Description of the Technical and Organizational Measures of ConfTool GmbH to Ensure Data Protection and Security (as of May 2018)

1 Allocation of responsibilities

The managing director Dr Harald Weinreich (MSc Computer Science) is responsible for ensuring compliance with legal regulations for IT security and data protection. He is at the same time chief information security officer and responsible for data compliance.

2 Building security, entrance security, room security

All data-processing servers and backup systems are located in buildings of Hetzner AG company in Nuremberg Metropolitan Region, Germany.

Access to the servers is granted only to authorized contract partners with an appointment. Contract partners must identify themselves on the spot. Authorized representatives require a written confirmation from the contract partner.

The data center parks of Hetzner AG are secured with safety fences. Entrances and server rooms are video-monitored.

The building security concept of Hetzner can be found at:
https://www.hetzner.de/pdf/en/Sicherheit_en.pdf

Hetzner GmbH is also certified according to DIN ISO / IEC 27001.
https://www.hetzner.com/unternehmen/zertifizierung?country=us

The headquarters of ConfTool GmbH are located in a residential building. The entrance door, the door to the office and the doors to the office spaces are secured by simple locking systems and an alarm system. Access is only possible through the managing director.
The office is not open to the public.

3 Access control to the electronic information processing system

Access to the servers is granted only to authorized contract partners with an appointment. Contract partners must identify themselves on the spot. Authorized representatives require a written confirmation from the contract partner.

Access to server rooms is possible only in company of an employee. Refer also to the data and security concept of Hetzner:
https://www.hetzner.de/pdf/en/Sicherheit_en.pdf

Hetzner Online has been certified following to the requirements to an information safety management system (ISMS) in accordance with DIN ISO/IEC 27001. The infrastructure and the operation of the entire data center parks in Nuremberg and Falkenstein/Vogtland have been tested by FOX Certification. For further information, please refer to:
https://www.hetzner.com/unternehmen/zertifizierung?country=us

The use of data transmission devices (Internet) is possible only by authorization.

Access to offices or home office locations of ConfTool GmbH is granted only personally known people under supervision. The building is protected by an alarm system from TELENOT ELECTRONIC GmbH.

4 Access Control

The conference management system ConfTool Pro implements the access control to the data of all users and participants: Each user is assigned a corresponding role (administrator, conference organizer, front desk, participants, etc.). The user role specifies the access options.

Access to all data of the conference management system is possible only via the Web interface and requires a unique user name and a password. The following rules apply for passwords: The minimum length is 5 characters, different letters and numbers have to be included and trivial passwords (such as "12345") are blocked.

Optionally, the password requirements can be raised to at least 8 characters with at least one special character, numbers, uppercase and lowercase letters.
All personally used passwords are stored as salted hashes using bcyrpt (was SHA256) and are not accessible to administrators.

After 10 unsuccessful login attempts, the login will be blocked for 10 minutes for the corresponding IP address and user. This measure has been taken to prevent brute-force attacks.
Additionally, a (barrier-free) CAPTCHA can be activated for the login (it will become effective after 3 failed login attempts) and for the registration of all new user accounts.
The session time-out for each user group may be adjusted differently, depending upon safety requirements. Administrators will usually be logged out automatically after one hour of inactivity, normal users will be logged out usually after 5 hours of inactivity, as they might need longer amounts of time to enter their submissions or reviews. Moreover, in these cases the potential damage that can be caused by "session hijacking" is minimal.
Administrators of ConfTool GmbH (also when they work from at home) use different passwords for each ConfTool instance. Passwords are coded with AES256, and as a second password threshold „One Time passwords “ are used and/or the IP address of the access computer will be cross-checked.

Access to data by Hetzner AG is not possible, the company does not have any access codes to the servers (see also access/admission).

For access to the system level, only SSH or SFTP with private / public key encryption are used. The private keys are secured additionally with a password.

Access to files in the upload area of the ConfTool system is also only possible via the Web interface, but not directly via the Web server. Access to ConfTool is controlled via user accounts. As per default, files are accessible only to participants who are logged in using their own user account.

Employees of ConfTool GmbH do not enter, modify or delete data in the ConfTool system.

