Data Processing Agreement between **Trusty Client** - the Controller - hereafter named the "Client" - and **Trusty AG**, Riedstrasse 7, 6330 Cham, Swtizerland - the Processor - hereafter named the "Service Provider" –	**Vertrag über die Datenverarbeitung** zwischen **Trusty Kunde** - dem für die Verarbeitung Verantwortlichen - im Folgenden "Kunde" genannt - und **Trusty AG**, Riedstrasse 7, 6330 Cham, Schweiz - dem Auftragsverarbeiter - im Folgenden "Dienstleister" genannt -
1. Background and Scope 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. 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. 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. 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.	**1. Hintergrund und Geltungsbereich** Der Dienstleister und der Auftraggeber sind ein Hauptvertragsverhältnis eingegangen, das durch die Allgemeinen Geschäftsbedingungen (die Bedingungen) geregelt wird. Letztere regeln die Bedingungen für die Nutzung der webbasierten Whistleblowing-Anwendung des Dienstleisters namens Trusty (die Anwendung) durch den Kunden. Zum Zweck und im Rahmen der Bereitstellung der Anwendung gemäß den genannten Bedingungen verarbeitet der Dienstleister personenbezogene Daten des Kunden in Übereinstimmung mit der Datenschutz-Grundverordnung und diesem Vertrag. Im Falle eines Widerspruchs zwischen diesem Vertrag und den Bedingungen hat dieser Vertrag in Bezug auf die Verarbeitung personenbezogener Daten Vorrang, sofern hierin nicht ausdrücklich etwas anderes vorgesehen ist. Dieser Vertrag kann in verschiedenen Sprachen zur Verfügung gestellt werden. Im Falle von Widersprüchen zwischen der englischen Fassung und einer Übersetzung ist die englische Fassung maßgebend.
2. Object, Nature and Purpose of Data Processing 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	**2. Gegenstand, Art und Zweck der Datenverarbeitung** Der Dienstleister stellt die webbasierte Anwendung zur Verfügung, mit der der Kunde als für die Datenverarbeitung Verantwortlicher personenbezogene Daten im Zusammenhang mit Whistleblowing-Meldungen empfangen, verarbeiten und speichern kann, die dem Kunden von Hinweisgebern übermittelt werden. Die Anwendung ist so konzipiert,

tool but, to the extent not regulated by the Terms, the Client decides how they use the Application. The personal data and other information that are intended to be collected and processed in the Application are listed in the Appendix 1. 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. 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.	dass sie als interner Meldekanal funktioniert, aber in dem Maße, wie es nicht durch die Bedingungen geregelt ist, entscheidet der Kunde, wie er die Anwendung nutzt. Die personenbezogenen Daten und sonstigen Informationen, die in der Anwendung erfasst und verarbeitet werden sollen, sind in Anhang 1 aufgeführt. Die in Anlage 1 aufgeführten Daten und Informationen werden in der vom Dienstleister betriebenen und auf einem virtuellen Server in der EU gehosteten Datenbank der Anwendung gespeichert, und zwar im Namen und für Rechnung des Kunden. Eine Übermittlung von Daten in Drittländer außerhalb des Europäischen Wirtschaftsraums erfolgt nur mit vorheriger Zustimmung des Kunden und nur dann, wenn die in den Artikeln 44 ff. der DSGVO festgelegten besonderen Bedingungen erfüllt sind. Der Dienstleister verarbeitet die genannten personenbezogenen Daten und andere Informationen in der Anwendung ausschließlich für den Betrieb und die Wartung der Anwendung, ihrer Webseiten und der Datenbank.
3. Technical and Organizational Measures 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. 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. 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.	**3. Technische und organisatorische Maßnahmen** Die technischen und organisatorischen Maßnahmen sowie deren Umsetzung und Einhaltung sind in Anlage 2 aufgeführt. Soweit sich bei der Prüfung/Auditierung durch den Kunden ein Änderungsbedarf ergibt, werden diese einvernehmlich umgesetzt. Der Dienstleister stellt die Sicherheit der Daten gemäß den Anforderungen der DSGVO sicher. Bei den zu treffenden Maßnahmen handelt es sich um Maßnahmen der Datensicherheit und Maßnahmen, die ein dem Risiko angemessenes Schutzniveau hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme gewährleisten. Die technischen und organisatorischen Maßnahmen sind dem technischen Fortschritt und der Weiterentwicklung unterworfen. Insofern ist es dem Dienstleister gestattet, alternative angemessene Maßnahmen zu ergreifen. Das Sicherheitsniveau der festgelegten Maßnahmen darf nicht beeinträchtigt werden. Wesentliche Änderungen sind zu dokumentieren.

