Datensicherheitskonzept: Technische und Organisatorischen Maßnahmen der ConfTool GmbH zur Datensicherheit und zum Datenschutz (Stand: März 2024)
Anlage 3 der Vereinbarung zur Auftragsverarbeitung

1. Verantwortlichkeiten

Die Kontrolle der Einhaltung der gesetzlichen Regelungen für die IT-Sicherheit und den Datenschutz obliegen dem Geschäftsführer, Herrn Diplom-Informatiker Dr. Harald Weinreich. Er ist damit zugleich Verantwortlicher für die IT-Sicherheit den Datenschutz.

2. Gebäudesicherung, Eingangssicherung, Raumsicherung

Alle Daten verarbeitenden Server und Backup-Systeme befinden sich in Räumen der Firma Hetzner Online GmbH in Falkenstein/Vogtland, Deutschland.

Zugang zu den Servern wird nur autorisierten Vertragspartnern mit Terminvereinbarung gewährt, die sich vor Ort ausweisen können. Vertretungsberechtigte benötigen eine schriftliche Bestätigung des Vertragspartners.

Die Datacenterparks der Hetzner Online GmbH sind mit Sicherheitszäunen gesichert. Eingänge und Serverräume sind videoüberwacht.

Das Gebäudesicherungskonzept von Hetzner findet man unter: http://www.hetzner.de/pdf/Sicherheit.pdf

Die Hetzner Online GmbH ist **zertifiziert nach DIN ISO/IEC 27001.** https://www.hetzner.de/de/hosting/unternehmen/zertifizierung

Der Hauptsitz der ConfTool GmbH befindet sich in einem Wohnhaus. Die Gebäudetür, die Tür zum Büro und die Türen zu den Büroräumen sind durch einfache Schließanlagen und eine Alarmanlage gesichert. Zutritt ist nur über Einlass durch den Geschäftsführer möglich.
Im Büroraum findet kein Publikumsverkehr statt.

3. Zugangskontrolle zum EDV-System

Zugang wird nur autorisierten Vertragspartnern mit Terminvereinbarung gewährt, die sich vor Ort ausweisen können. Vertretungsberechtigte benötigen eine schriftliche Bestätigung des Vertragspartners.

Zugang zu den Serverräumen ist nur in Begleitung eines Mitarbeiters möglich. Siehe hierzu auch das Sicherungskonzept von Hetzner: http://www.hetzner.de/pdf/Sicherheit.pdf

Die Hetzner Online GmbH wurde nach den Anforderungen an ein Informationssicherheitsmanagementsystem (ISMS) gemäß DIN ISO/IEC 27001 zertifiziert. Die Infrastruktur und der Betrieb des gesamten Datacenterparks in Falkenstein/Vogtland wurde durch die FOX Certification geprüft. Weitere Informationen findet man unter: https://www.hetzner.de/de/hosting/unternehmen/zertifizierung

Die Nutzung von Datenübertragungsgeräten (Internet) ist nur durch Autorisierung möglich.

Der Zugang zu Büroräumen oder den Homeoffice Standorten der ConfTool GmbH wird nur persönlich bekannten Personen unter Aufsicht gewährt. Das Gebäude ist durch eine Alarmanlage der Firma TELENOT ELECTRONIC GmbH gesichert.

4. Zugriffskontrolle

Das Konferenz-Management-System ConfTool Pro implementiert die Zugriffskontrolle auf die Benutzer- und Teilnehmerdaten, indem jedem Benutzer eine entsprechende Rolle (Administrator, Konferenzorganisator, Frontdesk, Teilnehmer etc.) zugewiesen wird. Die Benutzerrolle legt die Zugriffsmöglichkeiten fest.

Ein Zugriff auf sämtliche Daten des Konferenz-Management-Systems ist nur über die Webschnittstelle möglich und erfordert einen individuellen Benutzernamen und ein Passwort.
Für Passwörter gelten Regeln: Die minimale Länge beträgt 5 Zeichen, es müssen unterschiedliche Buchstaben und Zahlen enthalten sein und triviale Passwörter (wie „12345“) sind gesperrt.
Optional lässt sich die Anforderung auf mindestens 8 Zeichen mit min. einem Sonderzeichen, Zahlen, Groß- und Kleinbuchstaben festsetzen.
Alle persönlich gesetzten Passwörter werden als gesalzene Hashes mit bcrypt verschlüsselt gespeichert und sind auch für Administratoren nicht zugänglich.