Company data of ConfTool GmbH is encrypted by "TrueCrypt" and "VeraCrypt" using AES256 (also when employees work from at home). All Backup media are encrypted using the same method.

4.1 Input and modification

A more comprehensive processing of participant data is limited to the conference manager and to employees who are assigned the appropriate roles by the conference manager in the ConfTool system.

Participants themselves can only enter, change or delete their own data. The assignment is ensured by way of user profiles, for which the e-mail address and the user name serve as key attributes.

Registrations, entries, changes and deletions by users of the ConfTool system are recorded and can be accessed in a log area by organizers of the event.

4.2 Data Deletion Concept

At the end of the contract period, the database is destroyed with all data and all backup files.

The database is destroyed by executing the command "drop database"; therefore the database can only be restored with forensic means immediately after the destruction and furthermore only by persons who have physical access to the data storage / hard disk or an image file thereof.

	Backup files are overwritten by executing the command "wipe" with random numbers. This makes data recovery impossible, given the current state of knowledge, not even by forensic means.
5 Securing communication	Any access to the ConfTool system, including the data input by participants, are carried out exclusively via encrypted connections (https). **EV (extended validation)** certificates of the company *Comodo* with SHA-2 and 4096 bit length are employed. The administration of the server pool, the administration of the ConfTool software and the backup of the data is also executed only in encrypted form.
6 Data transmission control	Company data are stored on ConfTool GmbH servers at Hetzner AG.
6.1 Encryption during data transmission	WebDAV is used via HTTPS / SSL with SHA-2 certificates from Comodo.
6.2 Data carrier transport	Is not realized.
6.3 Transmission control	Data are only transmitted to known and attributable internal addressees as well as the contact person of the contract partner, based on the criterion of conclusiveness.
7 Separation rule	The system is designed in such a way that the data of each conference are organized in separate databases. Uploaded files (uploads) by authors and organizers are also saved in separate directories for each conference.
Database	All users can only access the database of the ConfTool system via the Web interface of the system. Customers cannot directly access the servers or the database system.
Upload area	Access to the uploaded files is possible only via the Web interface of ConfTool.
8 Availability control	Standby servers are available to ConfTool GmbH. They can be used in unpredictable outages. Power supply is ensured via a redundant, uninterruptible power supply (UPS). Qualified personnel of Hetzner AG provide a "24/365-stand-by-service" support for ConfTool GmbH. Hetzner AG ensures an exchange of defective hardware within a maximum of 4 hours. In our experience, exchange of defective hardware takes place usually within under 30 minutes.
8.1 Data and backups	All databases are backed up at least twelve times a day (usually hourly) on two additional commercial rental servers, which are property of Hetzner AG and located in Germany. Data is transferred via encrypted, secure connections only. After 7 days, the hourly backups are deleted. After this period, only daily backups are stored. Daily backups are automatically deleted after 12 months and cannot be retrieved. On request of the customer, backups can be deleted immediately after the uninstallation of the database. It is the responsibility of the customer to create backups that will be available after the system has been uninstalled and after the daily backups have been deleted automatically. The ConfTool system provides appropriate export functions for customers.

Before an instance of the ConfTool system is deleted, the customer will be consulted. Deletion will only be executed once the customer has confirmed that all data has been saved.

In order to avoid confusion, during the deletion process the name of the instance as well as the name of the customer are displayed. Deletion procedures are always carried out by two employees at the same time in order to prevent errors.

8.2 Hardware and network

Both the power supply and the network are monitored by Hetzner AG employees as part of their "24/365 stand-by service".

Several monitoring systems control the availability and load of the servers. In the event of a failure or an abnormality, employees of ConfTool GmbH are notified by e-mail and text message within 5 minutes.

