

<p><b>Data Processing Agreement</b> between <b>Trusty Client</b> - the Controller - hereafter named the "Client" - and <b>Trusty AG</b>, Riedstrasse 7, 6330 Cham, Switzerland - the Processor - hereafter named the "Service Provider" -</p> <p><b>1. Background and Scope</b></p> <p>The Service Provider and the Client have entered into the principal contractual relationship, which is governed by the Terms of Service (the Terms). The latter stipulate terms and conditions for the use of the Service Provider's web-based whistleblowing Application called Trusty (the Application) by the Client.</p> <p>For the purpose and within the scope of providing the Application under the said Terms, the Service Provider shall process personal data for the Client in accordance with the GDPR and this agreement.</p> <p>If there is a discrepancy between this agreement and the Terms, this agreement shall take precedence in relation to the personal data processing, unless explicitly provided otherwise herein.</p> <p>This agreement may be made available in different languages. In case of conflicts between the English version and any translation, the English version shall prevail.</p> <p><b>2. Object, Nature and Purpose of Data Processing</b></p> <p>The Service Provider is providing the web-based Application where the Client, as the data controller, can receive, process and store personal data related to whistleblowing reports submitted to the Client by whistleblowers. The Application has been designed to work as an internal reporting channel tool but, to the extent not regulated by the Terms, the Client decides how they use the Application.</p>	<p><b>Contrato de procesamiento de datos</b> entre <b>Cliente de Trusty</b> - el Responsable del Tratamiento - en adelante denominado "Cliente" - y <b>Trusty AG</b>, Riedstrasse 7, 6330 Cham, Suiza - el Encargado del Tratamiento - en adelante denominado "Proveedor de Servicios" -</p> <p><b>1. Antecedentes y Ámbito de Aplicación</b></p> <p>El Proveedor de Servicios y el Cliente han establecido una relación contractual principal regulada por los Términos y Condiciones Generales (los "Términos"). Estos regulan las condiciones para el uso de la aplicación de denuncias en línea basada en la web proporcionada por el Proveedor de Servicios llamada Trusty (la "Aplicación") por parte del Cliente.</p> <p>Con el propósito y en el marco de la provisión de la Aplicación de acuerdo con los Términos mencionados, el Proveedor de Servicios procesa los datos personales del Cliente de acuerdo con el Reglamento General de Protección de Datos (GDPR) y este contrato.</p> <p>En caso de conflicto entre este contrato y los Términos, este contrato prevalece en lo que respecta al procesamiento de datos personales, a menos que se establezca expresamente lo contrario aquí.</p> <p>Este contrato puede proporcionarse en varios idiomas. En caso de conflictos entre la versión en inglés y una traducción, prevalece la versión en inglés.</p> <p><b>2. Objeto, Naturaleza y Propósito del Procesamiento de Datos</b></p> <p>El Proveedor de Servicios proporciona la Aplicación web, a través de la cual el Cliente, en calidad de responsable del tratamiento, puede recibir, procesar y almacenar datos personales relacionados con informes de denuncias recibidos de informantes. La Aplicación está diseñada como un canal de informes internos, pero en la medida en que no esté regulada por los Términos, el Cliente decide cómo utilizar la Aplicación.</p>
---	---