4. Requests by Affected Persons 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 contacts the Service Provider directly in this respect, the Service Provider will immediately forward this request to the Client without delay.	**4. Anträge von Betroffenen** Der Dienstleister darf Daten nicht auf direkte Aufforderung durch Betroffene berichtigen, löschen oder deren Verarbeitung einschränken. Sofern sich ein Betroffener diesbezüglich direkt an den Dienstleister wendet, wird der Dienstleister dieses Verlangen unverzüglich an den Auftraggeber weiterleiten.
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.	**5. Qualitätssicherung und sonstige Pflichten des Dienstleisters** Neben der Einhaltung der Bestimmungen dieses Vertrages hat der Dienstleister die gesetzlichen Pflichten nach Art. 28 bis 33 DSGVO zu erfüllen; dabei hat er insbesondere die Einhaltung der folgenden Anforderungen sicherzustellen: • Vertraulichkeit gemäß Artikel 28, Absatz 3, Satz 2, Klausel b, Artikel 29 und Artikel 32, Absatz 4. Der Dienstleister betraut nur solche Personen mit der in diesem Vertrag definierten Datenverarbeitung, die zur Vertraulichkeit verpflichtet und zuvor mit den für ihre Tätigkeit relevanten Datenschutzbestimmungen vertraut gemacht worden sind. Der Dienstleister und jede ihm unterstellte Person, die Zugang zu personenbezogenen Daten hat, darf diese Daten nur nach den Weisungen des Kunden (einschließlich der in diesem Vertrag und in den Bedingungen erteilten Befugnisse) verarbeiten, es sei denn, dies ist gesetzlich vorgeschrieben. • Der Dienstleister und der Kunde arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. • Der Kunde wird unverzüglich über Kontrollen und Maßnahmen der Aufsichtsbehörde unterrichtet, soweit sie sich auf die Verarbeitung personenbezogener Daten im Rahmen dieses Vertrages beziehen. Dies gilt auch, wenn gegen den Dienstleister im Zusammenhang mit Verstößen gegen zivil- oder strafrechtliche Gesetze, Verwaltungsvorschriften oder Verordnungen über die Verarbeitung personenbezogener Daten im Rahmen dieses Vertrages ermittelt

• 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.
• 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).
	wird oder er Gegenstand einer Untersuchung durch eine zuständige Behörde ist.
	• Sofern der Kunde einer Prüfung durch die Aufsichtsbehörde, einem Ordnungswidrigkeiten- oder Strafverfahren, einem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem sonstigen Anspruch im Zusammenhang mit der Verarbeitung personenbezogener Daten im Rahmen dieses Vertrages ausgesetzt ist, wird der Dienstleister alle Anstrengungen unternehmen, um den Kunden nach besten Kräften zu unterstützen.
	• Der Dienstleister überwacht regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um sicherzustellen, dass die Verarbeitung in seinem Verantwortungsbereich in Übereinstimmung mit den Anforderungen des geltenden Datenschutzrechts erfolgt und die Rechte der betroffenen Personen geschützt werden.
	• Der Dienstleister benachrichtigt den Kunden unverzüglich, spätestens jedoch 24 Stunden, nachdem er von einer Sicherheitsverletzung Kenntnis erlangt hat, schriftlich darüber. Diese Benachrichtigung muss mindestens und soweit dies angesichts der Art des Vorfalls möglich ist, Folgendes enthalten:
	  • Informationen über die Art der festgestellten Sicherheitsverletzung,
	  • welche Kategorien von registrierten Personen davon betroffen sind, und
	  • die ungefähre Anzahl der betroffenen registrierten Personen, einschließlich der Kategorien umfassender personenbezogener Daten und deren Anzahl, sowie die Präventiv- oder Abhilfemaßnahmen, die der Dienstleister infolge der festgestellten Sicherheitsverletzung ergriffen hat.
	Der Dienstleister unterstützt den Kunden bei der Einhaltung der Verpflichtungen in Bezug auf die Sicherheit personenbezogener Daten, die Meldepflicht bei Datenschutzverletzungen, die Datenschutz-Folgenabschätzung und die vorherige Konsultation gemäß den Artikeln 32 bis 36 der DSGVO.

