legislación de la Unión o de los Estados miembros a la que esté sujeto el Encargado del tratamiento le exija tratar datos personales al margen de las instrucciones del Responsable del tratamiento, el Encargado notificará al Responsable del tratamiento dichos requisitos legales antes del tratamiento, a menos que la legislación en cuestión prohíba dicha notificación por motivos de interés público importante. En este último caso, el Encargado del tratamiento informará al Responsable sin dilación indebida tan pronto como sea legalmente posible. 3.4. El Encargado del tratamiento informará al Responsable del tratamiento sin demora indebida si considera que una instrucción infringe la legislación aplicable. El Encargado del tratamiento podrá suspender la ejecución de la instrucción hasta que haya sido confirmada o modificada por el Responsable del tratamiento.	**3. Instruction Authority** 3.1. The Processor processes personal data exclusively in accordance with the instructions of the Controller. The instructions are set out in this DPA and may be amended, supplemented or replaced by the Controller by means of individual instructions in text form. The instructions issued by the Controller must be documented by both the Controller and the Processor. 3.2. If the Controller issues individual instructions that go beyond the contractually agreed scope of services, the resulting costs shall be borne by the Controller, unless they are necessary to prevent or remedy legal violations in the Processor's area of responsibility. 3.3. Where the Processor is required by Union or Member State law to which the Processor is subject to process personal data outside the instructions of the Controller, the Processor shall notify the Controller of such legal requirements before processing, unless the law in question prohibits such notification on grounds of important public interest. In the latter case, the Processor will inform the Controller without undue delay as soon as legally possible. 3.4. The Processor shall inform the Controller without undue delay if it considers that an instruction violates applicable laws. The Processor may suspend the implementation of the Instruction until it has been confirmed or amended by the Controller.
4. Confidencialidad El Encargado del tratamiento garantiza que las personas autorizadas a tratar datos personales se han comprometido a mantener la confidencialidad o están sujetas a una obligación legal de confidencialidad adecuada.	**4. Confidentiality** The Processor guarantees that the individuals authorized to process personal data have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality.
5. Medidas técnicas y organizativas 5.1. El Encargado del tratamiento garantizará todas las medidas técnicas y organizativas requeridas en virtud del Art. 32 del RGPD para proteger los datos del Responsable del tratamiento. A tal fin, las partes acuerdan las medidas técnicas y organizativas específicas que figuran en el **Anexo 2** del presente ATD. 5.2. Con el fin de adaptarse a las circunstancias técnicas y jurídicas, el Responsable del tratamiento está autorizado a modificar las medidas adoptadas al respecto. Al hacerlo, no se menoscabará el nivel de seguridad acordado contractualmente.	**5. Technical and organizational measures** 5.1. The Processor shall ensure all technical and organizational measures required under Art. 32 GDPR to protect the Controller's data. To this end, the Parties agree on the specific technical and organizational measures set out in **Annex 2** to this DPA. 5.2. In order to adapt to technical and legal circumstances, the Processor is permitted to change the measures taken in this respect. In doing so, the contractually agreed security level shall not be undercut.