Nach 10 erfolglosen Login-Versuchen wird das Login für 10 Minuten für die betreffende IP-Adresse und den Benutzer gesperrt. Auf diese Weise werden „Brute-Force“-Angriffe verhindert.
Zusätzlich lassen sich sowohl für das Login (nach 3 missglückten Logins) als auch die Registrierung neuer Benutzerkonten ein (barrierefreies) zwei unterschiedliche CAPTCHA-Optionen aktivieren (Google *reCaptcha* und *SecurImage* Captcha von ConfTool).
Die Sitzungszeit für unterschiedliche Benutzergruppen lässt sich – je nach Sicherheitsanforderung – unterschiedlich einstellen. Für Administratoren erfolgt in der Regel nach einer Untätigkeit von einer Stunde ein automatisches Logout, für „normale“ Benutzer hingegen in der Regel erst nach 5 Stunden, da diese häufig für die Eingabe von Einreichungen oder Gutachten sehr lange benötigen und der potenzielle Schaden eines „Session-Hijackings“ sich in solchen Fällen sehr in Grenzen hält.
Administratoren der ConfTool GmbH verwenden (auch bei Homeoffice-Einsatz) für jede Instanz unterschiedlichen Passwörter, Passwörter sind mit AES256 verschlüsselt und es gibt als zweite Passwortschwelle „One-Time-Passwords“ bzw. eine Prüfung der IP-Adresse des Zugriffsrechners.

Ein Zugriff auf Daten durch die Hetzner GmbH ist nicht möglich, die Firma hat keine Zugangsdaten zu den Servern (siehe auch Zugang/Zutritt).

Für den Zugriff auf Systemebene wird nur SSH bzw. SFTP mit Private-/Public-Key-Verfahren verwendet. Die privaten Schlüssel sind zusätzlich mit einem Passwort gesichert.

Der Zugriff auf Dateien im Upload-Bereich des ConfTool-Systems ist ebenfalls nur über die Webschnittelle, nicht aber direkt über den Web-Server möglich. Der Zugriff im ConfTool wird über Benutzerkonten gesteuert. Die Dateien sind als Grundeinstellung nur Teilnehmern mit erfolgter Anmeldung über das eigene Benutzerkonto zugänglich.

Durch die Mitarbeiter der ConfTool GmbH erfolgt keine Eingabe, Veränderung oder Löschung von Daten im ConfTool-System.

Verschlüsselungen aller Firmendaten der ConfTool GmbH (auch bei Homeoffice-Einsatz) erfolgen durch „VeraCrypt“ mit AES256. Ebenfalls sind alle Backup-Medien mit Firmendaten entsprechend verschlüsselt.

4.1 Eingabe und Veränderung

Eine umfassendere Bearbeitung von Teilnehmerdaten ist begrenzt auf den Konferenzleiter und auf Mitarbeiter, denen der Konferenzleiter im ConfTool-System entsprechende Rollen zuweist.

Die Teilnehmer selbst können nur ihre eigenen Daten eingeben, ändern oder löschen. Die Zuordnung wird über Benutzerprofile mit der Mail-adresse und dem Benutzernamen als Schlüsselattribute sichergestellt.

Anmeldungen, Eingaben, Veränderungen und Löschungen durch Benutzer des ConfTool Systems werden aufgezeichnet und sind in einem Log-Bereich für die Organisatoren der Veranstaltung zugänglich. Das Log lässt sich durch die Organisatoren deaktivieren, sofern Bedenken bezüglich des Datenschutzes bestehen.

