Gasometer B | Guglgasse 8/2/85 | A-1110 Wien
T +43 (0) 1 969 03 04 10 | F +43 (0) 1 969 03 04 40
office@omanbros.com | www.omanbros.com

# Anlage ./2: Technisch-organisatorische Maßnahmen (TOMs)

## Vertraulichkeit

**Zutrittskontrolle**:
Der Zutritt zu den Servern bei **Hutchison Drei Austria** (Wien) wird videoüberwacht. Der Zutritt ist mit elektronischer Zutrittskontrolle und versperrbaren Racks gesichert.

Der Zutritt zu den Servern bei **EWW ITandTEL** (Wien) wird mit elektronischer Zutrittskontrolle und versperrbaren Racks gesichert.

Die Datacenter-Parks der **Hetzner Online GmbH** (Falkenstein, Deutschland) haben folgende Zutrittsbeschränkungen:

- elektronisches Zutrittskontrollsystem mit Protokollierung
- Hochsicherheitszaun um den gesamten Datacenter-Park
- dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- 24/7 personelle Besetzung der Rechenzentren
- Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
- Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters

Der Zutritt zu **Büroräumlichkeiten** (Gasometer Wien) erfolgt nur unter Begleitung von Mitarbeitern.

**Zugangskontrolle**:
Schutz vor unbefugter Systembenutzung durch Kennwörter (einschließlich branchenüblicher Policy), ausschließlich kabelbasierte Netzwerke, getrennte WLAN'S für Besucher, automatische Sperrmechanismen bei mehrfachen Fehleingaben, Desktopsperren, Clean Desk-Richtlinie

**Zugriffskontrolle**:
Verwendung von unterschiedlichen Applikationen mit unterschiedlichen Berechtigungen, Einzelüberprüfung bei neuen Aufträgen und Ausscheiden von Mitarbeitern, Aktenschredder

**Trennungskontrolle**:
getrennte Kundenaccounts für Mail- und Webserver mit eigenen Benutzern, getrennte ftp-/ftps-Benutzer, Speichern der Daten unterschiedlicher Kunden in unterschiedlichen Verzeichnissen bei shared-Webhosting und shared E-Mail Kunden. Trennung durch unterschiedliche Datenbank-Berechtigungen bei hosted exchange-Kunden. Trennung von Produktiv- und Testsystemen.

Gasometer B | Guglgasse 8/2/85 | A-1110 Wien
T +43 (0) 1 969 03 04 10 | F +43 (0) 1 969 03 04 40
office@omanbros.com | www.omanbros.com

## Integrität

**Weitergabekontrolle** (kundenabhängig):
VPN-Zugänge oder Einschränkung auf bestimmte IP-Adressen bei Fernzugriffen, SSL/TLS verschlüsselte Ports für IMAP, POP3 und SMTP, SSL-Verschlüsselung für Webmail, Webspace-Administration und von uns zur Verfügung gestellten Applikationen, SSH-Zugänge für Root-Server. Zurverfügungstellung von sftp bzw. ftps.

Kontrollierte Vernichtung von Datenträgern. Verschlüsselung externer Backup – Speichermedien

**Eingabekontrolle**:
Logging der Server-Zugriffe, Aufzeichnung der Zugriffe auf Fremdsysteme im Rahmen von Supportleistungen und Wartungen mit Fernsoftware, Protokollierung er Stammdatenerfassung, Änderung und Löschung, Routinen für die Löschung von Protokollen.

**Systemsicherheit**:
Betrieb von Systemen zur Abwehr von Viren und Schadsoftware, Spamfilterung von Emails auf shared Mailservern, Absicherung der Systeme durch Firewalls

**Softwaresicherheit**:
Laufende Wartung von Betriebssystemen (einspielen von Updates und Sicherheitspatches) bis zur möglichen aktuellsten Version. Skriptsprachen und Datenbank-Systeme in aktuellen Versionen werden prinzipiell zur Verfügung gestellt, für die Verwendung dieser Versionen für aktuelle Versionen von Web-Applikationen wie Content Management Systemen, Webshops, etc. und deren regelmäßige Wartung ist jedoch der Auftraggeber verantwortlich.

## Verfügbarkeit, Belastbarkeit, Wiederherstellbarkeit

**Verfügbarkeitskontrolle**:
USV, Überspannungsschutz, Klimatisierung, Dieselgeneratoren, Feuer- und Rauchmeldeanlagen in allen Rechenzentren-Locations, Verwendung von Raid-Systemen, Replikation der shared hosted Systeme im Abstand von 5-10 Minuten, shared Mailserver werden in Echtzeit zwischen unseren Mailservern in Österreich und Deutschland repliziert, Systemmonitoring.

**Belastbarkeit**:
Infrastruktur ist so ausgelegt, dass genügend Kapazitäten für ein „Fail Over" im Falle eines Hardware-Defekts vorhanden sind. Ersatzlösungen und Vorhalt von Hardware für Systeme mit hoher Ausfallswahrscheinlichkeit.

**Wiederherstellbarkeit**: Tägliche Datensicherung auf Imagebasis für shared webhosting systeme, dedizierten Servern und Kundenservern (auftragsabhängig), und/oder Datensicherung auf File-Ebene, Erstellung von Offsite-Copies (verschlüsselt) mit wöchentlicher Verbringung in geografisch getrennte Location mit definierten Löschungsfristen.

Gasometer B | Guglgasse 8/2/85 | A-1110 Wien
T +43 (0) 1 969 03 04 10 | F +43 (0) 1 969 03 04 40
office@omanbros.com | www.omanbros.com

## Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

**Datenschutz-Management**: Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutzmit Zugriffsmöglichkeit für Mitarbeiter, sie Mitarbeiter sind geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet

**Incident-Response-Management**: Einsatz von Firewalls, Virenscannern und Spamfiltern mit regelmäßiger Aktualisierung, Vorfälle werden dokumentiert und ausgewertet, dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen.

**Datenschutzfreundliche Voreinstellungen**: Zum Zeitpunkt der Einrichtung sind Shared-Hosting Services und dedizierte Server auf dem aktuellsten Software-Stand, für https://-Verschlüsselungen können Zertifikate erworben werden oder kostenlose Zertifikate (let’s encrypt) installiert werden (serverabhängig). Unverschlüsselte Mail-Ports für POP3, IMAP und SMTP werden gesperrt. Webserverlogs (Apache) werden maskiert, Verzeichnisinhalte von Webservern werden defaultmäßig nicht gelistet.

**Auftragskontrolle**: Die Auswahl von Sub-Auftragnehmern erfolgt unter Anwendung der Sorgfaltsgesichtspunkte in Bezug auf Datenschutz und Datensicherheit und unter Abschluss einer Auftragsverarbeitungsvereinbarung.