



TOM

Technische und organisatorische Maßnahmen  
nach § 64 BDSG neu und Art. 32 DS-GVO

Der Auftragnehmer gewährleistet im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die nach § 64 BDSG-neu BDSG und Anlage gesetzlich geforderten Sicherheitsmaßnahmen und wird sie auf Verlangen des Auftraggebers nachweisen. Folgende besondere technische und organisatorische Maßnahmen werden bei der Verarbeitung eingehalten:

## 1. Zutrittskontrolle

- elektronisches Zutrittskontrollsystem, die Türen sind stets geschlossen und der Zutritt zu den Geschäftsräumen ist ausschließlich über ein Codeschloss mit numerischer Tastatur möglich
- Video- und Alarmanlagen gesichert
- dokumentierte Codeschlüsselvergabe an Mitarbeiter
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- Videoüberwachung an den Ein- und Ausgängen, die Serverräume können nur von dedizierten Personen betreten werden und sind mit einer weiteren Zutrittskontrollsystem gesichert

## 2. Zugangskontrolle

- bei der Online-Software meinOnlineBüo
  - o Server-Passwörter, welche nur vom Auftraggeber nach erstmaliger Inbetriebnahme von ihm selbst geändert werden und dem Auftragnehmer nicht bekannt sind
  - o Das Passwort zur Administrationsoberfläche wird vom Auftraggeber selbst vergeben - die Passwörter sollten vordefinierte Richtlinien erfüllen. Bei zusätzlichen Maßnahmen können wir den Auftraggeber gerne kostenpflichtig unterstützen.
- bei der Administration von meinOnlineBüo
  - o Zugang ist passwortgeschützt, Zugriff besteht nur für Mitarbeiter von Auftragnehmer; verwendete Passwörter müssen komplexen Vorgaben entsprechen und eine Mindestlänge haben

## 3. Zugriffskontrolle

- Allgemein
  - o Private Besuche am Arbeitsplatz sind grundsätzlich untersagt
  - o Geschäftliche Besuche unterliegen einer durchgängigen Aufsicht
  - o Lieferanten werden persönlich vom Eingangsbereich abgeholt und stehen durchgängig unter Aufsicht
  - o Firewalls vor allen Systemen, die besondere Schutzmaßnahmen benötigen
- bei internen Verwaltungssystemen des Auftragnehmers
  - o Sicherheitsupdate- und Backupmanagement (nach dem jeweiligen Stand der Technik) stellen sicher, dass unberechtigte Zugriffe verhindert werden.
  - o Abgestufte Berechtigungsvergabe für Mitarbeiter des Auftragnehmers
  - o Firewalls vor allen Systemen, die besondere Schutzmaßnahmen benötigen

- bei der Online-Software meinOnlineBüo
  - o Die Verantwortung der Zugriffskontrolle obliegt dem Auftraggeber, da unsere Mitarbeiter auftragsbedingt keinen Zugriff haben
- bei der Administration von meinOnlineBüro
  - o Durch regelmäßige Sicherheitsupdates des Betriebssystems und der Standardsoftware und Backups (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
  - o Verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers

#### **4. Weitergabekontrolle**

- Alle Mitarbeiter sind auf das Datengeheimnis nach § 53 BDSG (neu) bzw. § 5 BDSG verpflichtet.
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.
- Sichere und verschlüsselte Verbindungen für alle Verbindungen zwischen den Standorten
- Für Kunden-Services werden sichere Zugangskanäle angeboten

#### **5. Eingabekontrolle**

- bei internen Verwaltungssystemen des Auftragnehmers
  - o Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzeptes
- bei der Online-Software meinOnlineBüro
  - o Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.
  - o Bei diesen Systemen haben unsere Mitarbeiter keinerlei Zugriffsmöglichkeit. Wir nehmen Sperrungen aus rechtlichen oder technischen Gründen sowie im Falle des Zahlungsverzuges vor.
- bei der Administration von meinOnlineBüro
  - o Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
  - o Unsere Mitarbeiter dürfen grundsätzlich ohne explizite Anweisung des Auftraggebers nicht auf Ihre Daten zugreifen bzw. Daten eingeben, verändern oder löschen.