<p>The personal data and other information that are intended to be collected and processed in the Application are listed in the Appendix 1.</p> <p>The data and information in the Appendix 1 shall be stored in the Application's database operated by the Service Provider and hosted on a virtual server in the EU, all on behalf of and for the Client. No data is transferred to third countries outside of the European Economic Area without the prior consent of the Client and may only occur if the special conditions defined in Articles 44 et seq. of the GDPR are fulfilled.</p> <p>The Service Provider shall process the said personal data and other information in the Application exclusively for operation and maintenance of the Application, its webpages and database.</p> <p><b>3. Technical and Organizational Measures</b></p> <p>Technical and organizational measures, together with their implementation and observance, are detailed in Appendix 2. Insofar as the inspection/audit by the Client shows the need for amendments, such amendments shall be implemented by mutual agreement.</p> <p>The Service Provider shall establish the security of the data in accordance the GDPR requirements. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems.</p> <p>The technical and organizational measures shall be subject to technical progress and further development. In this respect, the Service Provider is permitted to implement alternative adequate measures. The safety level of the specified measures must not be compromised. Substantial changes must be documented.</p> <p><b>4. Requests by Affected Persons</b></p> <p>The Service Provider shall not correct, delete or restrict the processing of data on a direct request by affected persons. Insofar as an affected person</p>	<p>Los datos personales y otra información que se deben recopilar y procesar en la Aplicación se detallan en el Anexo 1.</p> <p>Los datos e información enumerados en el Anexo 1 se almacenan en la base de datos de la Aplicación, operada por el Proveedor de Servicios y alojada en un servidor virtual en la UE, en nombre y por cuenta del Cliente. La transferencia de datos a terceros países fuera del Espacio Económico Europeo solo se realizará con el consentimiento previo del Cliente y solo si se cumplen las condiciones especiales establecidas en los Artículos 44 y siguientes del GDPR.</p> <p>El Proveedor de Servicios procesa los datos personales mencionados y otra información en la Aplicación exclusivamente para el funcionamiento y mantenimiento de la Aplicación, sus sitios web y la base de datos.</p> <p><b>3. Medidas Técnicas y Organizativas</b></p> <p>Las medidas técnicas y organizativas, así como su implementación y cumplimiento, se detallan en el Anexo 2. En caso de que la revisión o auditoría realizada por el Cliente revele la necesidad de cambios, estos se implementarán de común acuerdo.</p> <p>El Proveedor de Servicios garantiza la seguridad de los datos de acuerdo con los requisitos del GDPR. Las medidas a tomar incluyen medidas de seguridad de datos y medidas que aseguran un nivel de protección adecuado para el riesgo en cuanto a la confidencialidad, integridad, disponibilidad y resistencia de los sistemas.</p> <p>Las medidas técnicas y organizativas están sujetas al progreso técnico y al desarrollo. En este sentido, se permite al Proveedor de Servicios tomar medidas alternativas adecuadas. El nivel de seguridad de las medidas establecidas no debe verse afectado. Los cambios significativos deben documentarse.</p> <p><b>4. Solicitudes de los Interesados</b></p> <p>El Proveedor de Servicios no puede corregir, eliminar o restringir el procesamiento de datos a solicitud directa de los interesados. En caso de que un interesado se comunique directamente con el Proveedor de</p>
---	--

contacts the Service Provider directly in this respect, the Service Provider will immediately forward this request to the Client without delay.

### **5. Quality Assurance and Other Duties of the Service Provider**

In addition to complying with the provisions of this agreement, the Service Provider shall comply with statutory obligations in accordance with Articles 28 to 33 of the GDPR; in this respect, the Service Provider shall particularly ensure compliance with the following requirements:

- Confidentiality in accordance with Article 28, paragraph 3, sentence 2, clause b, Article 29 and Article 32, paragraph 4. The Service Provider entrusts only such persons with the data processing defined in this agreement who have been bound to confidentiality and have previously been familiarized with the data protection provisions relevant to their work. The Service Provider and any person acting under its authority who has access to personal data may only process that data in accordance with the instructions of the Client (which includes the powers granted in this agreement and in the Terms) unless otherwise required to do so by law.
- The Service Provider and the Client shall, upon request, cooperate with the supervisory authority in the performance of their duties.
- The Client shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to the processing of personal data under this agreement. This also applies insofar as the Service Provider is under investigation or is a party to an investigation by a competent authority in connection with infringements to any civil or criminal law, administrative rule, or regulation regarding the processing of personal data under this agreement.
- Insofar as the Client is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim of an affected person or a third party or any other claim in connection with the processing of personal data under this agreement, the Service Provider shall make every effort to support the Client to the best of his ability.

Servicios con respecto a esto, el Proveedor de Servicios transmitirá de inmediato esta solicitud al Cliente.