6. Derechos del interesado 6.1. El Responsable del Tratamiento es el único Responsable de salvaguardar los derechos de los interesados. 6.2. Dada la naturaleza del tratamiento, el Encargado del tratamiento, cuando sea posible, apoyará al Responsable del tratamiento con medidas técnicas y organizativas adecuadas para cumplir con su obligación de responder a las solicitudes de ejercicio de los derechos del interesado a que se refiere el RGPD. 6.3. El Encargado del tratamiento sólo está autorizado a facilitar información a terceros o a interesados con el consentimiento previo del Responsable del tratamiento. El Encargado del tratamiento transmitirá inmediatamente dichas solicitudes al Responsable del tratamiento.	**6. Data Subject Rights** 6.1. The Controller is solely responsible for safeguarding the rights of data subjects. 6.2. Given the nature of the processing, the Processor will, where possible, support the Controller with appropriate technical and organizational measures to comply with its obligation to respond to requests to exercise the rights of the data subject referred to in the GDPR. 6.3. The Processor is only authorized to provide information to third parties or data subjects with the prior consent of the Controller. The Processor shall immediately forward such requests to the Controller.
7. Obligación de apoyo 7.1. Teniendo en cuenta la naturaleza del tratamiento y la información disponible, el Encargado del tratamiento ayudará al Responsable del tratamiento a cumplir con las obligaciones establecidas en el Art. 32-36 DEL RGPD. 7.2. El Encargado del tratamiento informará al Responsable del tratamiento si tiene conocimiento de una perturbación grave de las operaciones del Encargado del tratamiento o de una infracción del presente ATD o de la normativa de protección de datos en relación con el tratamiento.	**7. Support obligation** 7.1. Taking into account the nature of the processing and the information available, the Processor shall assist the Controller in complying with the obligations set out in Art. 32-36 GDPR. 7.2. The Processor shall inform the Controller if it becomes aware of a serious disruption to the Processor's operations or a breach of this DPA or of data protection regulations in relation to the processing.
8. Supresión o devolución Una vez finalizada la prestación de servicios relacionados con el tratamiento, el Encargado del tratamiento suprimirá o devolverá todos los datos personales a discreción del Responsable del tratamiento y eliminará las copias existentes, a menos que exista la obligación de conservar los datos personales en virtud del Derecho de la Unión o de los Estados miembros.	**8. Deletion or Return** After completion of the provision of services relating to processing, the Processor will either delete or return all personal data at the discretion of the Controller and delete the existing copies, unless there is an obligation to store the personal data under Union or Member State law.

9. Derechos de control 9.1. Previa solicitud, el Encargado del tratamiento proporcionará al Responsable del tratamiento toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el Art. 28 RGPD y permitirá y contribuirá a las auditorías -incluidas las inspecciones- llevadas a cabo por el Responsable del tratamiento u otro auditor Encargado por el Responsable del tratamiento.	**9. Control Rights** 9.1. Upon request, the Processor shall provide the Controller with all information necessary to demonstrate compliance with the obligations set out in Art. 28 GDPR and shall enable and contribute to audits - including inspections - carried out by the Controller or another auditor commissioned by the Controller.
9.2. Las personas encargadas de una inspección deberán recibir del Encargado del tratamiento el acceso y la visión necesarios. El Encargado del tratamiento está obligado a facilitar la información necesaria, demostrar los procedimientos y proporcionar las pruebas requeridas para llevar a cabo una inspección.	9.2. The individuals entrusted with an inspection must be granted access and insight by the Processor as far as necessary. The Processor is obliged to provide the necessary information, demonstrate procedures and provide the evidence required to carry out an inspection.
9.3. Las inspecciones deberán llevarse a cabo sin perturbar de forma evitable las operaciones comerciales del Encargado del tratamiento. Salvo indicación contraria por motivos urgentes que deberá documentar el Responsable del tratamiento, las inspecciones se llevarán a cabo previo aviso con una antelación razonable y durante el horario comercial del Responsable del tratamiento, y con una frecuencia no superior a 12 meses.	9.3. Inspections must be carried out without avoidable disruption to the Processor's business operations. Unless otherwise indicated for urgent reasons to be documented by the Controller, inspections shall take place after reasonable advance notice and during Processor's business hours, and not more frequently than every 12 months.
9.4. El Responsable del tratamiento correrá con los gastos de las medidas necesarias para el cumplimiento de los derechos de inspección, con excepción de las medidas exigidas debido a un incumplimiento de la ley o del contrato por parte del Encargado del tratamiento.	9.4. The Controller shall bear the costs of the measures necessary for the fulfillment of the inspection rights, with the exception of measures required due to a breach of law or contract by the Processor.
10. Ubicación del tratamiento de datos La prestación del tratamiento de datos acordado contractualmente tiene lugar en un estado miembro de la Unión Europea (UE) o en otro estado parte del Acuerdo sobre el Espacio Económico Europeo (EEE). El Responsable del tratamiento consiente la transferencia del tratamiento a un tercer país, siempre que se cumplan los requisitos del Art. 44 y ss. RGPD.	**10. Location of Data Processing** The provision of the contractually agreed data processing takes place in a member state of the European Union (EU) or in another state party to the Agreement on the European Economic Area (EEA). The Controller consents to the transfer of processing to a third country, provided that the requirements of Art. 44 et seq. GDPR are met.