	Für Unterstützungsleistungen, die nicht auf Mängel seitens des Dienstleisters zurückzuführen sind, kann der Dienstleister eine Entschädigung zum Stundensatz von 250 CHF (ohne MwSt.) verlangen.
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 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.	**6. Unterauftragsvergabe** Der Dienstleister beauftragt dritte Dienstleister (Unterauftragnehmer) mit der Bereitstellung der Anwendung. Die Liste der Unterauftragnehmer findet sich in Anhang 1. Der Dienstleister informiert den Kunden 10 (zehn) Tage im Voraus über die Beauftragung eines neuen Unterauftragnehmers. Der Kunde kann der Beauftragung eines Unterauftragnehmers durch den Dienstleister aus angemessenen datenschutzrechtlichen Gründen schriftlich widersprechen, indem er den Dienstleister unverzüglich innerhalb von 5 (fünf) Tagen nach Erhalt der Mitteilung des Dienstleisters schriftlich darüber informiert. In dieser Mitteilung sind die angemessenen Gründe für den Einspruch zu erläutern. In einem solchen Fall erörtern die Parteien die Bedenken des Kunden nach Treu und Glauben mit dem Ziel, eine wirtschaftlich angemessene Lösung zu finden.
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).	**7. Das Recht des Kunden auf Überprüfung** Der Kunde hat das Recht, auf eigene Kosten Inspektionen durchzuführen oder durch unabhängige Dritte durchführen zu lassen, um die Einhaltung dieses Vertrags durch den Dienstleister zu überprüfen. Jede Kontrolle durch den Kunden ist dem Dienstleister rechtzeitig anzukündigen. Der Dienstleister stellt sicher, dass der Kunde die Einhaltung der Verpflichtungen des Dienstleisters gemäß Artikel 28 der DSGVO überprüfen kann. Der Dienstleister ist verpflichtet, dem Kunden auf Verlangen die erforderlichen Auskünfte zu erteilen und insbesondere die Durchführung der technischen und organisatorischen Maßnahmen nachzuweisen. Der Dienstleister kann einen Vergütungsanspruch für die Ermöglichung von Kontrollen des Kunden mit einem Stundensatz von 250 CHF (exkl. MwSt.) geltend machen.

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.	Der Dienstleister kann den Kunden nach eigenem Ermessen bei anderen von diesem durchgeführten Überprüfungen unterstützen, u.a. beim Ausfüllen von Fragebögen des Kunden zu Sicherheit, Datenschutz, Datenverarbeitung und ähnlichen Themen im Zusammenhang mit der Anwendung. In solchen Fällen kann der Dienstleister einen Vergütungsanspruch mit dem Stundensatz aus dem vorstehenden Absatz geltend machen.
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.	**8. Anweisungen des Kunden** Mündliche Anweisungen hat der Kunde unverzüglich schriftlich zu bestätigen. Der Dienstleister informiert den Kunden unverzüglich, wenn er der Meinung ist, dass eine Anweisung gegen datenschutzrechtliche Bestimmungen verstösst. Der Dienstleister ist dann berechtigt, die Ausführung der betreffenden Anweisung auszusetzen, bis der Kunde die Anweisung bestätigt oder abändert.
9. Deletion and Return of Personal Data 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. 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. 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.	**9. Löschung und Rückgabe von Personendaten** Kopien oder Duplikate der Daten dürfen nicht ohne Wissen des Kunden erstellt werden, ausgenommen Sicherungskopien, soweit sie für eine ordnungsgemäße Datenverarbeitung erforderlich sind, sowie Daten, die zur Erfüllung gesetzlicher Aufbewahrungspflichten benötigt werden. Der Dienstleister wird bei Beendigung der Bedingungen und damit dieses Vertrages nach Wahl des Kunden entweder i) die Daten endgültig löschen oder ii) alle Daten an den Kunden zurückgeben und dann alle vorhandenen Kopien endgültig löschen, es sei denn, der Dienstleister ist zur Aufbewahrung dieser Daten gesetzlich verpflichtet. Ungeachtet der vorstehenden Regelung ist der Dienstleister berechtigt, Kopien von Daten zu speichern, soweit dies erforderlich ist, um die vertragsgemäße Leistungserbringung zu dokumentieren oder um sich gegen Rechtsansprüche zu verteidigen. In einem solchen Fall dürfen die personenbezogenen Daten des Kunden vom Dienstleister nur zu den genannten Zwecken verarbeitet werden.

