# Technische und organisatorische Maßnahmen gem. Art. 32 DSGVO

ITSM IT-Systeme & Management GmbH

# Sicherheitskonzept

Technische und organisatorische Maßnahmen gem. Art. 32 DSGVO

## Grundsätzliche Maßnahmen

Grundsätzliche Maßnahmen, die der Wahrung der Betroffenenrechte, unverzüglichen Reaktion in Notfällen, den Vorgaben der Technikgestaltung und dem Datenschutz auf Mitarbeiterebene dienen:

- Die Mitarbeiter werden im Hinblick auf den Datenschutz und Vertraulichkeit sowie Informations-/IT-Sicherheit regelmäßig geschult (1x jährlich).
- Mitarbeiter werden im Hinblick auf den Datenschutz auf Verschwiegenheit verpflichtet und auf mögliche Haftungsfolgen hingewiesen.
- Die an Mitarbeiter ausgegebene Schlüssel werden nach deren Ausscheiden aus dem Unternehmen, bzw. Wechsel der Zuständigkeiten eingezogen, bzw. entzogen.
- Die eingesetzte Software wird stets auf dem aktuell verfügbaren Stand gehalten, ebenso wie Virenscanner und Firewalls.
- Es gelten die allgemeinen TOMs - sofern beim Standort andere Gegebenheiten vorhanden sind, werden diese nachfolgend aufgeführt.

## Zutrittskontrolle - Technische Maßnahmen

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Benutzeridentifikation von ausgeschiedenen Mitarbeitern werden deaktiviert.
- Nur berechtigte Personen haben Zutritt zu den Räumen in dem sich Server, Firewall und Netzwerkverteiler befinden.
- Server, Firewall und Netzwerkverteiler sind in ständig verschlossenen Räumen.
- Server sind in einem zutrittsgesichertem Raum.
- Sicherheitsschlösser
- Manuelles Schließsystem

## Zutrittskontrolle - Organisatorische Maßnahmen

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Besucher werden von einem Mitarbeiter zum gewünschten Ort begleitet.
- Zutrittsregelungen für betriebsfremde Personen.

## Zugangskontrolle - Technische Maßnahmen

Zugangskontrolle: Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

- Firewall (Hardware)
- Stets aktuelle Softwareversionen.
- Spezielle Benutzerprofile
- Notebooks sind verschlüsselt.
- Das automatische Ausführen von Anwendungen auf USB-Datenträgern und Wechselmedien wird blockiert
- Einsatz von VPN-Technologie oder einer anderen sicheren Verbindung.
- Einsatz von Mobile Device Management.
- Trivialpassworte werden vom System abgewiesen.
- Passwort kann vom Anwender selbst vergeben und selbst geändert werden.
- Stets aktueller Virenschutz.
- Verschlüsselung von Festplatten (FileVault, Bitlocker)
- Authentifikation mit Benutzer + Passwort+Multifaktorauthentifizierung.
- Protokollierung von Zugriffen auf Windows-Server.

## Zugangskontrolle - Organisatorische Maßnahmen

Zugangskontrolle: Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

- Passwörter sind nur seinem Benutzer bekannt.
- Benutzerrollen sind ausführlich dokumentiert.

## Zugriffskontrolle - Technische Maßnahmen

Zugriffskontrolle : Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

- Normale Anwender verfügen nicht über Administratorenrechte.
- Benutzer nach einer bestimmten Zeit der Inaktivität automatisch abgemeldet.
- Automatische Desktop- Sperre/ Bildschirmsperre mit Passwort.
- Anzahl der Administratoren ist auf das Notwendigste reduziert.
- Benutzerrechte werden durch Systemadministratoren verwaltet.
- Benutzerberechtigungen ausgeschiedener Mitarbeiter werden zeitnah gesperrt.

## Zugriffskontrolle - Organisatorische Maßnahmen

Zugriffskontrolle : Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

- Berechtigungskonzept vorhanden.

## Gewährleistung des Zweckbindungs-/Trennungsgebotes - Technische Maßnahmen

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Es existiert eine Trennung von Produktiv-, Test- und Schulungssystemen. Die Serverstrukturen befinden sich an den Standorten Fraureuth und Dresden. In Erfurt und Wildau gibt es keine Server.

## Gewährleistung des Zweckbindungs-/Trennungsgebotes - Organisatorische Maßnahmen

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Steuerung über Berechtigungskonzept.