11. Nombramiento de Subencargados del tratamiento 11.1. Las partes especificarán en el **Anexo 3** los Subencargados del tratamiento que se utilizarán. 11.2. El Responsable del tratamiento autorizará el recurso a Subencargados adicionales o la sustitución de Subencargados existentes. El Encargado del tratamiento informará al Responsable del tratamiento con antelación de cualquier cambio previsto en relación con el uso o la sustitución de un Subencargados del tratamiento. 11.3. El Responsable del tratamiento podrá oponerse a un cambio previsto. Si el Responsable plantea una objeción, el Encargado del tratamiento se abstendrá de recurrir al Subencargados correspondiente hasta que se haya aclarado la objeción. Si no hay respuesta del Responsable en el plazo de 14 días desde que fue informado, el cambio se considerará confirmado. 11.4. El Encargado del tratamiento tendrá un derecho extraordinario de rescisión si, en opinión del Encargado, el Responsable se niega a involucrar al Subencargados sin motivo justificado, o si no le es posible prestar el servicio sin el Subencargados rechazado. 11.5. Si se contrata a un Subencargados del tratamiento, el Encargado del tratamiento le impondrá las mismas obligaciones en materia de protección de datos que las establecidas en la ATD.	**11. Appointment of Subprocessors** 11.1. The Parties shall specify in **Annex 3** which subprocessors are to be used. 11.2. The Controller shall authorize the use of additional or the replacement of existing subprocessors. The Processor shall inform the Controller in advance of any intended change regarding the use or replacement of a subprocessor. 11.3. The Controller may object to an intended change. If the Controller raises an objection, the Processor shall refrain from using the respective subcontractor until the objection has been clarified. If there is no response from the responsible party within 14 days of being informed, the change shall be deemed confirmed. 11.4. The Processor shall have an extraordinary right of termination if, in the Processor's opinion, the Controller refuses to involve the subprocessor without good reason, or if it is not possible for the Processor to provide the service without the rejected subprocessor. 11.5. If a subprocessor is engaged, the Processor shall impose the same data protection obligations on the subprocessor as set out in the DPA.
12. Disposiciones finales 12.1. En caso de cuestiones de interpretación y litigios, se aplicará exclusivamente el texto inglés. 12.2. En todos los demás aspectos, se aplicarán las Condiciones Generales[1] del Procesador.	**12. Final Provisions** 12.1. In case of questions of interpretation and disputes, the English text shall apply exclusively. 12.2. In all other respects, the General Terms and Conditions of the Processor shall apply.

Anexo 1: Descripción del Tratamiento

Annex 1: Description of the Processing

Objeto del tratamiento *Subject-Matter of the Processing*	Apoyo a la contabilidad y teneduría de libros del Responsable del tratamiento mediante la asignación y conciliación de los pagos de sus clientes finales a través del envío de invitaciones de pago y la integración de métodos de pago de terceros. Apoyo a la contabilidad y teneduría de libros del Responsable del tratamiento mediante la asignación y conciliación de los pagos de sus clientes finales a través del envío de invitaciones de pago y la integración de métodos de pago de terceros. *Supporting the accounting and bookkeeping of the Controller by allocating and reconciling payments from its end customers by means of sending payment invitations and integrating third-party payment methods*
Duración del tratamiento *Duration of the Processing*	Basado en la vigencia del Acuerdo Principal *Based on the term of the Main Agreement*
Naturaleza del tratamiento *Nature of the Processing*	Organización, estructuración, almacenamiento, recuperación, consulta, uso, transmisión, alineación, combinación *Organization, structuring, storage, retrieval, consultation, use, transmission, alignment, combination*
Finalidad del tratamiento *Purpose of the Processing*	Prestación de los servicios del Encargado del tratamiento de conformidad con el Acuerdo Principal *Provision of the Processor's services in accordance with the Main Agreement*
Tipo de datos personales *Type of Personal Data*	Nombre, dirección, número de teléfono, dirección de correo electrónico y otros datos de contacto, datos de contratos y facturas, datos de transacciones (importe, finalidad, datos bancarios) y otros datos del cliente relacionados con el rendimiento, datos de uso del sistema (dirección IP, datos del dispositivo, navegador, sistema operativo, hora de acceso). *Name, address, telephone number, e-mail address and other contact data, contract and invoice data, transaction data (amount, purpose, bank details) and other performance-related customer data, system usage data (IP address, device details, browser, operating system, time of access)*
Categorías de interesados *Categories of Data Subjects*	Clientes finales y empleados del Responsable del Tratamiento . *End-Customers and Employees of the Controller.*

