# Technische und organisatorische Maßnahmen

**Stand: Mai 2018**

**Unternehmen:**
GfG – Gesellschaft für Gebäudemanagement mbH
Schulstraße 4
65439 Flörsheim am Main

**Kontakt:**
Tel.: 06145 / 590 610
E-Mail: info@gfg.de

nachfolgend zur Vereinfachung (GfG) genannt.

Zur Erbringung der vertraglich vereinbarten Leistungen nutzt GfG die folgenden technischen und organisatorischen Maßnahmen, welche den Forderungen des Artikels 32 (Datenschutz-Grundverordnung) entsprechen.

**eigene Räumlichkeiten**

Zugangskontrolle
Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte.

- Sämtliche Außentüren sind mit einem Schließsystem versehen und sind außerhalb der Bürozeiten grundsätzlich verschlossen.
- Alle Schlüssel sind personengebunden registriert.
- Besucher dürfen sich nur in Begleitung eines Mitarbeiters in den Räumlichkeiten bewegen.
- Personal von Dritten, insbesondere für Reinigungs- und Wartungsaufgaben werden sorgfältig ausgewählt.
- Alle Räumlichkeiten sind, je nach Erfordernis, durch entsprechende Schutzeinrichtungen wie z.B. zusätzlich durch Gitter und vollflächig durch eine Einbruchmeldeanlage geschützt.

**Rechenzentrum**

Zugangskontrolle
Verwehrung des Zugangs zu Verarbeitungsanlagen. mit denen die Verarbeitung durchgeführt wird, für Unbefugte.

- Der Zutritt zu den Datenzentren ist nur autorisierten Personen gestattet.
- Der Zutritt ist durch Biometrische Zutrittssysteme (Fingerabdruck) gesichert.
- Die Zutrittskontrollsysteme sowie die Alarmanlagen sind über USV und Netzersatzanlagen gegen Stromausfall gesichert.
- Die Datenzentren werden rund um die Uhr durch Sicherheitspersonal überwacht.
- Die Datenzentren verfügen über eine Einbruchmeldeanlage.

**eigene Räumlichkeiten**

Datenträgerkontrolle
Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern.

- Der Zugriff auf die Anwendungs- und Datenbankserver der Infrastruktur ist nur einzelnen und entsprechend qualifizierten Mitarbeitern oder Dritten gestattet.
- Die Systeme sind durch Firewalls und entsprechend gehärtete Konfigurationen aller Systemkomponenten gegen unbefugten Zugriff von außen bestmöglich abgesichert.

**Rechenzentrum**

Datenträgerkontrolle
Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern.

- Der Zugriff auf physische Systeme seitens des Infrastruktur-Anbieters erfolgt nur über eine SSH-Verbindung, wobei nur die SSH-Schlüsselauthentifizierung verwendet wird. Die Nutzung einer Passphrase auf Schlüssel ist obligatorisch.
- Der Zugriff ist auf ausgewählte Mitarbeiter des zuständigen Bereiches beschränkt. Technisch haben diese Mitarbeiter, deren Prozesse konform zu ITIL erstellt wurden, keine Möglichkeit Kunden-Volumes zu mounten oder deren Inhalte einzusehen.
- Der Zugriff wird zudem nur über ganz bestimmte und festgelegte Kommunikationswege ermöglicht um die Daten noch besser zu schützen.

**eigene Räumlichkeiten**

Speicherkontrolle
Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

- Der Zugriff auf die Anwendungs- und Datenbankserver der Infrastruktur ist nur einzelnen und entsprechend qualifizierten Mitarbeitern und Dritten gestattet. Die Systeme sind durch Firewalls und entsprechend gehärtete Konfigurationen aller Systemkomponenten gegen unbefugten Zugriff von außen bestmöglich abgesichert.
- Der Zugriff auf die Infrastruktur ist nur über den Administrator-Account möglich.
- Es sind nur die für den Betrieb notwendigen Ports geöffnet.

**Rechenzentrum**

Speicherkontrolle
Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

- Der Zugriff auf physische Systeme seitens des Infrastruktur-Anbieters erfolgt nur über eine SSH-Verbindung, wobei nur die SSH-Schlüsselauthentifizierung verwendet wird. Die Nutzung einer Passphrase auf Schlüssel ist obligatorisch.
- Der Zugriff ist auf ausgewählte Mitarbeiter des zuständigen Bereiches beschränkt. Technisch haben diese Mitarbeiter, deren Prozess konform zu ITIL erstellt wurde, keine Möglichkeit Kunden-Volumes zu mounten oder deren Inhalte einzusehen.
- Der Zugriff wird zudem nur über ganz bestimmte und festgelegte Kommunikationswege ermöglicht um die Daten noch besser zu schützen.

