METANET AG, Josefstrasse 218, 8005 Zürich
Telefon +41 44 310 87 66
Telefax +41 44 310 87 69
www.metanet.ch

# Technisch-organisatorische Massnahmen

## Präambel

Die METANET AG vermietet die Datenverarbeitungsanlage an den Auftraggeber. Dies beinhaltet die Vermietung von Hard- und Software, sowie die Bereitstellung von Anbindungen an das Internet sowie weitere Dienste entsprechend der jeweiligen Vereinbarung. Der Auftraggeber entscheidet allein und ausschliesslich darüber, welche personenbezogene Daten in welcher Weise verarbeitet werden. Die hierfür erforderlichen Programme zur Datenverarbeitung werden durch den Auftraggeber erstellt und eingesetzt. Die METANET AG sorgt für die technische Einsatzbereitschaft des Systems entsprechend den vertraglichen Vereinbarungen und führt Buch darüber, welche Anlagen durch den Auftraggeber in welchem Umfang genutzt werden. Die Datenverarbeitung erfolgt durch den Auftraggeber. Die METANET AG hat keinerlei Einfluss auf die durch den Auftraggeber durchgeführten Datenverarbeitungsvorgänge.

## Vertraulichkeit

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen in den Rechenzentren

  1. *Zutrittskontrollsystem*

     Ein Schliesssystem in Form einer mindestens 1-Faktor-Authentifizierung (z.B. Transponder, Chipkarte, Klingelsystem mit Personenkontrolle per Bild und Ton) ermöglicht den Zutritt zu Datenverarbeitungsanlagen erst nach positiver Zutrittsprüfung.
  2. *Schlüsselregelung*

     Schlüsselausgaben an Personen zum Zutritt zu Datenverarbeitungsanlagen werden dokumentiert.
  3. *Protokollierung der Besucher*

     Besucher, die Zutritt zu Datenverarbeitungsanlagen erhalten (z.B. im Falle von Hardware-Austausch durch den Hersteller) werden in einem Besucherbuch erfasst.
  4. *Einbruchmeldeanlage*

     Der Zutritt zu Datenverarbeitungsanlagen ist per Einbruchmeldeanlage abgesichert.
  5. *Videoüberwachung*

     Datenverarbeitungsanlagen werden per Videoüberwachung gesichert.

- Zugangskontrolle
  Keine unbefugte Systembenutzung

  1. *Passwortvergabe*

     Ein Zugang zu den Datenverarbeitungssystemen ist grundsätzlich nur mittels einer Kombination aus einem Benutzernamen und dem zugeordneten Passwort möglich.

2. *Passwortrichtlinie*

   Passwörter für Datenverarbeitungsanlagen müssen Mindest-Komplexitätsanforderungen der unternehmensweiten Richtlinie entsprechen; Passwörter von Mitarbeitern müssen regelmässig geändert werden.

3. *Administrativer Zugriff*

   Sämtliche Datenverarbeitungssysteme sind zu Wartungszwecken ausschliesslich über freigegebene IP-Adressbereiche und verschlüsselt erreichbar (z.B. VPN-Beschränkungen).

4. *Firewall*

   Schutz der Infrastruktur durch Firewalls (Soft- und/oder Hardware), Beschränkungen ungenutzter Ports sowie Benutzername und Passwort vor unberechtigten Zugriffen geschützt. Systeme, die Hauptvertragsleistungen bereitstellen, werden, entsprechend der jeweiligen Vereinbarung im Hauptvertrag, mit einer Firewall ausgestattet.

5. *Einsatz von Anti-Viren-Software*

   Systeme, die zum Zugriff auf Datenverarbeitungssysteme genutzt werden, sind mit einer Anti-Viren-Software ausgestattet. Diese Software wird regelmässig auf die neuesten Virus-Definitionen aktualisiert. Systeme, die Kundenleistungen bereitstellen, werden, entsprechend der jeweiligen Vereinbarung im Hauptvertrag, mit einer Anti-Viren-Software ausgestattet.

6. *Verschlüsselung von mobilen Datenträgern*

   Sofern mobile Datenträger oder mobile Geräte zum Einsatz kommen, werden die Inhalte verschlüsselt.

- Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems

  1. *Zuordnung von Benutzerrechten*

     Der Zugriff auf Datenverarbeitungssysteme wird für Personen auf die jeweils mindestens notwendigen Daten durch Vergabe entsprechender Benutzerrechte eingeschränkt. Die Datenverarbeitung selbst erfolgt durch den Kunden Der Auftragnehmer hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

  2. *Sichere Aufbewahrung von Datenträgern*

     Datenträger, die personenbezogene Daten enthalten, werden verschlossen gelagert

  3. *Verwaltung der Rechte durch einen eingeschränkten Personenkreis*

     Ausschliesslich berechtigte Systemadministratoren sind in der Lage, Rechte anderer Personen zu Datenverarbeitungssystem zu verwalten. Der Kreis der berechtigten Systemadministratoren wird auf die kleinstmögliche Auswahl von Personen reduziert. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

  4. *Protokollierung der Zugriffe*

     Zugriffe auf Dienste (z. B. Webdienste) werden in Log-Files protokolliert. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat jedoch keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

METANET AG, Josefstrasse 218, 8005 Zürich
Telefon +41 44 310 87 66
Telefax +41 44 310 87 69
www.metanet.ch

5. *Ordnungsgemässe Vernichtung von Datenträgern*

   Datenträger, die personenbezogene Daten enthalten werden gemäss DIN 66399 vernichtet.