Anexo 2: Medidas técnicas y organizativas
Annex 2: Technical and Organizational Measures

1. Garantía de confidencialidad **1.1. Control de acceso** Las oficinas de aufinity Group GmbH disponen de un mecanismo de cierre, un sistema de alarma con videovigilancia y conexión a un servicio de seguridad. Los sistemas informáticos funcionan en centros de datos seguros y se encuentran en armarios de servidores cerrados y protegidos por alarma. Sólo los administradores autorizados y nombrados tienen acceso, llaves y códigos	**1. Guarantee of confidentiality** **1.1. Access control** The aufinity Group GmbH office has a locking mechanism, an alarm system with video surveillance and a connection to a security service. The IT systems are operated in secure data centers and are located in locked and alarm-protected server cabinets. Only authorized and named administrators have access, keys and number codes to the server cabinets. Third parties only have access when accompanied by employees. Password-protected login processes are in

autorizados y nombrados tienen acceso, llaves y códigos numéricos a los armarios de servidores. Los terceros sólo tienen acceso cuando van acompañados de empleados. Para la autorización temporal de terceros existen procesos de acceso protegidos por contraseña. Con la ayuda de tarjetas de código, escáneres manuales o PIN, se regulan las autorizaciones de acceso individuales a secciones concretas de los centros de datos, y todas las entradas y salidas son registradas electrónicamente por la seguridad del centro de datos y grabadas por videovigilancia.

1.2. Almacenamiento y control de acceso
Los datos productivos son procesados exclusivamente por un proveedor de servicios informáticos seleccionado (en lo sucesivo, el proveedor de servicios informáticos). Sólo pueden acceder a ellos sus administradores. Los datos de registro se almacenan en la red de este proveedor de servicios de TI. Los registros de auditoría también se transmiten a un proveedor de registros alemán. Los empleados del servicio de atención al cliente tienen acceso limitado a los usuarios y a los datos de las transacciones que contienen información necesaria para los procesos. Los soportes de datos que contienen información confidencial deben eliminarse o destruirse como documentos confidenciales. Los soportes de datos que ya no sean necesarios deben eliminarse o destruirse físicamente.

1.3. Control del soporte de datos
El acceso a los sistemas informáticos sólo es posible mediante conexiones encriptadas y autenticadas y se registra en el registro de accesos y se almacena de acuerdo con los requisitos del proyecto. Los sistemas de almacenamiento se supervisan permanentemente. Cualquier fallo imprevisto de un soporte de datos se registra inmediatamente y se comunica a un grupo de administradores por correo electrónico. En caso de problema, se avisa inmediatamente al operador del centro de datos y se le pide que inspeccione inmediatamente el servidor afectado. Los soportes de almacenamiento defectuosos que ya no son necesarios se eliminan de acuerdo con la normativa de protección de datos antes de ser sustituidos por el fabricante o un tercero encargado por el fabricante.

1.4. Seudonimización y cifrado
Los datos personales y las operaciones de tratamiento de datos se seudonimizan siempre que es posible. Los datos almacenados se suprimen en cuanto dejan de ser necesarios para los fines previstos y la supresión no entra en conflicto con ninguna obligación legal de conservación; si los datos son necesarios para otros fines legalmente permitidos, se restringe su tratamiento.

place for the temporary authorization of third parties. With the help of code cards, hand scans or PINs, individual access authorizations to individual sections of the data centers are regulated, and all entries and exits are electronically logged by data center security and recorded by video surveillance.