4.2 Löschkonzept	Mit dem Ende der Vertragslaufzeit erfolgt eine Zerstörung der Datenbank mit allen Daten und aller Backup-Dateien. Die Datenbank wird mittels „drop database“ zerstört; damit ist eine Wiederherstellung der Datenbank mit forensischen Mitteln nur unmittelbar nach der Zerstörung und auch nur demjenigen möglich, der physischen Zugriff auf den Datenspeicher/die Festplatte oder eine Abbilddatei davon hat. Backup-Dateien werden beim endgültigen Löschen mittels „wipe“ mit Zufallszahlen überschrieben, eine Wiederherstellung ist damit nach heutigem Kenntnisstand auch mit forensischen Mitteln unmöglich. Weitere Informationen sind im Löschkonzept der ConfTool GmbH vermerkt.
5. Sicherung der Kommunikation	Sämtlicher Zugriff auf das ConfTool-System als auch die Eingabe der Teilnehmerdaten erfolgen ausschließlich über verschlüsselte Verbindungen (https). Es werden **EV (Extended Validation)**-Zertifikate der Firma *Sectigo Limited* mit SHA-2 und 4096 Bit Länge verwendet. Die Administration des Serverpools und die Administration der ConfTool-Software als auch die Sicherung der Daten erfolgt ebenfalls ausschließlich auf verschlüsselte Weise. Unsere Mail-Server nutzen zum Transport Verschlüsselung per STARTTLS (TLS 1.2 und 1.3), wobei ebenfalls offizielle Zertifikate der Firma *Sectigo Limited* zum Einsatz kommen. Unsere Server verfügen über gültige SPF-Einträge, DKIM-Signaturen und entsprechende DMARC DNS-Einträge. Für die Kommunikation per E-Mail steht darüber hinaus die Verschlüsselung mit PGP zur Verfügung, sofern vom Kunden gewünscht.
6. Kontrolle der Weitergabe	Firmendaten werden auf den Servern der ConfTool GmbH bei der Hetzner GmbH gespeichert.
6.1 Verschlüsselung bei der Datenübertragung	Es wird WebDAV per HTTPS/SSL mit SHA-2-Zertifikaten von der Firma *Sectigo Limited* eingesetzt.
6.2 Datenträgertransport	Findet nicht statt.
6.3 Übermittlungskontrolle	Es werden Daten ausschließlich an bekannte und zuzuordnende interne Adressaten sowie den Ansprechpartner des Vertragspartners nach Schlüssigkeit übermittelt.
7. Trennungsgebot	Das System ist so gestaltet, dass die Daten tagungsbezogen in getrennten Datenbanken organisiert sind. Hochgeladene Dateien (Uploads) von Autoren und Organisatoren werden ebenfalls tagungsbezogen in jeweils gesonderten Verzeichnissen gespeichert.
Datenbank	Einziger Zugang für alle Benutzer des ConfTool-Systems zur Datenbank besteht über die Webschnittstelle des Systems. Ein direkter Zugriff auf die Server oder das Datenbanksystem ist für Kunden nicht möglich.
Upload-Bereich	Zugriff auf die hochgeladenen Dateien ist ebenfalls nur über die Webschnittstelle von ConfTool möglich.

8. Verfügbarkeitskontrolle

Der ConfTool GmbH stehen Ersatzserver zur Verfügung, sodass diese bei unvorhersehbaren Ausfällen zum Einsatz kommen können.

Die Stromzufuhr wird über eine redundante, unterbrechungsfreie Stromversorgung (USV) sichergestellt.

Das qualifizierte Fachpersonal der Hetzner GmbH leistet durch den „24/365-Stand-by-Service“ Support für die ConfTool GmbH. Die Hetzner GmbH sichert einen Austausch von defekter Hardware innerhalb von höchstens 4 Stunden zu. Unserer Erfahrung nach erfolgt dies in der Regel in unter 30 Minuten.

8.1 Daten und Backups

Alle Datenbanken werden mindestens zwölfmal täglich (in der Regel stündlich) auf zwei weiteren kommerziellen, in Deutschland befindlichen Mietservern der Hetzner GmbH automatisch gesichert. Die Übertragung der Daten erfolgt nur mit gesicherten Verbindungen.

Nach 7 Tagen werden die stündlichen Backups gelöscht und nur noch tägliche Backups vorgehalten. Die täglichen Backups werden nach 12 Monaten automatisch unwiderruflich gelöscht.

Auf Anfrage des Kunden können Backups auch sofort nach Deinstallation und unwiederbringlich gelöscht werden.

Für Backups über längere Zeiträume nach Deinstallation des Systems sind die Kunden zuständig. Das ConfTool-System bietet entsprechende Export-Funktionen für den Kunden.

Vor dem Löschen einer Instanz des ConfTool-Systems wird in jedem Falle der Kunde konsultiert und erst nach der Bestätigung des Sicherns der Daten durch den Kunden das Löschen durchgeführt.

Während des Löschvorgangs wird der Name der Instanz als auch der Kunden angezeigt, um Verwechslungen zu verhindern. Löschvorgänge werden immer durch 2 Mitarbeiter gleichzeitig durchgeführt, um Fehler zu verhindern.

8.2 Hardware und Netzwerk

Die Funktion der Stromversorgung und des Netzwerkes wird von den Mitarbeitern der Hetzner GmbH im „24/365-Stand-by-Service“ überwacht.

Mehrere **Monitoring-Systeme** überwachen die Verfügbarkeit und die Last der Server. Bei Ausfällen oder Auffälligkeiten erfolgt innerhalb von 5 Minuten eine Benachrichtigung der Mitarbeiter der ConfTool GmbH per E-Mail und SMS.

