Multipage

Multipage -
Ein Produkt der GBG AG
Technische und organisatorische Maßnahmen

1. Zutrittskontrolle
    1. Es ist sicherzustellen, dass der Zutritt zum Betriebsgelände in dem die Auftraggeberdaten verarbeitet werden, Unbefugten nicht ohne weiteres möglich ist.
    2. Fremdpersonal und Gäste dürfen sich nur in Begleitung, nach Anmeldung und mit entsprechender Kennzeichnung auf dem Betriebsgelände bewegen.
    3. Gebäude und Räumlichkeiten sind – sofern bei der Größe des Betriebes sinnvoll – in differenzierte Sicherheitsbereiche zu unterteilen und der Zugang zu den Räumlichkeiten entsprechend der dienstlichen Notwenigkeit zu erteilen.
    4. Zur Nachvollziehbarkeit ist eine Dokumentation über ausgegebene Schlüssel, Chip-, Transponder und Zugangskarten zu führen.
    5. Der Zugang zu IT-Serverräumen ist nur autorisiertem IT-Personal möglich.
    6. Das Gelände sollte durch eine Alarmanlage und/oder Sicherheitsdienst außerhalb der Betriebszeiten geschützt sein.
2. Zugangskontrolle
    1. Die unbefugte Nutzung der IT-Systeme ist durch technische Maßnahmen zu verhindern. Sie sind durch personalisierte Zugangsdaten mit individuellem Kennwort, oder andere Schutzmaßnahmen (Chipkarte, biometrische Zugänge, etc.) zu schützen.
    2. Beim Verlassen des Arbeitsplatzes ist das IT-System durch Bildschirmsperre vor unbefugtem Zugriff zu schützen. Die Sperrung ist nur durch Kennworteingabe aufzuheben.
    3. Alle PC-Systeme sind durch Virenscanner mit regelmäßigen Updates zu schützen.
    4. Das Unternehmensnetzwerk (LAN) muss am Übergang zum Internet durch eine Firewall geschützt sein.
    5. Wireless LAN ist mit aktuellen Sicherheitsstandards gegen unbefugten Zugriff zu schützen (z.B. WPA2, Radius-Authentifizierung).
    6. Mobile Geräte sollten durch eine eigenständige Firewall geschützt und - sofern sie personenbezogene Daten verarbeiten - verschlüsselt werden.
    7. Sofern personenbezogene Auftraggeberdaten auf portable Medien (USB-Sticks, Speicherkarten, USB-Festplatten, etc.) übertragen werden, sind diese nach aktuellen Sicherheitsstandards zu verschlüsseln.
    8. Der Zugriff auf das Unternehmensnetzwerk von außen erfolgt ausschließlich über eine gesicherte Authentifizierung und einem gesichertem Protokoll.
3. Zugriffskontrolle
    1. Es existiert ein dokumentiertes Berechtigungskonzept mit differenzierten Gruppen.
    2. Jeder Mitarbeiter darf nur die Berechtigungen innehaben, die er für die Ausführung seiner Tätigkeit benötigt.

3. Die erteilten Berechtigungen sind einer regelmäßigen (mind. einmal pro Kalenderjahr) Überprüfung zu unterziehen.
4. Es ist eine personelle Trennung zwischen Berechtigungsbewilligung und Berechtigungsvergabe sicherzustellen.
5. Datenträger (optisch, magnetisch, elektrisch, Papier) sind so zu entsorgen, dass die Daten nach der Vernichtung nicht wiederherstellbar sind.

4. Weitergabekontrolle
    1. Es muss gewährleistet sein, dass personenbezogene Auftraggeberdaten bei der Übermittlung weder gelesen, kopiert oder verändert werden können.
    2. Es muss sichergestellt sein, dass jederzeit überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen sind.
5. Eingabekontrolle

Zwecks Nachvollziehbarkeit ist eine Protokollierung der jeweiligen Applikationsbenutzung erforderlich.

6. Auftragskontrolle
    1. Es ist sicherzustellen, dass Auftraggeberdaten nur entsprechend der Zweckbindung verarbeitet werden.
    2. Die Mitarbeiter die nach §5 BDSG mit personenbezogenen Daten umgehen, sind auf das Datengeheimnis zu verpflichten.
    3. Sofern Subunternehmer eingesetzt werden, die mit personenbezogenen Auftraggeberdaten arbeiten, ist dies durch den Auftraggeber zustimmungspflichtig. Diese Subunternehmer sind gem. §11 zu verpflichten und unterliegen den hier aufgeführten technische und organisatorischen Maßnahmen.
    4. Der Auftragnehmer räumt dem Auftraggeber ein Auditrecht ein, um sich von den umgesetzten technischen und organisatorischen Maßnahmen zu überzeugen.
7. Verfügbarkeitskontrolle

Die IT-Serverräume sind mit technischen Maßnahmen gegen Ausfall und Datenverlust geschützt. Hierzu zählen eine unterbrechungsfreie Stromversorgung, Brandschutzmaßnahmen, Überspannungsschutz, Klimaanlage, Diebstahlschutz, sowie ein umgesetztes Backup- und Virenschutzkonzept.