Hetzner AG offers special hardware to protect against DDOS attacks at network level for all servers. More details can be found here: https://www.hetzner.com/unternehmen/ddos-schutz?country=us

The reliability of the network is ensured by multiple redundant upstreams:
1. Peerings (660GBit/s): 300 GBit/s DE-CIX, 100 GBit/s AMS-IX, 100 GBit/s NL-IX-FFM, 100 GBit/s ECIX and others.
2. Transit network (1090GBit/s): 400 GBit/s core Backbone, 300 GBit/s Telia, 100 GBit/s GTZ, 100 GBit/s NTT, 100 GBit/s TATA and others
3. Private Peerings (780GBit/s): 240GBit/s Google, 100GBit/s OVH, 80 GBit/s Amazon, 40 GBit/s KabelDeutschland, 40 GBit/s RETN, 40 GBit/s Rostelecom, 20 GBit/s Facebook, 20 GBit/s Microsoft, 20 GBit/s Megafon 20 GBit/s Init7, 20 Telefonica and many more.

see: https://www.hetzner.com/unternehmen/rechenzentrum?country=us

8.3 Planning for total failure

The servers are located at 2 different computing centers of Hetzner AG. If one of the centers should fail completely, one of the backup servers will take over the tasks of the failed server.

9 Server security

All servers are equipped with a firewall. The firewall is equipped with a monitoring software.

All files that have been uploaded by clients are scanned for viruses using the anti-virus program "ClamAV". The anti-virus program is updated automatically every day.

Uploaded files cannot be executed on the servers, due to the system structure and the use of file attributes.

All servers are scanned by the company "Comodo" for security holes (in accordance with the requirements of the PCI compliance test) usually monthly, but at least quarterly.
See: https://www.hackerguardian.com/hackerguardian/faqs.html

The corresponding scan protocols are available on request.

9.1 Control against abuse

Attempts of unauthorized access to the server via the network (ssh, smtp, http, php) are logged for all servers and transmitted hourly via e-mail to the staff of ConfTool GmbH.

9.2 Contract data centers

The contract data centers of Hetzner AG are located in the Nuremberg area.

They are spatially distributed and not visible from the outside as such. Road directions to the centers will be communicated to customers upon request only. Only dedicated servers are used.

Technical staff is on site all days of the year around the clock to monitor the servers.

9.3 Operating systems

The servers and backup systems run under Ubuntu Linux (server version 14.04 LTS and LTS 16.04).

Security updates are carried out daily, provided updates exist. Check for updates is carried out automatically, installation of updates is initiated manually.

9.4 Software services

In order to minimize the chance that the system is compromised due to security holes, only necessary services and programs are installed on the servers. Only the following systems are accessible via the Internet:

Apache 2.4 with mod-ssl and PHP 5.5.9 and 7.0.13 (Ports 80 und 443), each with the latest Ubuntu server package security updates.

All unnecessary, safety-critical functions have been deactivated for PHP. See:
http://www.conftool.net/en/technical_documentation/security_hints.html

OpenSSH 6.6. 1p1 and 7.2p2 (does *not* run on standard port 22)

Postfix 2.11.0 and 3.1.0 (dedicated mail server)

9.5 Data carrier

In order to reduce the likelihood of data loss to a minimum, the mass storage devices used are RAID1 hard disk systems with hardware RAID controllers. All hard disks used are enterprise-class HDDs that are designed for continuous load.

The state of the RAID system is monitored every 10 minutes and in case of exceptional occurrences, ConfTool GmbH employees are automatically notified by e-mail.

Hard disks are usually replaced using a "hot-swap" procedure without system downtime.

9.6 Deletions before removal from service

Before any server is removed from service, it will be booted with a rescue system via the network by ConfTool GmbH and all hard disks will be completely overwritten using the tool "shred". All data will be deleted irrevocably.

see: http://manpages.ubuntu.com/manpages/trusty/man1/shred.1.html

10 Privacy Statement

Our privacy statement can be found at:
https://www.conftool.net/en/about_conftool/privacy.html

All data, information, and other performance outcomes generated in context of the execution of this contract are property of the customer.

All employees are contractually bound to confidentiality, professional discretion and nondisclosure.

ConfTool GmbH agree to treat any kind of information that is disclosed to them, including all data, confidentially, to not pass it on to a third party and to use it exclusively for the purpose of the proposed works that are outlined in this agreement. Personal data are stored and used exclusively to process the orders and to contact the clients.

This does not apply if ConfTool GmbH is legally obliged to provide information to a third party (e. g. in the context of a tax audit with respect to the responsible auditors).

In all cases, the necessary data transmission is carried out in accordance with the provisions of the **General Data Protection Regulation (GDPR)**.

The scope of the data is limited to a minimum.