Die Hetzner GmbH bietet für alle Server spezielle Hardware zum Schutz gegen **DDOS-Angriffe** auf Netzwerkebene. Mehr Details unter: https://www.hetzner.de/de/hosting/unternehmen/ddos-schutz

Die Ausfallsicherheit des Netzwerkes wird durch vielfach redundante Upstreams sichergestellt:
1. Peerings (2830 GBit/s): 1300 GBit/s DE-CIX, 300 GBit/s AMS-IX, 200 GBit/s FICIX, 100 GBit/s NL-IX, 100 GBit/s France-IX, 100 GBit/s ECIX und viele weitere.
2. Transit networks (4100 Gbit/s): 900 GBit/s core Backbone, 600 GBit/s Telia, 400 GBit/s GTT, 400 GBit/s TATA, 400 GBit/s DTAG und viele weitere.
3. Private Peerings (5090 GBit/s): 800GBit/s Google, 400GBit/s Cloudflare, 400GBit/s OVH, 200 GBit/s Amazon, 200GBit/s Facebook, 200GBit/s Microsoft und viele weitere.

Siehe: https://www.hetzner.de/hosting/unternehmen/rechenzentrum

8.3 Planung für den Totalausfall

Die Server sind auf 2 deutsche Rechenzentren der Hetzner GmbH verteilt. Sollte ein Zentrum ganz ausfallen, so kann jeweils einer der Backup-Server die Aufgaben des ausgefallenen Servers übernehmen.

9. Sicherung der Server

Alle Server sind mit einer Firewall ausgestattet. Die Firewall wird mittels einer Monitoring-Software überwacht.

Die Firewalls blockieren grundsätzlich alle nicht notwendigen Ports. Zudem sind Regeln gegen Brute-Force-Angriffe im Einsatz.

Ergänzend hierzu wird das Werkzeug fail2ban eingesetzt, ein Intrusion Prevention System, das zum automatischen Bestimmen und Blockieren von IP-Adressen dient, von denen mehrere fehlgeschlagene Verbindungsversuche stattgefunden haben.

Alle von Kunden im ConfTool-System hochgeladenen Dateien als auch alle an die ConfTool GmbH gesendeten E-Mails werden mit dem Anti-Viren-Programm „ClamAV“ nach Viren gescannt. Das Anti-Viren-Programm wird täglich automatisch aktualisiert.

E-Mails mit ausführbaren Attachments werden bereits vom Mail-Server aus Sicherheitsgründen abgelehnt. Hierzu gehören auch .docm und .doc-Dateien, da diese Trojaner in Form von Word-Makros enthalten können.

Eine Ausführung hochgeladener Dateien auf den Servern ist aufgrund der Systemstruktur und der Dateiattribute verhindert.

Alle Server werden in der Regel monatlich, aber mindestens vierteljährlich, von der Firma *Sectigo Limited* auf Sicherheitslücken gescannt (gemäß den Anforderungen für eine PCI-Konformität).
Siehe: https://www.hackerguardian.com/frequently-asked-questions

Die entsprechenden Protokolle sind auf Anfrage erhältlich.

9.1 Missbrauchskontrolle

Versuche des unautorisierten Zugriffs auf die Server über das Netzwerk (ssh, smtp, https) werden für alle Server protokolliert und stündlich per E-Mail an die Mitarbeiter der ConfTool übermittelt. Das Intrusion Prevention System blockiert dabei entsprechende IP-Adressen automatisch.

9.2 Vertragsrechenzentren

Die Vertragsrechenzentren der Firma Hetzner GmbH befinden sich in Falkenstein/Vogtland.

Sie sind räumlich verteilt und von außen als solche nicht erkennbar. Straßenangaben werden eigenen Kunden nur auf Anfrage mitgeteilt. Es handelt sich um dedizierte Server.

Für die Server gibt es vor Ort Fachpersonal, das an allen Tagen des Jahres rund um die Uhr verfügbar ist.

9.3 Betriebssysteme

Die Server und Backup-Systeme laufen unter Ubuntu-Linux (Ubuntu Pro, Server-Version 20.04 LTS / 22.04 LTS).

Sicherheits-Updates werden täglich durchgeführt, sofern Updates existieren. Die Überprüfung auf Updates geschieht automatisch, die Installation wird manuell eingeleitet.

9.4 Software-Dienste

Auf den Servern sind nur die notwendigen Dienste und Programme installiert, um eine Kompromittierung durch Sicherheitslücken zu minimieren. Zugänglich über das Internet sind nur:

Apache 2.4 mit mod-ssl (auf Port 443, nur TLS 1.2 und 1.3 sind aktiviert) und PHP 7.4.3 bzw. 8.1.2, jeweils mit aktuellen Sicherheits-Patches des Ubuntu-Serverpakets.