1.2. Storage and access control
Productive data is processed exclusively by a selected IT service provider - hereinafter referred to as the IT service provider. Access is only possible by its administrators. Log data is stored within the network of this IT service provider. Audit logs are also transmitted to a German log provider. Customer service employees have limited access to users and transaction data that contain information necessary for the processes. Information carriers containing confidential information must be disposed of or destroyed as confidential documents. Data carriers that are no longer required must be physically deleted or destroyed.

1.3. Data carrier control
IT system access is only possible with encrypted, authenticated connections and is logged in the access log and stored according to project requirements. The storage systems are permanently monitored. Any unplanned failure of a data carrier is registered immediately and reported to an administrator group by e-mail. In the event of a problem, the data center operator is alerted immediately and requested to inspect the affected server immediately. Defective storage media that are no longer required are deleted in accordance with data protection regulations before being replaced by the manufacturer or a third party commissioned by the manufacturer.

1.4. Pseudonymization and encryption
Personal data and data processing operations are pseudonymized where possible. Stored data is deleted as soon as it is no longer required for its intended purpose and the deletion does not conflict with any statutory retention obligations; if the data is required for other and legally permissible purposes, its processing is restricted.

2. Garantía de integridad **2.1. Control de entrada** Todos los datos se procesan en el centro de datos del proveedor de servicios informáticos. Además, los datos principales se almacenan en paralelo en un sistema interno y externo mediante los denominados registros de auditoría. **2.2. Control de transporte** Los datos de aufinity Group GmbH se almacenan y procesan exclusivamente en centros de datos seguros. Todas las conexiones están encriptadas mediante SSL. Todos los datos recogidos y procesados por el servicio de atención al cliente se intercambian a través de conexiones encriptadas. **2.3. Control de pedidos** Todas las personas que procesan datos personales están obligadas por aufinity group GmbH a cumplir con el secreto de los datos, el secreto de las telecomunicaciones de acuerdo con la Sección 88 TKG y el secreto social de acuerdo con la Sección 35 (1) SGB I y garantiza que están instruidos en consecuencia. Los datos sólo se transmitirán a terceros si es necesario para la tramitación del contrato o si el cliente ha dado su consentimiento previo. Una vez al año, se comprueba si el proveedor de alojamiento cumple la política de tratamiento de datos personales. Los subcontratistas se seleccionan cuidadosamente. **2.4. Control de separación** Los datos de otros clientes del proveedor de servicios informáticos se separan mediante discos virtuales encriptados. Los datos personales sólo se almacenan en los sistemas de bases de datos asociados a los sistemas de aplicación. El proveedor de servicios informáticos no necesita acceder a los datos personales salvo para analizar y, en su caso, rectificar errores o realizar copias de seguridad. Los entornos productivo y de pruebas están separados entre sí.	**2. Guarantee of integrity** **2.1. Input control** All data is processed in the IT service provider's data center. In addition, the core data is stored in parallel in an internal and external system via so-called audit logs. **2.2. Transport control** The data of aufinity Group GmbH is stored and processed exclusively in secure data centers. All connections are SSL-encrypted. All data collected and processed by customer service is exchanged via encrypted connections. **2.3. Order control** All persons who process personal data are obliged by aufinity group GmbH to comply with data secrecy, telecommunications secrecy in accordance with Section 88 TKG and social secrecy in accordance with Section 35 (1) SGB I and ensures that they are instructed accordingly. Data will only be transferred to third parties if this is necessary for the purpose of processing the contract or if the customer has given their prior consent. Once a year, the hosting provider is checked for compliance with the policy on handling personal data. Subcontractors are carefully selected. **2.4. Separation control** Data from other customers of the IT service provider is separated by virtual encrypted disks. Personal data is only stored in the database systems associated with the application systems. The IT service provider does not require access to personal data except for the purpose of analyzing and, if necessary, rectifying errors or making backup copies. The productive and test environments are separated from each other.
3. Garantía de disponibilidad y resistencia Los sistemas de almacenamiento de datos están duplicados en dos ubicaciones y se utiliza RAID. Se realizan copias de seguridad diarias de todos los datos de los clientes. Los servidores reciben alimentación ininterrumpida. El diseño de todos los componentes necesarios para la prestación del servicio es estrictamente redundante. Los componentes importantes están distribuidos en dos ubicaciones conectadas. Se utiliza un procedimiento de copia de seguridad en espejo para la copia de seguridad de los datos en varias ubicaciones.	**3. Guarantee of availability and resilience** The data storage systems are mirrored across two locations and RAID is used. All customer data is backed up daily. The servers are supplied with uninterrupted power. The design of all components required for service provision is strictly redundant. Important components are distributed across two linked locations. A mirrored back-up procedure is used for data backup across several locations.
4. Procedimiento de revisión periódica, valoración y evaluación de la eficacia de las medidas técnicas y organizativas Las medidas mencionadas se revisan periódicamente, teniendo en cuenta las directrices y recomendaciones técnicas pertinentes de la Oficina Federal de Seguridad de la Información, y se adaptan a los cambios o ampliaciones de las estructuras informáticas y a la evolución de los requisitos de protección y las amenazas.	**4. Procedure for regular review, assessment and evaluation of the effectiveness of the technical and organizational measures** The aforementioned measures are regularly reviewed, taking into account the relevant technical guidelines and recommendations of the Federal Office for Information Security, and adapted to changing or expanding IT structures and changing protection requirements and threats.

