# Anlage 1

**Version:** 1.1
**Stand:** 01.07.2021

Gerst ITS
Customized IT-Solutions

## Technische und organisatorische Maßnahmen nach Art.32 DSGVO

# 1. Zutrittskontrolle

Mit der Zutrittskontrolle soll verhindert werden, dass unberechtigte Personen Zutritt zu den informationsverarbeitenden Systemen von Gerst ITS bekommen. Unser Rechenzentrum gewährleistet einen hohen Schutz durch moderne Sicherheitstechnik und umfassende Objekt- und Datenschutzmaßnahmen. Der Zutritt zum Rechenzentrum ist dabei nur einem eingeschränkten Kreis von autorisierten Mitarbeitem möglich.

## 1.1 Organisatorische Maßnahmen

### 1.1.1 Empfang- und Ausweispflicht

Der Standort des Rechenzentrumgebäudes wird 24/7 durch einen Sicherheitsdienst überwacht. Auffälligkeiten werden durch die Einbruchmeldeanlage und Kontrollgänge des Sicherheitsdienstes entdeckt. Am Standort des Rechenzentrums besteht für alle Besucher und externen Mitarbeiter die Pflicht, sich mit einem amtlichen Dokument auszuweisen (Personalausweis/Reisepass). Jeder Besucher muss sich in ein elektronisches Besucherprotokoll eintragen. Jeder Besucher erhält zur Kennzeichnung einen Besucherausweis, der ersichtlich getragen werden muss. Einen Zugang zu unserer Rackfläche im Rechenzentrum hat nur Gerst ITS und der Rechenzentrumsbetreiber, für Wartungsarbeiten an Klima/Luftzufuhr, Uplink-Verkabelung und Spannungszufuhr. Die Arbeiten werden entsprechend vom Betreiber des Rechenzentrums dokumentiert.

### 1.1.2. Schlüsselvergabe

Durch das installierte Zutrittskontrollsystem können nur Personen in das Rechenzentrum gelangen, die im Vorfeld Berechtigungen beim Rechenzentrumsbetreiber beantragt haben und sich gemäß dessen Vorgaben autorisiert haben. Hierfür existiert ein formaler Genehmigungsprozess. Der Zutritt zum Rechenzentrum erfolgt über ein spezielles RFID-Zugangstoken, die nach Anforderung und Unterschrift des Empfängers dem Berechtigten ausgehändigt wird. Die Vergabe der RFID-Tokens wird vom Rechenzentrumsbetreiber durchgeführt und dokumentiert. Die Berechtigungen können losgelöst von der physischen Verfügbarkeit der RFID-Tokens geändert, gelöscht oder gesperrt werden.

## 1.1 Technische Maßnahmen

Das Rechenzentrum wird durch folgende technische Maßnahmen vor unberechtigtem Zutritt geschützt:

- Zutrittskontrollsystem
- Einbruchmeldeanlage
- Videokameras
- Sicherheitsschleusen und -türen
- Bereichswechselkontrolle

Ein wichtiger Bestandteil des Sicherheitskonzeptes ist der Zutritt zum zentralen Rechenzentrum über eine Personalvereinzelungsanlage (Sicherheitsschleuße).

### 1.2.1 Türsicherung

Eine Sicherheitsschleuse gewährleistet, dass nur einzelne berechtigte Personen das Rechenzentrum betreten können. Um die Sicherheitsschleuse betreten zu können, wird ein elektronischer Schlüssel (so genannter RFID-Token), der für den Zugang explizit freigeschaltet sein muss, benötigt. Nur nach positiver Prüfung der Sicherheitsmerkmale wird der Zutritt zum Rechenzentrum durch die Sicherheitsschleuse gewährt.

### 1.2.2. Zutrittskontrollsystem und Überwachung

Der Standort des Rechenzentrums verfügt über Zugangsleser an allen Außentüren, sowie an den Zugängen an den Fahrstühlen. Alle Zugänge zum Rechenzentrum sind videoüberwacht.

# 2. Zugangskontrolle

Mit der Zugangskontrolle soll ein Eindringen unberechtigter Personen in die Informationsverarbeitenden Systeme von Gerst ITS verhindert werden. Hierzu sind technische und organisatorische Maßnahmen hinsichtlich der Benutzeridentifikation und Authenthifizierung implementiert.

## 2.1. Organisatorische Maßnahmen

### 2.1.1. Benutzer- und Berechtigungsverfahren

Benutzer, die im Rahmen Ihrer Aufgabenerfüllung zu einem System Rechte erlangen sollen, müssen diese Berechtigungen über einen formalen Benutzer- und Berechtigungsprozess beantragen. Im Benutzer- und Berechtigungs-Verwaltungssystem werden die Benutzerkennungen und Berechtigungen von Benutzern geführt. Technisch erfolgt die Genehmigung für das Erteilen und Löschen von Zugriffsrechten, in denen der Vorgang dokumentiert wird. Im Verwaltungssystem werden Berechtigungen von Benutzern gesperrt, wenn die Berechtigungen nicht mehr benötigt oder unberechtigt benutzt werden.