In PHP wurden alle unnötigen, sicherheitskritischen Funktionen deaktiviert. Siehe:
http://www.conftool.net/en/technical_documentation/security_hints.html

OpenSSH 9.6p1 (der SSH-Server läuft nicht auf dem Standard-Port 22, logins sind nur mit privater Schlüsseldatei möglich)

	Postfix 3.3.0 mit aktuellen Patches des Ubuntu-Pakets (dedizierter Mail-Server)
9.5 Datenträger	Bei den Massenspeichern handelt es sich um RAID1-Fesplattensysteme mit Hardware-RAID-Controllern, um die Wahrscheinlichkeit eines Datenverlustes auf ein Minimum zu reduzieren. Als Festplatten werden nur dauerbelastbare HDDs der Enterprise-Klasse eingesetzt. Der Zustand des RAID-Systems wird 10-minütig überwacht und bei außergewöhnlichem Zustand werden die Mitarbeiter der ConfTool GmbH automatisch per E-Mail benachrichtigt. Der Austausch einer Festplatte führt in der Regel im „Hot-Swap“-Verfahren ohne Systemausfall.
9.6 Löschungen bei Außerbetriebnahme	Wenn ein Server außer Betrieb genommen wird, so wird zuvor der Server von der ConfTool GmbH mit einem Rescue-System über das Netzwerk gebootet und danach werden die Festplatten mit dem Tool „dd“ zweimal komplett überschrieben und somit unwiderruflich gelöscht. Zudem garantiert der Betreiber der Datacenter Parks Hetzner Online GmbH, dass alle außer Betrieb genommenen Festplatten entweder mehrfach überschrieben oder zerstört (geschreddert) werden. https://www.hetzner.com/AV/TOM.pdf
10. Sicherung der Mitarbeiter-PCs	Alle PCs sind mit einer Firewall und einem Virenscanner ausgestattet. Das Anti-Viren-Programm wird täglich automatisch aktualisiert. Ausstehende Sicherheitsupdates werden jeweils täglich (automatisch) und so schnell wie möglich eingespielt. Alle PCs werden zudem wöchentlich mithilfe eines zusätzlichen Werkzeugs auf ausstehende Updates bei den installierten Programmen überprüft (aktuell mit „PatchMyPC“). Auf allen PCs sind nur für die Arbeit notwendige Programme installiert. Verschlüsselungen aller Firmendaten auf den PCs erfolgen durch „VeraCrypt“ mit AES256. Ausführbare Dateien als E-Mail-Anhänge werden bereits vom Mail-Server abgelehnt und nicht an Mitarbeiter weitergeleitet. In den Office-Anwendungen wurde die Ausführung von Makros grundsätzlich deaktiviert. Für die Anzeige von PDF-Dateien werden nur PDF-Viewer verwendet, die keine Makros ausführen. Die Windows Powershell wurde so konfiguriert, dass sie nur von Microsoft signierte Programme ausführen kann. Nicht notwendige Windows 10-Dienste wie Cortana als auch die Übermittelung von Telemetriedaten an Microsoft wurden soweit wie möglich deaktiviert. Alle Mitarbeiter werden regelmäßig zum Thema Sicherheit geschult und für das Thema sensibilisiert und über aktuelle Sicherheitsrisiken zeitnah informiert.
11. Datenschutzerklärung	Es gilt unsere Datenschutzerklärung gemäß: https://www.conftool.net/de/mehr_ueber_conftool/datenschutz.html Sämtliche im Rahmen der Durchführung dieses Auftrags generierten Daten, Informationen und sonstigen Ergebnisse stehen im Eigentum des Kunden.

Alle Mitarbeiter sind vertraglich zur Vertraulichkeit und Geheimhaltung von betriebsinternen Daten gegenüber Dritten verpflichtet.

Die ConfTool GmbH verpflichtet sich, sämtliche ihr anvertraute Informationen, einschließlich Daten, geheim zu halten und nicht für andere Zwecke als für die in dieser Vereinbarung vorgesehenen Arbeiten zu verwenden. Personenbezogene Daten werden ausschließlich für die Bearbeitung der Aufträge und der Kontaktaufnahme gespeichert und verwendet.

Dies gilt nicht für den Fall, dass die ConfTool GmbH von Rechts wegen zu einer Auskunft an einen Dritten verpflichtet ist (bspw. im Rahmen einer Steuerprüfung ggü. den zuständigen Prüfern).

In allen Fällen erfolgt eine notwendige Übermittlung von Daten gemäß den Bestimmungen der EU Datenschutz-Grundverordnung (DSGVO).

Der Umfang der erfassten Daten beschränkt sich auf ein Minimum.