### **5. Aseguramiento de la Calidad y Otras Obligaciones del Proveedor de Servicios**

Además de cumplir con las disposiciones de este contrato, el Proveedor de Servicios debe cumplir con las obligaciones legales según los Artículos 28 al 33 del Reglamento General de Protección de Datos (GDPR); en particular, debe garantizar el cumplimiento de los siguientes requisitos:

- Confidencialidad según el Artículo 28, Párrafo 3, Oración 2, Cláusula b, Artículo 29 y Artículo 32, Párrafo 4. El Proveedor de Servicios asigna solo a aquellas personas con la responsabilidad de procesar datos definidos en este contrato que están obligadas a la confidencialidad y que han sido informadas previamente sobre las disposiciones de protección de datos relevantes para su actividad. El Proveedor de Servicios y cualquier persona subordinada a él que tenga acceso a datos personales solo puede procesar estos datos de acuerdo con las instrucciones del Cliente (incluidos los poderes otorgados en este contrato y en los términos), a menos que esto esté legalmente prescrito.
- El Proveedor de Servicios y el Cliente colaborarán con la autoridad de supervisión a solicitud en el cumplimiento de sus tareas.
- El Cliente será informado de inmediato sobre inspecciones y medidas de la autoridad de supervisión en la medida en que se refieran al procesamiento de datos personales en el marco de este contrato. Esto también se aplica si se investiga al Proveedor de Servicios en relación con violaciones de leyes civiles o penales, regulaciones administrativas o disposiciones sobre el procesamiento de datos personales en el marco de este contrato, o si es objeto de una investigación por parte de una autoridad competente.
- Si el Cliente está expuesto a una auditoría por parte de la autoridad de supervisión, un procedimiento por infracciones o penales, una reclamación de responsabilidad por parte de una persona afectada o un tercero, o cualquier otra reclamación relacionada con el procesamiento de datos

- The Service Provider shall regularly monitor the internal processes as well as the technical and organizational measures to ensure that the processing in its area of responsibility is executed in accordance with the requirements of the applicable data protection law and that the rights of the affected people are protected.
- Without undue delay and no later than 24 hours after the Service Provider has become aware of a security breach, the Service Provider shall notify the Client thereof in writing. This notification shall, at a minimum, and to the extent possible in light of the nature of the incident, include the following:
  - information on the nature of the identified security breach,
  - what categories of registered individuals are affected by it, and
  - the approximate number of the affected registered individuals, including categories of comprehensive personal data and the number of these in addition to what preventive or mitigating measures the Service Provider has implemented as a result of the found security breach.

The Service Provider shall assist the Client in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments, and prior consultations referred to in Articles 32 to 36 of the GDPR.

The Service Provider may claim compensation for support services which are not attributable to failures on the part of the Service Provider, with the hourly rate of 250 CHF (VAT not included).

## 6. Subcontracting

The Service Provider is engaging third party service providers (subcontractors) for the purpose of providing the Application. The list of subcontractors is provided in Appendix 1.

The Service Provider shall provide a 10 (ten) days advance notice before engaging any new subcontractor. The Client may object in writing to the Service Provider's appointment of a subcontractor on reasonable grounds relating to data protection by notifying the Service Provider promptly in

personales en el marco de este contrato, el Proveedor de Servicios hará todos los esfuerzos para apoyar al Cliente en la medida de lo posible.

- El Proveedor de Servicios supervisa regularmente los procesos internos, así como las medidas técnicas y organizativas, para garantizar que el procesamiento en su área de responsabilidad se realice de acuerdo con los requisitos de la legislación de protección de datos aplicable y se protejan los derechos de las personas afectadas.

- El Proveedor de Servicios notificará al Cliente de inmediato, y a más tardar 24 horas después de haber tenido conocimiento de una violación de seguridad, por escrito. Esta notificación debe contener al menos, y en la medida de lo posible dada la naturaleza del incidente:

- Información sobre la naturaleza de la violación de seguridad identificada,
- qué categorías de personas registradas están afectadas, y
- el número aproximado de personas registradas afectadas, incluidas las categorías de datos personales más amplias y su número, así como las medidas preventivas o correctivas que el Proveedor de Servicios ha tomado como resultado de la violación de seguridad identificada.

El Proveedor de Servicios apoya al Cliente en el cumplimiento de las obligaciones relacionadas con la seguridad de los datos personales, la obligación de notificar violaciones de datos, la evaluación de impacto de protección de datos y la consulta previa según los Artículos 32 al 36 del GDPR.

Para los servicios de apoyo que no se deban a defectos por parte del Proveedor de Servicios, el Proveedor de Servicios puede solicitar una compensación a una tarifa por hora de 250 CHF (sin IVA).

