

Anlage 1 – Technische und organisatorische Schutzmaßnahmen (Sicherheit der Verarbeitung gemäß Artikel 32 DS-GVO)

Präambel

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, konkretisiert diese Anlage nach Artikel 32 EU-Datenschutzgrundverordnung („DS-GVO“), die getroffenen technischen und organisatorischen Schutzmaßnahmen, die sich aus der zugrunde liegenden Datenverarbeitung ergeben, um ein dem Risiko angemessenes Datenschutzniveau zu gewährleisten

Diese Anlage findet Anwendung auf alle Tätigkeiten, bei denen Mitarbeiter des Auftragsverarbeiters (Auftragnehmer) mit personenbezogenen oder sonstigen Daten des Verantwortlichen (Auftraggeber) in Berührung kommen können.

§1 Getroffene technische und organisatorische Sicherheitsmaßnahmen zur Gewährleistung eines angemessenen Datenschutzniveaus

(1) Maßnahmen zur Sicherstellung der Vertraulichkeit auf Dauer:
<p>Die betriebsrelevanten meetyoo-Systeme befinden sich in einem zertifizierten und speziell für den Betrieb von IT-Infrastruktur konzipierten Hochsicherheitsrechenzentrum in Berlin.</p> <p>meetyoo ist gemäß ISO 27001 zertifiziert. Das aktuelle Zertifikat können Sie unter folgendem Link einsehen: https://www.certipedia.com/quality_marks/9105037096?locale=de</p> <p>a) Zutrittskontrolle: <u>Zutrittskontrollsystem Rechenzentrum:</u> 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 ausgewiesene 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.</p> <p><u>Zutrittskontrollsystem Büroflächen Friedrichstrasse:</u> 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 hereingelassen und zum gewünschten Ansprechpartner begleitet.</p> <p>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.</p> <p>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 schmalen Winkel nach unten kippbar und mit Sicherheitsglas ausgeführt, so dass ein Eindringen nicht möglich ist.</p>

b) Zugangskontrolle:

Die **Vergabe der Berechtigungen** 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.

Bildschirm Sperre: Gemäß der **Nutzungsvereinbarung für IT-Arbeitsplätze** ist jeder Mitarbeiter von meetyoo dazu verpflichtet, bei Verlassen des Arbeitsplatzes den Bildschirm 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.

c) Zugriffskontrolle

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. Über Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte sowie die Protokollierung von Zugriffen werden die Daten vor unbefugten Lesen, Kopieren, Verändern oder Entfernen geschützt.

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 Penetrationstests (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 gewährleistet. 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.

d) Trennungskontrolle

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. Auskunftersuchen 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.

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.

(2) Maßnahmen zur **Sicherstellung der Integrität auf Dauer:**

Maßnahmen zur Verhinderung von unbefugtem Lesen, Kopieren, Verändern oder Entfernen von personenbezogenen Daten bei elektronischer Übertragung oder Transport.

a) Weitergabekontrolle

Einrichtung von Standleitungen bzw. VPN-Tunneln. Verschlüsselte Übertragung von Daten aus bzw. nach externen Netzen mittels geeigneter Transportprotokolle.

b) Eingabekontrolle

Die Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten geschieht auf Basis eines Berechtigungskonzepts. Eingabe, Änderung und Löschung von Daten sind durch individuelle Benutzernamen (nicht Benutzergruppen) nachvollziehbar.

(3) Maßnahmen zur **Sicherstellung der Verfügbarkeit auf Dauer:**

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 Vollast 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.

(4) Maßnahmen zur **Pseudonymisierung und Anonymisierung** personenbezogener Daten:

Es findet eine strikte Trennung der Kundenstammdaten und Kundenumsatzdaten, durch den Einsatz von voneinander separierten Systemen, statt. Es handelt sich hierbei um ein CRM- sowie ein ERP-System. Unter der Einhaltung der geltenden Gesetze, werden die Daten automatisiert anonymisiert. Nach Ablauf der jeweiligen Speicherfrist werden diese Daten ebenfalls automatisiert gelöscht.

(5) Maßnahmen zur **Verschlüsselung** personenbezogener Daten:

Der Datenaustausch von personenbezogenen Daten erfolgt unter der Nutzung von folgenden Verschlüsselungsmechanismen:

- Verwendung von verschlüsselten Passwörtern
- Verschlüsselte Übertragung von Daten aus bzw. nach externen Netzen mittels geeigneter Transportprotokolle (SSL/TLS, etc)
- Verwendung von verschlüsselten Datenträgern und Mobile Devices

<p>(6) Maßnahmen zur Sicherstellung der Belastbarkeit der Systeme und Dienste auf Dauer:</p> <p>Im Rahmen unseres Informationssicherheitsmanagements werden regelmäßige und dokumentierte Penetrationstests durchgeführt. Geräte zur Überwachung von Temperatur und Feuchtigkeit sind in den Serverräumen installiert. Die Systeme und Dienste sind so ausgelegt, dass auch punktuelle hohe Belastungen von Verarbeitungen möglich sind.</p>
<p>(7) Maßnahmen zur raschen Wiederherstellung der Verfügbarkeit bei einem physischem oder technischem Zwischenfall:</p> <p>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.</p>
<p>(8) Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen:</p> <p>meetyoo ist gemäß ISO 27001 zertifiziert. Das aktuelle Zertifikat können Sie unter folgendem Link einsehen: https://www.certipedia.com/quality_marks/9105037096?locale=de</p> <p>Im Rahmen unseres Informationssicherheitsmanagements werden die technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten regelmäßig auditiert und bewertet.</p> <p>Alle Mitarbeiter werden auf das Datengeheimnis verpflichtet und regelmäßig geschult.</p> <p>Ein Datenschutzbeauftragter wurde bestellt und unterstützt meetyoo in enger Zusammenarbeit in der Umsetzung und Bewertung unseres Datenschutzmanagements.</p>
<p>(9) Maßnahmen zur Datenlöschung und Einschränkung der Verarbeitung:</p> <p>meetyoo unternimmt folgende Maßnahmen zur Datenlöschung:</p> <ul style="list-style-type: none"> ▪ Datenlöschung mittels Software inkl. Protokollierung ▪ Physikalische Zerstörung der Datenträger inkl. Protokollierung ▪ Schreddern von papierhaften Dokumenten inkl. Protokollierung