**eigene Räumlichkeiten / Rechenzentrum**

Benutzerkontrolle
Verhinderung der Nutzung automatisierter Verarbeitungssystem mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte.

- Die Zugriffsrechte der Anwender und Administratoren orientieren sich an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen nach dem Need-to-know Prinzip.

**eigene Räumlichkeiten**

Zugriffskontrolle
Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben.

- Die Zugriffsrechte der Anwender und Administratoren orientieren sich an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen nach dem Need-to-know-Prinzip.
- Der Schutz gegen unberechtigte interne und externe Zugriffe erfolgt durch Verschlüsselung und Firewalls.
- Alle Mitarbeiter sind gemäß Art. 24 Abs. 1 und 2 und Art 39 Abs. 1 lit a der DSGVO im Bereich „IT-Sicherheit“ und „Datenschutz für Mitarbeiter“ geschult und auf das Datengeheimnis verpflichtet.

**Rechenzentrum**

Zugriffskontrolle
Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben.

- Die Zugriffsrechte der Anwender und Administratoren orientieren sich an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen nach dem Need-to-know-Prinzip.
- Der Schutz gegen unberechtigte interne und externe Zugriffe erfolgt durch Verschlüsselung und Firewalls.

**eigene Räumlichkeiten**

Übertragungskontrolle
Gewährleistung, dass überprüft und festgestellt werden kann, an welchen Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

- Alle VPN-Aktivitäten werden durch SSL/TLS geschützt.
- Verschlüsselung relevanter Inhalte, sowohl beim physischen, als auch digitalen Transport von Daten.

**Rechenzentrum**

Übertragungskontrolle
Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

- Alle Datenübertragungen werden durch SSL/TLS geschützt.
- Sicherung bei der elektronischen Übertragung durch den Einsatz geeigneter Fernwartungslösungen.
- Der Schutz gegen unberechtigte interne und externe Zugriffe erfolgt durch Firewalls.

**eigene Räumlichkeiten / Rechenzentrum**

Eingabekontrolle
Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind.

- Die Zugriffsrechte der Anwender und Administratoren orientieren sich an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen.
- Aufgrund von individuellen Nutzerkennungen sowie Protokolldaten kann überprüft und festgestellt werden, ob und von wem personenbezogene Daten und Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

**eigene Räumlichkeiten / Rechenzentrum**

Transportkontrolle
Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

- Alle VPN-Aktivitäten werden durch SSL/TLS geschützt.
- Verschlüsselung relevanter Inhalte, sowohl beim physischen, als auch digitalen Transport von Daten.

**eigene Räumlichkeiten**

Wiederherstellung
Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können. Maßnahme zum Schutz gegen zufällige Zerstörung oder Verlust personenbezogener Daten.

- Spiegelung der Daten mittels RAID-5 + HotSpare
- Tägliche Backups zu getrennten Standorten.
- Unterbrechungsfreie Stromversorgung (USV).
- Eine weitere Stromversorgung als Ersatzleitung.
- Kühlsysteme je Abschnitt.
- Bauabschnitte verfügen über Brand-, Wasser- und Einbruchsschutz.

**Rechenzentrum**

Wiederherstellung
Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können. Maßnahme zum Schutz gegen zufällige Zerstörung oder Verlust personenbezogener Daten.

- Spiegelung der Daten mittels RAID-5 + HotSpare
- Spiegelung der Daten auf einem anderen Server.
- Tägliche Backups zu getrennten Standorten.
- 2 Unterbrechungsfreie Stromversorgungen (USV).
- 2 Netzersatzanlagen für das gesamte Gebäude.
- Elektro-Installation mit Überspannungsschutz und Energieverteilung.
- Redundante Klimageräte N+1
- Bauabschnitte verfügen über Brand-, Wasser- und Einbruchsschutz.