Upon request, the Service Provider shall provide the Client with information on nature and the time of the data's deletion.	Der Dienstleister erteilt dem Kunden auf Anfrage Auskunft über Art und Zeitpunkt der Löschung der Daten.
10. Final Provisions	**10. Schlussbestimmungen**
Modifications 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 trusty.report webpages or through the Application. Such amended Agreement will become effective 10 (ten) days after their posting in the Application. 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. Term of the Agreement 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. The right to isolated extraordinary notice of cancellation hereby remains intact, as do statutory rights of rescission. Jurisdiction The parties agree that any claims and disputes that may arise from the agreement shall be settled by the court in Zug, Switzerland.	Änderungen Der Dienstleister behält sich das Recht vor, nach eigenem Ermessen jederzeit Teile des Vertrags zu ändern, zu modifizieren, hinzuzufügen oder zu entfernen, indem er solche Änderungen auf den trusty.report-Webseiten oder über die Anwendung veröffentlicht. Solcher geänderten Vertrag tritt 10 (zehn) Tage nach seiner Veröffentlichung in der Anwendung in Kraft. Der Kunde ist verpflichtet, diesen Vertrag regelmäßig auf Änderungen zu überprüfen. Die fortgesetzte Nutzung der Anwendung nach Inkrafttreten solcher Änderungen bedeutet die verbindliche Annahme dieser Änderungen durch den Kunden. Laufzeit dieses Vertrages Dieser Vertrag tritt zwischen den Parteien zusammen mit den Bedingungen in Kraft und endet auch mit der Kündigung oder einer sonstigen Beendigung der Bedingungen. Das Recht zur isolierten außerordentlichen Kündigung bleibt hiervon ebenso unberührt wie die gesetzlichen Rücktrittsrechte. Gerichtsstand Die Parteien vereinbaren, dass für alle Ansprüche und Streitigkeiten, die sich aus diesem Vertrag ergeben können, das Gericht in Zug, Schweiz, zuständig ist.
Appendix 1 to the Data Processing Agreement	**Anlage 1 zum Vertrag über die Datenverarbeitung**
List of Personal Data and Other Information Processed in the Application	**Liste der personenbezogenen Daten und anderer Informationen, die in der Anwendung verarbeitet werden**
• personal data relating to a whistleblower (reporting person), if provided: first name, last name, address, email address, telephone number, relationship toward the Client;	• Personenbezogene Daten des Hinweisgebers (der meldenden Person), falls angegeben: Vorname, Nachname, Adresse, E-Mail-Adresse, Telefonnummer, Beziehung zum Kunden;

• 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; • personal data relating to the users of the Application authorised by the Client: first name, last name, email address, function with the Client.	• personenbezogene Daten der Personen, die verdächtigt werden, an dem Verstoß/Fehlverhalten beteiligt zu sein, und der Personen, die von dem Verstoß/Fehlverhalten wissen, falls angegeben: vollständiger Name, Position, Organisation; eine sachliche Beschreibung des Verstoßes/Fehlverhaltens sowie eine Beschreibung der Umstände des Vorfalls, einschließlich Zeit und Ort des Vorfalls; • personenbezogene Daten der vom Kunden autorisierten Nutzer der Anwendung: Vorname, Nachname, E-Mail-Adresse, Funktion beim Kunden.

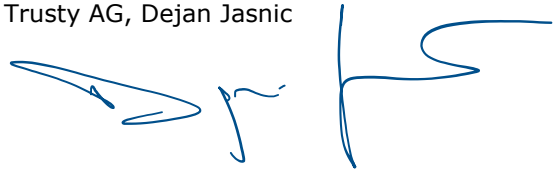
List of subcontractors:
• Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany;
  ○ Provides hosting of the Application on the virtual server in Nuremberg, Germany;
• AWS EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxembourg;
  ○ Provides notification email relay service.
	Liste von Unterauftragnehmern:
	• Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland;
	  ○ Bietet das Hosting der Anwendung auf dem virtuellen Server in Nürnberg, Deutschland;
	• AWS EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxembourg;
	  ○ Bietet einen E-Mail-Relay-Dienst für Benachrichtigungen an.