## 6. Subcontratación

El Proveedor de Servicios subcontrata a terceros proveedores de servicios (subcontratistas) para proporcionar la aplicación. La lista de subcontratistas se encuentra en el Anexo 1.

El Proveedor de Servicios informará al Cliente con 10 (diez) días de antelación sobre la contratación de un nuevo subcontratista. El Cliente puede oponerse por escrito a la contratación de un subcontratista por parte del Proveedor de Servicios por razones adecuadas de protección de datos,

writing within 5 (five) days of receipt of the Service Provider's notice. Such notice shall explain the reasonable grounds for the objection. In such event, the parties shall discuss the Client's concerns in good faith with a view to achieving commercially reasonable resolution.

### **7. The Client's Inspection Rights**

The Client shall, at its own expense, have the right to conduct inspections, or have them conducted by independent third parties, with the purpose of verifying the Service Provider's compliance with this agreement. Any inspection by the Client shall be announced to the Service Provider in good time.

The Service Provider shall ensure that the Client can verify the Service Provider's compliance with the obligations under Article 28 of the GDPR. The Service Provider is obligated to provide the Client with the necessary information upon request and in particular to provide proof of the implementation of the technical and organizational measures.

The Service Provider may assert a claim for remuneration for enabling Client's inspections with the hourly rate of 250 CHF (VAT not included).

The Service Provider may at its own discretion provide support to the Client in any other reviews conducted by the latter, including but not limited to completing Client's questionnaires on security, privacy, data processing and similar topics related to the Application. In such cases the Service Provider may assert a claim for remuneration with the hourly rate from the preceding paragraph.

### **8. The Client's Instructions**

The Client shall immediately confirm any oral instructions in writing.

The Service Provider shall inform the Client immediately if it believes that an instruction violates data protection regulations. The Service Provider shall then be entitled to suspend the execution of the relevant instructions until the Client confirms or alters said instructions.

notificando al Proveedor de Servicios de inmediato dentro de los 5 (cinco) días posteriores a la recepción de la comunicación del Proveedor de Servicios. En tal caso, las Partes discutirán de buena fe las preocupaciones del Cliente con el objetivo de encontrar una solución económicamente adecuada.

### **7. Derecho del Cliente a la Revisión**

El Cliente tiene el derecho, a su propio costo, de realizar inspecciones o permitir que terceros independientes las realicen para verificar el cumplimiento de este contrato por parte del Proveedor de Servicios. Cualquier inspección por parte del Cliente debe ser anunciada al Proveedor de Servicios con suficiente antelación.

El Proveedor de Servicios garantiza que el Cliente pueda verificar el cumplimiento de las obligaciones del Proveedor de Servicios según el Artículo 28 del GDPR. El Proveedor de Servicios está obligado a proporcionar la información necesaria al Cliente a solicitud, y en particular, demostrar la implementación de las medidas técnicas y organizativas.

El Proveedor de Servicios puede reclamar una compensación por facilitar las inspecciones del Cliente con una tarifa por hora de 250 CHF (sin IVA).

El Proveedor de Servicios puede, a su discreción, ayudar al Cliente en otras revisiones realizadas por este, incluido el llenado de cuestionarios del Cliente sobre seguridad, privacidad, procesamiento de datos y temas similares relacionados con la aplicación. En tales casos, el Proveedor de Servicios puede reclamar una compensación a la tarifa por hora mencionada anteriormente.

### **8. Instrucciones del Cliente**

Las instrucciones verbales deben confirmarse por escrito de inmediato por el Cliente.

