Anlage zum Vertrag gemäß § 11 BDSG

Getroffene technische und organisatorische Schutzmaßnahmen

(1) Schutzmaßnahmen der **Zutrittskontrolle:**

Die betriebsrelevanten meetyoo-Systeme befinden sich in einem zertifizierten und speziell für den Betrieb von IT-Infrastruktur konzipierten **Hochsicherheitsrechenzentrum** in Berlin.

Zutrittskontrollsystem Rechenzentrum:
Der **Zutritt zu den gemieteten RZ-Flächen** erfolgt über einen Zutrittschip in Kombination mit einem PIN-Code. Die Zutrittschips sind personengebunden und ausschließlich autorisierten Mitarbeitern namentlich zugeordnet. Zusätzlich muss der Zutritt zu den Flächen im Vorfeld angemeldet werden.
Die Ausgabe der Zutrittschips erfolgt nur an eingewiesene Mitarbeiter und wird ebenso, wie die Nutzung der Chips, protokolliert. Fremdpersonal darf die RZ-Flächen nur unter ständiger Aufsicht eines meetyoo Mitarbeiters betreten. Die Fläche sowie die Zugänge zur Fläche sind rund um die Uhr videoüberwacht. Die meetyoo Serverschränke sind einzeln verschließbar.

Zutrittskontrollsystem Büroflächen Friedrichstrasse:
Der **Zutritt zu den Büroflächen in der Friedrichstrasse** wird ebenfalls über ein Zutrittskartensystem geregelt. Ausgabe und Nutzung der Karten werden protokolliert, die erlaubten Zutrittszeiten werden individuell angepasst. Besucher und Fremdpersonal werden vom Empfang herein gelassen und zum gewünschten Ansprechpartner begleitet.

Der **Zutritt zum Bürogebäude** ist werktags von 7:00 - 20:00 Uhr für die Öffentlichkeit möglich. Außerhalb dieser Zeit wird eine zusätzliche Zutrittskarte zur Freischaltung der Eingangstüren und des Fahrstuhls benötigt. Diese zusätzliche Karte wird nur an ausgewählte Mitarbeiter ausgegeben. Die Ausgabe wird ebenso protokolliert wie die Nutzung. Im Foyerbereich des Gebäudes ist immer (24x7) ein Concierge anwesend.

Alle Türen sind in einbruchhemmender Ausführung gefertigt und - sofern es sich um Notausgänge handelt - durch eine lokale Alarmanlage gesichert. Die Büroräume liegen im 3. Geschoss. Die Fenster sind nur mit sehr schmalem Winkel nach unten kippbar und mit Sicherheitsglas ausgeführt, so dass ein Eindringen nicht möglich ist.

(2) Schutzmaßnahmen der **Zugangskontrolle:**

meetyoo ist gemäß ISO 27001 zertifiziert. Das aktuelle Zertifikat können Sie unter folgendem Link einsehen: https://www.certipedia.com/quality_marks/9105037096?locale=de

Die Vergabe von Berechtigungen für den Systemzugriff erfolgt ausschließlich im Rahmen des zur Erbringung der jeweiligen arbeitsvertraglichen Pflichten notwendigen Umfangs.

Passwort-Regeln: Der **Zugang zu Systemen** von meetyoo wird mittels Kennwortverfahren kontrolliert. Ein individueller User Log-In bei Anmeldung am System ist durch strenge Passwortregeln sichergestellt. Diese beinhaltet u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennwortes.

Bildschirmsperre: Gemäß der **Nutzungsvereinbarung für IT-Arbeitsplätze** ist jeder Mitarbeiter von meetyoo dazu verpflichtet, bei Verlassen des Arbeitsplatzes den Bilschirm zu sperren. Ergänzend wird der Bildschirm nach fünf Minuten der Inaktivität automatisch gesperrt. Arbeitsplatzrechner von Mitarbeitern, die ihren Arbeitsplatz aufgabenbedingt häufig kurz verlassen müssen (z.B. Empfang), sind zusätzlich durch einen USB-Dongle gesichert.