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	**Anlage 2 zum Vertrag über die Datenverarbeitung** **Technische und organisatorische Massnahmen** Der Dienstleister verhindert den unberechtigten internen Zugriff auf die Anwendung durch regelmässige Sicherheitsupdates nach dem Stand der Technik und sichert damit kritische Netzzugänge ab. Die Vergabe von Berechtigungen an die Mitarbeiter des Dienstleisters ist revisionssicher. Der elektronische Zugang des Kunden zur Anwendung ist passwortgeschützt. Nach der Eröffnung des Kundenanwendungskontos muss das anfängliche Benutzerpasswort vom Kunden geändert werden und ist dem Dienstleister nicht bekannt. Das Passwort des Kunden wird vom Kunden selbst festgelegt; das Passwort muss den vordefinierten Richtlinien bezüglich der Mindestanzahl von Zeichen und Zahlen entsprechen. Der

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). 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. 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. 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. 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.	Kunde ist für die Autorisierung und Eröffnung zusätzlicher Benutzerkonten für die Anwendung verantwortlich. Die Daten der Anwendung werden physisch oder logisch isoliert und getrennt von anderen Daten des Dienstleisters gespeichert. Backups der Daten werden unter Verwendung eines ähnlichen Systems der physischen oder logischen Isolierung durchgeführt. Backups aller Anwendungsdaten werden täglich durchgeführt. Ausfallsicherheitsmaßnahmen wie Sicherheitsprogramme (Firewalls, Verschlüsselungsprogramme, Spamfilter) und die Überwachung aller relevanten Server werden eingesetzt. Um die Vertraulichkeit zu gewährleisten, speichert die Anwendung keine IP-Adressen und Zeitstempel. Die Anwendung unterstützt den Betrieb in einer Serverfarm und gewährleistet einen ununterbrochenen Betrieb (24x7x365). Eine beliebige Skalierbarkeit für Leistung und zusätzliche Dienste ist gegeben. Es werden keine lizenzierten Programme verwendet. Die Software verwendet Open-Source-Lösungen (Mysql, Apache, Laravel, jQuery, Bootstrap). Um die Sicherheit und den Datenschutz bei der Datenübertragung zu gewährleisten, wird eine SSL/TLS-Verschlüsselung eingesetzt. Textdaten aus dem Inhalt der Berichte und aus dem Kommunikationskanal mit einem Hinweisgeber werden mit dem symmetrischen AES-CBC-Algorithmus unter Verwendung der OpenSSL-Erweiterung verschlüsselt. Die Dateien werden mit AES 256 CTR verschlüsselt. Alle Passwörter in der Anwendung werden mit dem Bcrypt-Algorithmus komprimiert. Die Anwendung verwendet Linux Iptables/Netfilter Firewall. Die Pseudonymisierung der Daten von Hinweisgebern wird durch zufällig generierte Benutzernamen für jeden einzelnen Hinweisgeber gewährleistet. Das Programm zeichnet einen Prüfpfad für jede Eingabe/Einsicht/Änderung auf. Alle Zugriffs- und Schlüsselereignisse werden protokolliert, und diese Protokolle sind für den Dienstleister bei Bedarf zugänglich. Beendete Anwendungskonten werden dauerhaft gelöscht und überschrieben. Der Kunde kann Inhalte einzelner Berichte selbst löschen; in diesem Fall werden die Inhalte ebenfalls dauerhaft gelöscht und überschrieben.

	Der Dienstleister beauftragt regelmässig einen Drittanbieter mit der Durchführung eines Penetrationstests der Applikation und behebt anschliessend allfällige identifizierte Sicherheitslücken.
Subcontractors 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. 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. Both documents are incorporated into this Agreement by reference and are available at https://trusty.report/documents/.	**Unterauftragnehmer** Die technischen und organisatorischen Maßnahmen (hier auch TOMs genannt) in Bezug auf den Hosting-Server sind in sind im Vertrag zwischen dem Dienstleister und der Hetzner Online GmbH, Anlage 2 beschrieben. Die technischen und organisatorischen Maßnahmen in Bezug auf die E-Mail-Relay-Dienste sind im Vertrag zwischen dem Dienstleister und SMTP.de ApS, Annex 1, geregelt. Beide Dokumente werden durch Verweis in den Vertrag aufgenommen und sind unter https://trusty.report/documents/ abrufbar.
PUBLISHED ON March 1st 2023	**VERÖFFENTLICHT AM 1. März 2023**

Trusty AG, Dejan Jasnic



(Trusty Client/ Trusty Kunde)_____