El Proveedor de Servicios informará al Cliente de inmediato si considera que una instrucción infringe las disposiciones de protección de datos. En ese caso, el Proveedor de Servicios tiene el derecho de suspender la

<p><b>9. Deletion and Return of Personal Data</b></p> <p>Copies or duplicates of the data shall not be created without the knowledge of the Client, except for backup copies as far as they are necessary to ensure proper data processing as well as data required for compliance with statutory storage obligations.</p> <p>Upon termination of the Terms and consequently this agreement the Service Provider shall, at the choice of the Client either i) permanently delete, or ii) return all the data to the Client and then permanently delete all the existing copies, unless the Service Provider is legally obliged to store such data.</p> <p>Notwithstanding the preceding provision, the Service Provider is entitled to save copies of data to the extent necessary to be able to document delivery of services as per the Terms or to defend itself against legal claims. In such a case, the Client's personal data may be processed by the Service Provider for the stated purposes only.</p> <p>Upon request, the Service Provider shall provide the Client with information on nature and the time of the data's deletion.</p> <p><b>10. Final Provisions</b></p> <p>Modifications</p> <p>The Service Provider reserves the right, at its sole discretion, to change, modify, add, or remove portions of the Agreement at any time by posting such changes on <a href="https://trusty.report">trusty.report</a> webpages or through the Application. Such amended Agreement will become effective 10 (ten) days after their posting in the Application.</p> <p>The Client is obliged to check the Agreement periodically for changes. Continued use of the Application after such changes have become effective constitutes the Client's binding acceptance of such changes.</p> <p>Term of the Agreement</p>	<p>ejecución de la instrucción en cuestión hasta que el Cliente confirme o modifique la instrucción.</p> <p><b>9. Eliminación y Devolución de Datos Personales</b></p> <p>No se deben crear copias o duplicados de los datos sin el conocimiento del Cliente, excepto las copias de seguridad necesarias para un procesamiento de datos adecuado, así como los datos necesarios para cumplir con las obligaciones legales de retención.</p> <p>Al finalizar las Condiciones y, por lo tanto, este Contrato, a elección del Cliente, el Proveedor de Servicios eliminará permanentemente los datos o devolverá todos los datos al Cliente y luego eliminará permanentemente todas las copias existentes, a menos que el Proveedor de Servicios esté legalmente obligado a retener estos datos.</p> <p>Sin perjuicio de la disposición anterior, el Proveedor de Servicios tiene derecho a almacenar copias de datos en la medida en que sea necesario para documentar la prestación contractual del servicio o para defenderse contra reclamaciones legales. En tal caso, los datos personales del Cliente solo pueden procesarse por el Proveedor de Servicios para los fines mencionados.</p> <p>El Proveedor de Servicios proporcionará al Cliente información sobre la naturaleza y el momento de la eliminación de los datos a solicitud.</p> <p><b>10. Disposiciones Finales</b></p> <p>Cambios</p> <p>El Proveedor de Servicios se reserva el derecho, a su discreción, de cambiar, modificar, agregar o eliminar partes del contrato en cualquier momento mediante la publicación de dichos cambios en los sitios web de <a href="https://trusty.report">trusty.report</a> o a través de la aplicación. El contrato modificado entra en vigencia 10 (diez) días después de su publicación en la aplicación.</p> <p>El Cliente está obligado a revisar regularmente este contrato en busca de cambios. El uso continuado de la aplicación después de la entrada en vigencia de dichos cambios implica la aceptación vinculante de estos cambios por parte del Cliente.</p>
---	--