## Weitergabekontrolle - Technische Maßnahmen

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- E-Mail-Verschlüsselung TLS
- Speichermedien (z. B. Festplatten, USB-Sticks) werden vor ihrer Aussonderung sicher gelöscht oder sicher vernichtet.
- Bereitstellung über verschlüsselte Verbindungen wie z.B. sftp, https.
- Das Unternehmen stellt die Hard- und Software für den Home-Office Arbeitsplatz.
- Das Unternehmen stellt die Hard- und Software für den Mobile-Office Arbeitsplatz.
- Aktenvernichter mit geeigneter Sicherheitsstufe.
- Einrichtung von VPN Tunneln oder andere sichere Verbindungen.

## Weitergabekontrolle - Organisatorische Maßnahmen

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Einsatz von zertifizierten Papierentsorgungsunternehmen mit Protokollerstellung.

## Eingabekontrolle - Organisatorische Maßnahmen

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen).

## Verfügbarkeitskontrolle - Technische Maßnahmen

Es soll durch geeignete Maßnahmen sichergestellt werden, dass EDV-Systeme die an sie gestellten Anforderungen zuverlässig erfüllen. Dazu gehören Infrastrukturmaßnahmen, System-Wartung, Datensicherung o. Ä. (Verfügbarkeitskontrolle, d. h. Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind).

- Serverräume sind nicht unter sanitären Anlagen
- Tests für eine Datenwiederherstellung werden durchgeführt.
- Tägliche Datensicherung fürs Produktivsystem pds
- Rauchmeldeanlagen im Serverraum.
- Unterbrechungsfreie Stromversorgung (USV)
- RAID System / Festplattenspiegelung vorhanden
- Getrennte Partitionen für Betriebssysteme und Daten.

## Datenschutzfreundliche Voreinstellungen - Organisatorische Maßnahme

Privacy by design / Privacy by default

- Zweckbindung der erhobenen und gespeicherten Daten wird eingehalten.
- Bei einer Zweckänderung wird das Einverständnis der Betroffenen eingeholt.
- Der Umfang der erhobenen personenbezogenen Daten und dessen Verarbeitung ist auf das Notwendige begrenzt.

## Datenschutz-Management - Technische Maßnahmen

Es soll durch geeignete Maßnahmen sichergestellt werden, dass der Stand der Informationssicherheit regelmäßig geprüft, aktualisiert und dokumentiert wird.

- Software-Lösungen für Datenschutz-Management im Einsatz.

## Datenschutz-Management - Organisatorische Maßnahme

Es soll durch geeignete Maßnahmen sichergestellt werden, dass der Stand der Informationssicherheit regelmäßig geprüft, aktualisiert und dokumentiert wird.

- Ein externer Datenschutzbeauftragter ist vorhanden.
  ad hoc datenschutz GmbH
  (Anthony Thomas)
  Im Bresselsholze 12
  07819 Triptis

  Tel.: 0365 52786230
  E-Mail: kontakt@adhoc-datenschutz.de

- Mitarbeiter geschult und auf Vertraulichkeit und Datengeheimnis verpflichtet.
- Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt.
- Regelmäßige Schulungen zur Auffrischung für bestehendes Personal (z. B. einmal pro Jahr).
- Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt.
- Führen eines Verzeichnis von Verarbeitungstätigkeiten.

## Incident-Response-Management - Technische Maßnahmen

- Einsatz von Spamfilter und regelmäßige Aktualisierung.
- Einsatz von Virenscanner und regelmäßige Aktualisierung.
- Einsatz von Firewall und regelmäßige Aktualisierung.

## Incident-Response-Management - Organisatorische Maßnahmen

- Einbindung von DSB in Sicherheitsvorfälle und Datenpannen.
- Dokumentation von Sicherheitsvorfällen und Datenpannen in der Software im DSMS.
- Einbindung IT-Admin bei Störung der PC Arbeitsplätze.

## Maßnahmen zur Datenminimierung

Maßnahmen, die gewährleisten, dass Daten nur insoweit verarbeitet werden, wie dies für einen konkreten Zweck erforderlich und angemessen ist.

- Es werden nur die personenbezogenen Daten erhoben/verarbeitet die für den jeweiligen Prozess notwendig sind.
- Es erhalten nur diejenigen Personen/Stellen Zugriff auf die personenbezogenen Daten, die diese für ihre Aufgabenerfüllung benötigen.

## Auftragskontrolle - Organisatorische Maßnahmen

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Schriftliche Festlegung der Weisungen.
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis.
- Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus.
- Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht.
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer.
- Auswahl von Auftragnehmern unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit).
- Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation.
- Abschluss eines Vertrages zur Auftragsverarbeitung gem. Art. 28 DSGVO