6. *Regelmässige Wartung der Datenverarbeitungssysteme*

- Trennungskontrolle
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden

1. *Festlegung von Datenbankrechten*

   Der Zugriff von Systemen und Benutzern auf Datenbanken wird auf die jeweils notwendigen Daten eingeschränkt.

2. *Trennung von Produktiv- und Testsystemen*

   Produktiv- und Testumgebungen werden isoliert voneinander betrieben. Ein Zugriff einer Umgebung auf Daten der jeweils anderen Umgebung wird durch den Einsatz von z.B. getrennten Datenbanksystemen und Serversystemen unterbunden.

3. *Logische Mandantentrennung*

   Durch den Einsatz unterschiedlicher softwareseitiger Mechanismen wird eine Trennung der Daten von Mandanten gewährleistet.

## Integrität

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport

1. *Transport*

   Sofern personenbezogene Daten weitergegeben werden, findet dies grundsätzlich verschlüsselt statt. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

- Eingabekontrolle
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

1. *Zuordnung von Benutzerrechten*

   Der Zugriff auf Datenverarbeitungssysteme wird für Personen auf die jeweils mindestens notwendigen Daten durch Vergabe entsprechender Benutzerrechte eingeschränkt.

2. *Protokollierung von Dateneingaben*

   Die Datenverarbeitung erfolgt durch den Kunden, Seitens des Auftragnehmers besteht kein Einfluss auf die durch den Kunden verwendeten Datenverarbeitungsprogramme. Die

METANET AG, Josefstrasse 218, 8005 Zürich
Telefon +41 44 310 87 66
Telefax +41 44 310 87 69
www.metanet.ch

Eingabekontrolle der Daten kann daher ausschliesslich durch den Kunden umgesetzt werden.

3. *Nachvollziehbarkeit der Eingabe*

   Die Datenverarbeitung erfolgt durch den Kunden. Seitens des Auftragnehmers besteht kein Einfluss auf die durch den Kunden verwendeten Datenverarbeitungsprogramme. Die Eingabekontrolle kann daher ausschliesslich durch den Kunden umgesetzt werden. Bei Änderungen durch den Auftragnehmer werden die Administrationszugriffe adäquat protokolliert.

## Verfügbarkeit und Belastbarkeit

- Verfügbarkeitskontrolle
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust

1. *Unterbrechungsfreie Stromversorgung in Serverräumen (Rechenzentren)*

   Serverräume sind durch unterbrechungsfreie Stromversorgungen geschützt. Der Schutz ist zweistufig aufgebaut. Bei Bedarf wird ein Notstrom-Aggregat automatisch aktiviert, das die Stromversorgung der Serverräume übernimmt.

2. *Klimaanlagen in Serverräumen (Rechenzentren)*

   Eine für den Betrieb von Serversystemen angemessene Temperatur und Luftfeuchtigkeit wird in Serverräumen durch ausreichend dimensionierte Klimaanlagen gewährleistet.

3. *Feuer- und Rauchmeldeanlagen in Serverräumen (Rechenzentren)*

   Durch den Einsatz von Feuer- und Rauchmeldeanlagen wird ein Brand frühzeitig erkannt. Feuerlöschanlagen löschen auftretende Brände.

4. *Datensicherungskonzept und Aufbewahrung von Datensicherungen*

   Datensicherungen von personenbezogenen Daten werden nur nach Vereinbarung bzw. gemäss des abgeschlossenen Hauptvertrages angefertigt und auf separaten und für Datensicherungen dediziert eingesetzten Systemen aufbewahrt.

5. *Monitoring*

   Systemkritische Instanzen werden durch Monitoring überwacht. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

6. *Hochwasser- und Erdbebenkritikalität*

   Das Rechenzentrum ist DIN-gerecht auf Hochwasser- und Erdbebenkritikalität geprüft.

## Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

- Datenschutz-Management
  Der Auftragnehmer etabliert ein Datenschutzmanagement, das den Schutz der personenbezogenen Daten sicherstellt.

- Incident-Response-Management
  Regelmässige Überprüfung der IT-Infrastruktur. Der Auftragnehmer etabliert einen Vorfallreaktionsplan.

METANET AG, Josefstrasse 218, 8005 Zürich
Telefon +41 44 310 87 66
Telefax +41 44 310 87 69
www.metanet.ch

- Datenschutzfreundliche Voreinstellungen
  Der Auftragnehmer stellt innerhalb seiner Möglichkeiten sicher, dass durch Voreinstellung nur Daten, die für den jeweiligen bestimmten Verarbeitungszweck unbedingt erforderlich sind, verarbeitet werden. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

- Auftragskontrolle
  Keine Auftragsverarbeitung ohne entsprechende Weisung des Auftraggebers

  1. *Auswahl von geeigneten Auftragnehmern*

     Bei der Auswahl von Auftragnehmern, die personenbezogene Daten im Auftrag verarbeiten, werden nur solche Auftragnehmer ausgewählt, die mindestens die gesetzlich vorgeschriebenen Anforderungen an die Verarbeitung von personenbezogenen Daten einhalten

  2. *Überwachung der Auftragnehmer*

     Der Auftragnehmer wird regelmässig auf die Einhaltung der zugesicherten technischen und organisatorischen Massnahmen bei der Verarbeitung von personenbezogenen Daten überprüft.