**eigene Räumlichkeiten / Rechenzentrum**

Zuverlässigkeit
Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

- In unregelmäßigen Abständen werden intern Ausfallszenarien, welche von Hardware- und/oder Softwarefehlern verursacht wurden, durchgeführt. Ziel dieser Szenarien ist festzustellen, ob alle Backups reibungslos funktionieren und in welcher Zeit das System wieder einsatzbereit ist.
- Nutzung von Monitoring-Tools um Probleme mit Hardware- und Softwarekomponenten frühzeitig zu erkennen und beheben zu können.
- Durchgehende Überprüfung des IT-Inventars durch entsprechende Tools.
- Überwachungsanlage mit automatischer Weitermeldung im Störungsfall.
- Ein Hardwareausfall wird direkt erkannt und im laufenden Betrieb behoben, wodurch dieser für den Nutzer also unbemerkt bleibt und auch keine sichtbare Einschränkung zur Folge hat.
- Um eine Nichtverfügbarkeit der Plattform mangels Hardwareressourcen ausschließen zu können werden verschiedene Funktionen eingesetzt, durch welche die zur Verfügung stehenden Ressourcen gezielt und in Echtzeit angepasst werden können.

**eigene Räumlichkeiten / Rechenzentrum**

Datenintegrität
Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

- Einsatz von Firewalls um potentielle Angriffe und daraus resultierende Fehlfunktionen zu verhindern.
- In unregelmäßigen Abständen werden intern Ausfallszenarien, welche von Hardware- und/oder Softwarefehlern verursacht wurden, durchgeführt. Ziel dieser Szenarien ist festzustellen, ob alle Backups reibungslos funktionieren und in welcher Zeit das System wieder einsatzbereit ist.
- Nutzung von Monitoring-Tools um Probleme mit Hardware- und Softwarekomponenten frühzeitig zu erkennen und beheben zu können.
- Durchgehende Überprüfung des IT-Inventars durch entsprechende Tools.
- Ein Hardwareausfall wird direkt erkannt und im laufenden Betrieb behoben, wodurch dieser für den Nutzer also unbemerkt bleibt und auch keine sichtbare Einschränkung zur Folge hat.
- Um eine Nichtverfügbarkeit der Plattform mangels Hardwareressourcen ausschließen zu können werden verschiedene Funktionen eingesetzt, durch welche die zur Verfügung stehenden Ressourcen gezielt und in Echtzeit angepasst werden können.

**eigene Räumlichkeiten**

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

- Die Verarbeitung der personenbezogenen Daten geschieht ausschließlich im Rahmen der vertraglich festgelegten Weisungen des Auftraggebers.
- Mit Unternehmen, die mit der Verarbeitung personenbezogener Daten beauftragt sind, wurden entsprechende und geeignete Auftragsdatenverarbeitungsverträge geschlossen.
- Die Zugriffsrechte der Anwender und Administratoren orientieren sich an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen nach dem Need-to-know Prinzip.

**Rechenzentrum**

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

- Die Verarbeitung der personenbezogenen Daten geschieht ausschließlich im Rahmen der vertraglich festgelegten Weisungen des Auftraggebers.
- Mit Unternehmen, die mit der Verarbeitung personenbezogener Daten beauftragt sind, wurden entsprechende und geeignete Auftragsdatenverarbeitungsverträge geschlossen.
- Die Zugriffsrechte der Anwender und Administratoren orientieren sich an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen nach dem Need-to-know Prinzip.
- Das Rechenzentrum, in denen unsere externen Server stehen ist nach DIN ISO 27001 zertifiziert.

**eigene Räumlichkeiten**

Verfügbarkeitskontrolle
Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind. Maßnahmen zum Schutz gegen zufällige Zerstörung oder Verlust personenbezogener Daten.

- Spiegelung der Daten mittels RAID-5 + HotSpare
- Tägliche Backups zu getrennten Standorten.
- Unterbrechungsfreie Stromversorgung (USV).
- Eine weitere Stromversorgung als Ersatzleitung.
- Kühlsysteme je Abschnitt.
- Bauabschnitte verfügen über Brand-, Wasser- und Einbruchsschutz.

**Rechenzentrum**

Verfügbarkeitskontrolle
Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind. Maßnahmen zum Schutz gegen zufällige Zerstörung oder Verlust personenbezogener Daten.

- Spiegelung der Daten mittels RAID-5 + HotSpare
- Spiegelung der Daten auf einem anderen Server.
- Tägliche Backups zu getrennten Standorten.
- 2 Unterbrechungsfreie Stromversorgungen (USV).
- 2 Netzersatzanlagen für das gesamte Gebäude.
- Elektro-Installation mit Überspannungsschutz und Energieverteilung.
- Redundante Klimageräte N+1
- Bauabschnitte verfügen über Brand-, Wasser- und Einbruchsschutz.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.