(3) Schutzmaßnahmen der **Zugriffskontrolle:**

meetyoo ist gemäß ISO 27001 zertifiziert. Das aktuelle Zertifikat können Sie unter folgendem Link einsehen: https://www.certipedia.com/quality_marks/9105037096?locale=de

Die **Vergabe der Berechtigungen** erfolgt ausschließlich im Rahmen des zur Erbringung der jeweiligen arbeitsvertraglichen Pflichten notwendigen Umfangs. Die Berechtigungen für die Zugriffe auf die unterschiedlichen Systeme werden erst nach Durchlaufen des jeweiligen Einarbeitungsplans und nur nach Freigabe durch den Fachabteilungsleiter erteilt. Diese Freigaben werden zentral dokumentiert. Dies gilt auch für den Bereich der Administration der Systeme. Auch die Administration erfolgt - soweit möglich - ausschließlich mit personenbezogenen Accounts.

Die **Patchung der IT-Systeme** erfolgt im Rahmen des dokumentierten Patchmanagement-Prozesses. Neue Patches werden zunächst in einer Testumgebung getestet und dann im Operativsystem eingespielt. Die dafür vorgesehenen Zeitfenster sind abhängig von der Risikoklasse der Fehler, die damit gepatcht werden.

Das Netzwerk von meetyoo ist in mehrere, durch **Firewalls voneinander getrennte Zonen** unterteilt. Bei der Gestaltung der Kommunikation zwischen diesen Zonen wird streng darauf geachtet, dass keine Kommunikation von den Demilitarisierten Zonen in das interne Netz von meetyoo gestattet ist. Personenbezogene Daten werden weitestgehend im internen Netz abgelegt. Die Sicherheit dieser Maßnahmen wird regelmäßig durch externe Dienstleister und intern im Rahmen von Penetrationtests (als Black- und Whitebox-Tests) überprüft.

Der **Virenschutz** erfolgt gemäß eines festgelegten und dokumentierten Prozesses. Alle Clientrechner sind mit entsprechender Anti-Viren-Software ausgestattet und kommunizieren regelmäßig mit einem zentralen Server, der die Aktualität der Signaturen gewährleitstet. Durch diesen zentralen Server werden auch alle ausgehenden E-Mails auf einen etwaigen Virenbefall geprüft, um sicher zu stellen, dass aus dem Netz von meetyoo keine Viren in Umlauf gebracht werden. Zusätzlich werden alle eingehenden E-Mails mit Hilfe eines Service-Providers auf Virenbefall geprüft. Betroffene Mails werden nicht zugestellt.

(4) Schutzmaßnahmen der **Weitergabekontrolle:**

Die **Übertragung der zur Veröffentlichung** vorgesehenen Events erfolgt unverschlüsselt. Die Links und individuelle Kennworte werden an die Teilnehmer per unverschlüsselter Mail versendet. Das Verfahren ist nicht für die Übertragung von vertraulichen Inhalten vorgesehen. Eine Veränderung der gestreamten Inhalte bei laufender Übertragung ist auch ohne Verschlüsselung praktisch kaum möglich bzw. extrem aufwendig.

(5) Schutzmaßnahmen der **Eingabekontrolle::**

Eingaben in der Anwendung sind nur über die Kommentarfunktion möglich. Diese werden mit der User-ID an den Moderator übermittelt und sind so nachvollziehbar.
Die genutzten Systeme erlauben die Protokollierung der Eingaben. Da zur Erfassung personenbezogener Daten ausschließlich benutzerindividuelle Logins benutzt werden dürfen, ist auch nachträglich nachvollziehbar, durch wen die Daten erfasst bzw. manipuliert wurden. Die so entstandenen Protokolle werden zentral in einem Log-Server aufbewahrt. Von dort können auch entsprechende Berichte generiert werden.

(6) Schutzmaßnahmen der **Verfügbarkeitskontrolle:**

Die **betriebsrelevanten Systeme** von meetyoo sind redundant ausgelegt.