5. Documentación escrita de otras medidas Se ha creado una política de seguridad de datos para garantizar el cumplimiento de las directrices y medidas. Esta Política de Seguridad de Datos es vinculante para todos los empleados, invitados y todos los subarrendatarios en las instalaciones de aufinity Group GmbH. Cualquier infracción será comunicada al supervisor y a la dirección de aufinity Group GmbH y podrá ser sancionada.	**5. Written documentation of further measures** A data security policy has been created to ensure compliance with the guidelines and measures. This Data Security Policy is binding for all employees, guests and all subtenants on the premises of the aufinity Group GmbH. Any violation will be reported to the supervisor and the management of aufinity Group GmbH and may be penalized.

Anexo 3: Subencargados

Annex 3: Subprocessors

Dembach Goo Informatik GmbH & Co. KG	Hohenzollernring 72, 50672 Cologne, Germany https://www.dg-i.net/ info@dg-i.net	Alojamiento, supervisión y funcionamiento de los servicios *Hosting, monitoring and operation of services*	Alemania *Germany*
Google Inc.	1600 Amphitheatre Parkway, Mountain View, CA 94043, USA https://www.google.com	Alojamiento y almacenamiento en la nube *Hosting and Cloud Storage*	USA
Mailgun Technologies Inc.	112 E Pecan St #1135, San Antonio, TX 78205, USA https://www.mailgun.com/	Análisis sintáctico y envío de correos electrónicos del sistema *Parsing and sending system e-mails*	USA
Functional Software, Inc.	132 Hawthorne Street, San Francisco, CA 94107, USA www.sentry.io	Detección de errores de código en el software para la estabilidad del sistema de nuestros servicios *Detection of code errors within the software for the system stability of our services*	USA
Datadog Inc.	620 8th Avenue, Floor 45, New York, NY 10018, USA	Identificación de errores de código en el software para la estabilidad del sistema de nuestros servicios *Identification of code errors within the software for the system stability of our services*	USA
Sensible Technologies Inc.	1400 Castro St, San Francisco, CA 94114, USA	Tratamiento estructurado de los datos de las facturas *Structured processing of invoice data*	USA
DigitalOcean LLC.	101 Avenue of the Americas, 10th Floor, New York, NY 10013, USA https:// www.digitalocean.com/	Notificación a sistemas externos para actualizar el estado de los datos de las transacciones y suministro de red cifrada *Notification of external systems to update the status of transaction data and provision of encrypted network*	USA