<p>This agreement enters into force between the parties together with the Terms and also ceases to be in effect with the cancellation or any other termination of the Terms.</p> <p>The right to isolated extraordinary notice of cancellation hereby remains intact, as do statutory rights of rescission.</p> <p>Jurisdiction</p> <p>The parties agree that any claims and disputes that may arise from the agreement shall be settled by the court in Zug, Switzerland.</p> <p><b>Appendix 1 to the Data Processing Agreement</b></p> <p><b>List of Personal Data and Other Information Processed in the Application</b></p> <ul style="list-style-type: none"> <li>• personal data relating to a whistleblower (reporting person), if provided: first name, last name, address, email address, telephone number, relationship toward the Client;</li> <li>• personal data relating to the persons suspected to be involved and the persons being aware of the violation/wrongdoing, if provided: full name, position, organization; a factual description of the violation/wrongdoing, as well as a description of the circumstances of the incident, including time and place of the incident;</li> <li>• personal data relating to the users of the Application authorised by the Client: first name, last name, email address, function with the Client.</li> </ul> <p><b>List of subcontractors:</b></p> <ul style="list-style-type: none"> <li>• Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany; <ul style="list-style-type: none"> <li>◦ Provides hosting of the Application on the virtual server in Nuremberg, Germany;</li> </ul> </li> </ul>	<p><b>Duración de este Contrato</b></p> <p>Este Contrato entra en vigencia entre las Partes junto con las Condiciones y también termina con la rescisión o cualquier otra terminación de las Condiciones.</p> <p>El derecho a la terminación extraordinaria aislada no se ve afectado, al igual que los derechos legales de rescisión.</p> <p>Jurisdicción</p> <p>Las Partes acuerdan que para cualquier reclamo y disputa que pueda surgir de este Contrato, el tribunal en Zug, Suiza, será competente.</p> <p><b>Anexo 1 al Contrato de Procesamiento de Datos</b></p> <p><b>Lista de datos personales y otra información procesada en la aplicación</b></p> <ul style="list-style-type: none"> <li>• Datos personales del informante (persona que realiza la denuncia), si se proporcionan: nombre, apellido, dirección, dirección de correo electrónico, número de teléfono, relación con el cliente;</li> <li>• Datos personales de las personas que se sospecha que están involucradas en la infracción/comportamiento incorrecto y de las personas que conocen la infracción/comportamiento incorrecto, si se proporcionan: nombre completo, cargo, organización; una descripción objetiva de la infracción/comportamiento incorrecto y una descripción de las circunstancias del incidente, incluyendo la hora y el lugar del incidente;</li> <li>• Datos personales de los usuarios autorizados de la aplicación por parte del cliente: nombre, apellido, dirección de correo electrónico, función en el cliente.</li> </ul> <p><b>Lista de subcontractistas:</b></p> <ul style="list-style-type: none"> <li>• Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Alemania;</li> <li>• Proporciona el alojamiento de la aplicación en el servidor virtual en Núremberg, Alemania;</li> </ul>
--	--

- AWS EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxembourg;
  - Provides notification email relay service.

## **Appendix 2 to the Data Processing Agreement**

### **Technical and Organizational Measures**

The Service Provider prevents unauthorized internal access to the Application by applying security updates regularly by using state of the art technology, hence securing critical network access points. Allocation of authorisations to the Service Provider's staff is revision-proof.

Electronic access to the Application by the Client is password protected. After opening of the Client Application Account, the initial user password is required to be changed by the Client and is not known to the Service Provider. The Client's password is determined by the Client himself; the password must comply with predefined guidelines relating to the minimum number of characters and numbers. The Client is responsible for authorising and opening additional user accounts for the Application.

The Application data are physically or logically isolated and saved separately from other Service Provider's data. Backups of data are performed using a similar system of physical or logical isolation. Backups of all Application data are performed daily.

Resilience measures such as security programs (firewalls, encryption programs, spam filters) and monitoring of all relevant servers are employed.

In order to ensure confidentiality, the Application does not store IP addresses and time stamps.

The Application supports functioning in a server farm and ensures uninterrupted functioning (24x7x365). Any scalability for performance and additional services is provided. No licensed programs are used. The software is using open-source solutions (Mysql, Apache, Laravel, jQuery, Bootstrap).

- AWS EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxemburgo;
  - Ofrece un servicio de retransmisión de correo electrónico para notificaciones.

## **Anexo 2 al Contrato de Procesamiento de Datos**

### **Medidas técnicas y organizativas**

El proveedor de servicios evita el acceso interno no autorizado a la aplicación mediante actualizaciones de seguridad regulares de acuerdo con el estado de la técnica, asegurando así los accesos críticos a la red. La asignación de permisos al personal del proveedor de servicios es a prueba de auditorías.

El acceso electrónico del cliente a la aplicación está protegido por contraseña. Después de abrir la cuenta de la aplicación del cliente, la contraseña inicial debe ser cambiada por el cliente y no es conocida por el proveedor de servicios. La contraseña del cliente es establecida por el cliente mismo; la contraseña debe cumplir con las pautas predefinidas con respecto al número mínimo de caracteres y números. El cliente es responsable de la autorización y apertura de cuentas de usuario adicionales para la aplicación.

Los datos de la aplicación se almacenan física o lógicamente aislados y separados de otros datos del proveedor de servicios. Las copias de seguridad de los datos se realizan utilizando un sistema similar de aislamiento físico o lógico. Las copias de seguridad de todos los datos de la aplicación se realizan diariamente.