8. Trennungsgebot

Es ist sichergestellt, dass die Daten des Auftraggebers getrennt von denen anderer Auftragnehmer verarbeitet werden (Mandantenfähigkeit). Es muss eine strikte Trennung zwischen Produktiv- und Testsystemen geben. Es darf nicht mit Produktivdaten auf Testsystemen getestet werden.

Multipage

Multipage
Technische und organisatorische Maßnahmen im Detail

Vertraulichkeit

- Physische Zugangskontrolle
  Unsere Server und Datenbanksysteme sind in einem Rechenzentrum entsprechend der ISO 27001 Zertifizierung installiert. Somit ist kein unbefugter Zugang zu diesen Datenverarbeitungseinrichtungen möglich.
  - Wir benennen befugte Personen (Betriebsangehörige)
  - diese erhalten Berechtigungsausweise (RFID) oder Schlüssel
  - Firmenfremde sind nicht Zugangsberechtigt und werden wie Besucher behandelt
  - Wir führen Anwesenheitsaufzeichnungen
  - wir erstellen Besucherausweise
  - Die Sicherung auch außerhalb der Arbeitszeit erfolgt durch Alarmanlagen
  - Wir unterscheiden Sicherheitsbereiche
  - RFID gesicherter Eingang wird auch für Lieferungen genutzt
  - Türen sind gesichert durch elektrische Türschließer und Ausweisleser
  - zur Objektsicherung zählen wir die Absicherung von Schächten und des Geländes

- Elektronische Zugangskontrolle
  Durch verschiedene Maßnahmen stellen wir sicher, dass keine unbefugte Nutzung der Systeme zur Datenverarbeitung und -speicherung möglich ist. Wir verwenden und fordern von allen Anwendern sichere Passwörter, die sich regelmäßig ändern müssen. Die Netzwerkverbindungen sind SSL verschlüsselt. Unsere Mitarbeiter sind auf das Datengeheimnis verpflichtet und nehmen regelmäßig an Schulungen teil.

- Interne Zugangskontrolle
  Wir stellen sicher, dass lediglich notwendigen Personen erweiterte Nutzerrechte für den Zugang zu und die Änderung von Daten zugewiesen sind. So ist ein unbefugtes Lesen, Kopieren, Ändern oder Löschen von Daten im System durch das Berechtigungskonzept und die Zugangsrechte auf Need-to-know-Basis umgesetzt. Änderungen an den Nutzerrechten werden dokumentiert und geprüft. Zugänge werden protokolliert.

- Trennung nach Zweck
  Eine getrennte Verarbeitung von Daten, die für verschiedene Zwecke erhoben werden ist realisiert durch die Trennung von Systemen und die Unterstützung des Anwenders zu mehreren Zwecken.

- Pseudonymisierung
  Dies liegt in der Verantwortung unsere Kunden.

Integrität

- Kontrolle der Datenübermittlung
  Datenübermittlung ist SSL verschlüsselt, damit kein unbefugtes Lesen, Kopieren, Ändern oder Löschen von Daten bei deren elektronischer/m Übermittlung oder Transport möglich ist.

- Kontrolle der Dateneingabe
  Multipage überprüft, ob und von wem personenbezogene Daten eingegeben bzw. in diesem geändert oder gelöscht werden und protokolliert dies.

Verfügbarkeit und Belastbarkeit

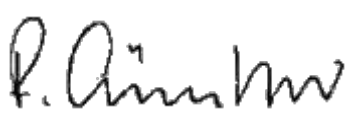
- Verfügbarkeitskontrolle
  Wir haben technische Vorkehrungen getroffen, um versehentliches oder absichtliches Zerstören oder den Verlust von Daten möglichst auszuschließen. Dazu zählen wir unsere Datensicherungs- und Backup-Konzeption, die innerhalb und außerhalb des Standortes der Systeme umfasst. Unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldeverfahren, Monitoring und Notfallplanung sind realisiert.

- Rasche Wiederherstellung
  Durch unsere hochverfügbare technische Clusterumgebung ist eine rasche Wiederherstellung und die Verfügbarkeit der Systeme und Daten sichergestellt.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Wir unterscheiden folgende Verfahren:

- Datenschutzmanagement
- Reaktionsmanagement
- Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen
- Auftrags- oder Vertragskontrolle
  Die Verarbeitung durch Dritte erfolgt ausschließlich auf entsprechende Weisungen durch dafür benannte Mitarbeiter und basiert auf eindeutigen vertraglichen Vereinbarungen. Unsere Auswahl der Dienstleister beinhaltet eine verpflichtende Vorab-Evaluierung sowie regelmäßige Nachkontrollen zur Überwachung.



Roland Günther
Geschäftsführer GBG AG