Alle geschäftsrelevanten Daten von meetyoo werden im Rahmen eines strukturierten **Backup-Plans** in regelmäßigen Abständen gesichert. Dies gilt auch und besonders für personenbezogene Daten. Die ordnungsgemäße Abarbeitung der Backup-Jobs wird täglich kontrolliert. Einmal monatlich wird zusätzlich ein Archiv angelegt. Die archivierten Daten werden in einem Safe aufbewahrt. Ebenfalls einmal monatlich findet eine Notfallübung statt, in deren Rahmen die Wiederherstellung von Daten aus dem Backup getestet wird. Das Ergebnis des Tests wird dokumentiert.

Es existiert ein **Notfallhandbuch**, in dem für alle betriebsrelevanten Systeme von meetyoo unterschiedliche Fehlerszenarien und entsprechende Arbeitsanweisungen zur Behebung dokumentiert sind. Dieses Notfallhandbuch ist teil unseres Qualitäts- und Informationssicherheits-Managementsystems und unterliegt einer regelmäßigen Revision (mindestens einmal jährlich). Auf Basis dieses Handbuchs werden einmal im Quartal Notfallübungen durchgeführt, um die korrekte Reaktion aller beteiligten Instanzen zu kontrollieren und zu festigen.

Die geschäftsrelevanten Systeme von meetyoo befinden sich auf einer speziell für den Betrieb von IT-Infrastruktur konzipierten **Rechenzentrumsfläche**. Die Stromversorgung erfolgt über zwei getrennte Versorgungsringe und ist jeweils über eine USV abgesichert. Die USV garantiert bei Volllast eine Überbrückungszeit von 30 Minuten. Die weitere Absicherung erfolgt über ein Dieselaggregat, dass für weitere 24 Stunden die Stromversorgung garantiert.

Auf der RZ-Fläche sind eine **Brandfrühsterkennungsanlage** und eine nicht toxische Gas-Löschanlage installiert.

(7) Schutzmaßnahmen der **Trennungskontrolle:**

meetyoo ist gemäß ISO 27001 zertifiziert. Das aktuelle Zertifikat können Sie unter folgendem Link einsehen: https://www.certipedia.com/quality_marks/9105037096?locale=de

Das Netzwerk von meetyoo ist in mehrere, durch Firewalls voneinander getrennte Zonen unterteilt. Bei der Gestaltung der Kommunikation zwischen diesen Zonen wird streng darauf geachtet, dass keine Kommunikation von den Demilitarisierten Zonen in das interne Netz von meetyoo gestattet ist.

Personenbezogene Daten werden nur im für unsere Dienstleistungserbringung **absolut notwendigen Rahmen erhoben.** Sobald die Daten nicht mehr benötigt werden, werden diese **gelöscht**. Die Überprüfung eines Datenbestandes auf nicht mehr benötigte Daten erfolgt gemäß eines festgelegten Reviewplans. Davon unberührt bleibt der individuelle Anspruch auf Auskunft, Korrektur und Löschung personenbezogener Daten nach §35 BDSG. Auskunftsersuchen können jederzeit an den betrieblichen Datenschutzbeauftragten von meetyoo gerichtet werden und werden schnellstmöglich beantwortet. Die Löschung von Einzelverbindungsnachweisen unterliegt zusätzlich den Anforderungen des TKG. Diese werden selbstverständlich beachtet.

Veränderungen an bestehenden Systemen sowie Einführung neuer Systeme erfolgen prinzipiell nur nach einem **ausgiebigen Test in einem komplett vom Betriebsnetzwerk** von meetyoo entkoppelten Testnetz. Vor der Portierung einer solchen Änderung/Neuanschaffung in das Betriebsnetz erfolgt ein dokumentierter Abnahmetest und eine FMEA inklusive der Definition entsprechender Gegenmaßnahmen.

(8) Maßnahmen zur **Datenlöschung:**
meetyoo unternimmt folgende Maßnahmen zur **Datenlöschung:** • Datenlöschung mittels Software inkl. Protokollierung • Physikalische Zerstörung der Datenträger inkl. Protokollierung • Schreddern von papierhaften Dokumenten inkl. Protokollierung