Se utilizan medidas de seguridad contra fallos como programas de seguridad (firewalls, programas de cifrado, filtros de spam) y la supervisión de todos los servidores relevantes.

Para garantizar la confidencialidad, la aplicación no almacena direcciones IP y marcas de tiempo.

La aplicación es compatible con el funcionamiento en una granja de servidores y garantiza un funcionamiento continuo (24x7x365). Se proporciona una escalabilidad para el rendimiento y servicios adicionales.

<p>SSL/TLS encryption is used to ensure security and privacy during data transfer. Textual data from the contents of the reports and from the communication channel with a whistleblower are encrypted with the symmetric AES CBC algorithm using the OpenSSL extension. Files are encrypted using AES 256 CTR cipher. All passwords in the Application are compressed with the Bcrypt algorithm. The Application uses Linux Iptables/Netfilter firewall.</p> <p>Pseudonymisation of whistleblower data is provided with randomly generated usernames for each whistleblower individually. The program records an audit trail for each entry/insight/change. All access and key events are logged, and these logs are accessible to the Service Provider, if necessary.</p> <p>Terminated Application accounts are permanently deleted and overwritten. The Client may delete contents of individual reports by himself; in this case the contents are also permanently deleted and overwritten.</p> <p>The Service Provider regularly mandates a third party provider to perform a web-application penetration test on the Application and subsequently resolves identified security vulnerabilities, if any.</p> <p><b>Subcontractors</b></p> <p>Technical and organizational measures (herein also referred to as TOMs) relating to the hosting server are detailed in the agreement between the Service Provider and Hetzner Online GmbH, Appendix 2.</p> <p>Technical and organizational measures relating to the notification email relay services are detailed in the agreement between the Service Provider and AWS EMEA SARL, Annex 1.</p> <p>Both documents are incorporated into this Agreement by reference and are available at <a href="https://trusty.report/documents/">https://trusty.report/documents/</a>.</p>	<p>No se utilizan programas con licencia. El software utiliza soluciones de código abierto (Mysql, Apache, Laravel, jQuery, Bootstrap).</p> <p>Para garantizar la seguridad y la privacidad en la transferencia de datos, se utiliza un cifrado SSL/TLS. Los datos de texto del contenido de los informes y del canal de comunicación con un informante se cifran con el algoritmo simétrico AES-CBC utilizando la extensión OpenSSL. Los archivos se cifran con AES 256 CTR. Todas las contraseñas en la aplicación se comprimen con el algoritmo Bcrypt. La aplicación utiliza el firewall Linux Iptables/Netfilter.</p> <p>La pseudonimización de los datos de los informantes se garantiza mediante nombres de usuario generados aleatoriamente para cada informante individual. El programa registra un rastro de auditoría para cada entrada/vista/cambio. Todos los eventos de acceso y claves se registran, y estos registros están disponibles para el proveedor de servicios según sea necesario.</p> <p>Las cuentas de la aplicación finalizadas se eliminan y sobrescriben permanentemente. El cliente puede eliminar el contenido de informes individuales; en este caso, el contenido también se elimina y sobrescribe permanentemente.</p> <p>El proveedor de servicios contrata regularmente a un proveedor externo para realizar una prueba de penetración de la aplicación y luego corrige cualquier vulnerabilidad de seguridad identificada.</p> <p><b>Subcontratistas</b></p> <p>Las medidas técnicas y organizativas (también conocidas como TOMs) con respecto al servidor de alojamiento se describen en el contrato entre el proveedor de servicios y Hetzner Online GmbH, Anexo 2.</p> <p>Las medidas técnicas y organizativas con respecto a los servicios de retransmisión de correo electrónico se rigen por el contrato entre el proveedor de servicios y SMTP.de ApS, Anexo 1.</p> <p>Ambos documentos se incorporan por referencia en el contrato y están disponibles en <a href="https://trusty.report/documents/">https://trusty.report/documents/</a>.</p>
---	---

**PUBLISHED ON March 1<sup>st</sup> 2023**

**PUBLICADO EL 1 de marzo de 2023**

Trusty AG, Dejan Jasnic



(Trusty Client/ Cliente de Trusty)\_\_\_\_\_