#### **6. Auftragskontrolle**

- Auf Wunsch Vertrag zur Datenverarbeitung
  - o schriftliche Festlegung der weisungsbefugten Mitarbeiter des Auftraggebers
  - o Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datenschutzgeheimnis
  - o Schriftliche Hinweise an die Mitarbeiter zum Datenverarbeitungszweck. Sie erhalten schriftliche Weisung zum Umgang mit personenbezogenen Daten.
  - o Wirksame Kontrollrechte gegenüber dem Auftragnehmer
  - o Laufende Überprüfung der Verfahren des Auftragnehmers
  - o Eindeutige Vertragsgestaltung
- Formalisierte Auftragserteilung
  - o Auftragsformular
  - o Aufträge sind nur von verifizierten Kontaktadressen möglich (E-Mail und Fax)
  - o Schriftliche Fassung und Dokumentation von Änderungen

## 7. Verfügbarkeitskontrolle

- bei internen Verwaltungssysteme des Auftragnehmers
  - o Backup- und Recovery-Konzept mit Sicherung aller relevanten Daten in angemessenen Intervallen.
  - o Sachkundiger Einsatz von Schutzprogrammen (Virens Scanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).
  - o Einsatz von Festplattenspiegelung bei allen relevanten Servern.
  - o Monitoring aller relevanten Server.
  - o Einsatz unterbrechungsfreier Stromversorgung.
  - o Maßnahmen gegen DDoS und sonstige Angriffe gegen die Systeme nach dem Stand der Technik
- bei der Online-Software meinOnlineBüro
  - o der Schutz des Endgerätes obliegt dem Auftraggeber.
  - o Hilfe und Beratung bei Schutzmaßnahmen gegen mögliche Angriffe, der Schutz liegt aber im Verantwortungsbereich des Auftraggebers
- bei der Administration von meinOnlineBüro
  - o Backup- und Recovery-Konzept mit Sicherung der Daten.
  - o Einsatz von Festplattenspiegelung.
  - o Einsatz unterbrechungsfreier Stromversorgung.
  - o Einsatz von Softwarefirewall und Portreglementierungen.
  - o Maßnahmen gegen DDoS und sonstige Angriffe gegen die Systeme nach dem Stand der Technik
- Allgemein
  - o Firewalls
  - o Restriktive Einstellungen - nur sichere und erlaubte Dienste sind erreichbar
  - o Hardware-Firewall
  - o Software-Firewall
  - o Intrusion-Detection/Prevention-Systeme
  - o Anti-Viren-Software
  - o 24/7 Monitoring sämtlicher Dienste
  - o 24/7 Bereitschaftstechniker auf Abruf verfügbar
  - o erreichbar über Ticketsystem/E-Mail und zwei verschiedene Mobilfunknetze
  - o Stromversorgung
  - o 2 Trafostationen auf dem Gelände
  - o Unterbrechungsfreie Stromversorgung (USV) 320 kW
  - o Notstrom-Dieselmotor 500 kW
  - o N + 1 redundante Klimatisierung
  - o Geräte zur Überwachung von Temperatur in den Serverräumen
  - o Feuer- und Rauchmeldeanlagen
  - o Feuerlöschgeräte
  - o Schutzsteckdosenleisten in den Server-Racks
  - o Blitz- und Überspannungsschutz
  - o Notfallpläne

## 8. Trennungskontrolle

- bei der Online-Software meinOnlineBüro
  - o Datenverarbeitung erfolgt grundsätzlich auf je nach Zweck getrennten Systemen

- o Daten werden physikalisch oder logisch von anderen Daten getrennt gespeichert.
- o Die Datensicherung erfolgt ebenfalls auf logisch und/oder physikalisch getrennten Systemen.
- bei der Administration von meinOnlineBüro
  - o Die Trennungskontrolle obliegt dem Auftragnehmer.

## Impressum

Alle Rechte vorbehalten. Kein Teil dieses Dokuments darf in irgendeiner Form ohne schriftliche Genehmigung der meinOnlineBüro GmbH reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

## Kontakt

**mein ONLINE Büro**   
meinOnlineBüro GmbH

Lochhamer Str. 31  
82152 Planegg

Telefon: +49 89 9545 776 80

Telefax: +49 3212 9576010

E-Mail: [info@meinonlinebuero.de](mailto:info@meinonlinebuero.de)

Internet: [www.meinonlinebuero.de](http://www.meinonlinebuero.de)