## 2.2. Technische Maßnahmen

### 2.2.1. Authentisierungsverfahren

Zugangsberechtigungen sind so feingranular wie möglich konfiguriert, so dass Personen nur dort Zugang haben, wo sie diesen auf Grund ihrer Funktion und ihrer Aufgabenerfüllung benötigen. Die Zugangskontrollverfahren gelten für alle Mitarbeiter von Gerst ITS. Alle Systeme sind durch Authentifizierungsverfahren (Benutzer-ID und Passwort) geschützt, die unberechtigte Zugriffe unterbinden. Werden im Rahmen des Authentifizierungsverfahrens Passwörter eingesetzt, müssen diese den internen Passwortrichtlinien und Systemen entsprechen. Passwörter, die nach den Richtlinien nicht der Qualität entsprechen, sind nicht erlaubt. Die Systeme werden nach einer bestimmten Zeit der Inaktivität automatisch gesperrt. Zusätzlich werden Accounts automatisch deaktiviert, wenn deren Passwöter nicht geändert werden.

Ein Fernzugriff auf interne Systeme ist nur in authentifizierter Form möglich, bei dem z.B. asymmetrische Authentisierungsverfahren (Public-/Private-Key-Verfahren) eingesetzt werden, die zusätzlich zur Nachweisbarkeit protokolliert werden. Der Zugriff auf interne Systeme wird nur betimmten autorisierten Administratoren gewährt. Der Zugriff auf interne Systeme über Verbindungen kann nur durch einen zusätzlichen SSL Tunnel erfolgen.

### 2.2.2. Verschlüsselung

Alle Daten werden mit nativen Verschlüsselungsalgorythmen auf den Festpaltten selbst verschlüsselt. Daten mit hohen Schutzbedürfnissen werden zusätzlich nach aktuellem Stand der Technik mit verschlüsselten Verfahren gesichert. Die eingesetzten Verschlüsselungsverfahren basieren auf dem aktuellen Stand der Technik. Datenträger, die nicht mehr zum produktiven Einsatz kommen, werden durch sichere Lösch- und Überschreibverfahren gelöscht.

# 3. Zugriffskontrolle

Mit der Zugriffskontrolle sollen unerlaubte Handlungen in den informationsverarbeitenden Systemen von Gerst ITS verhindert werden, indem Maßnahmen zur Überwachung und Protokollierung der Zugriffe implementiert werden.

## 3.1. Berechtigungsvergabe

Die Systeme wurden in der Weise konfiguriert, dass ein regulärer Zugriff mit administrativen Rechten nur für interne, autorisierte Mitarbeiter möglich ist. Hier wurden bedarfsorientierte Berechtigungskonzepte ausgestaltet, die die Zugriffsrechte, sowie deren Überwachung und Protokollierung definieren. Eine Berechtigungsvergabe wird stets nach dem Need-to-know-Prinzip vergeben. Je nach Autorisierung werden differenzierte Berechtigungen, untergliedert nach Rollen und Profilen von Benutzern eingerichtet.

## 3.2. Auswertungen

Zugriffe auf System-IDs und auffällige Zugriffsversuche werden protokolliert. Der Zugriff auf die Protokolle ist durch autorisierte Administratoren möglich. Beim auffälligen Zugriffsversuch wird zuätzlich eine Alarmierung an den zuständigen Systemverantwortlichen ausgelöst.

## 3.3. Veränderungen

Modifikationen an Zugriffsrechten können lediglich von Systemadministratoren vorgenommen werden, die die Freigabe erhalten haben. Veränderungen der Zugriffsrechte und Berechtigungen geschehen in der Regel innerhalb eines Arbeitstages, wenn nicht sogar bei Bedarf sofort. Netzwerkgeräte oder Systeme mit voreingestellten Zugriffsmöglichkeiten dürfen nicht im Produktivbereich verwendet werden.

## 3.4. Löschung

Das Löschen von Benutzerberechtigungen erfolgt zeitnah, spätestens jedoch innerhalb eines Arbeitstages. Das Löschen von Zugriffsrechten geschieht auch im Rahmen der Systemdiagnose. Hier werden obsolete Zugriffsrechte bereinigt.

# 4. Weitergabekontrolle

Im Rahmen der Weitergabekontrolle werden Maßnahmen beim Transport, der Übertragung und Übermittlung, sowie bei der nachträglichen Überprüfung von personenbezogenen Daten definiert.

## 4.1. Organisatorische Maßnahmen

### 4.1.1. Schulungsmaßnahmen

Alle Mitarbeiter von Gerst ITS sind zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DS-GVO) hin verpflichtet worden.

### 4.1.2. Klassifizierung der Informationen

Jede Information muss nach ihrem Schutzbedarf eingestuft werden. Handelt es sich um vertrauliche Informationen, müssen diese besonders behandelt werden. Vertrauliche, dienstliche Informationen dürfen nur über sichere Kommunikationswege übertragen werden. Es sind insbesondere folgende Regeln einzuhalten:

- Es müssen spezielle Verfahren und Regelungen zum Schutz der Informationen und Datenträger beim Transport, insbesondere über Unternehmensgrenzen hinweg eingehalten und dokumentiert werden.
- Es müssen so weit wie möglich kryptographische Verfahren, z.B. Verschlüsselung bei der Übertragung vertraulicher Daten, eingesetzt werden.
- Bei der Übergabe an externe Empfänger ist die erfolgte vollständige und sichere Übergabe nachweisbar zu dokumentieren.

## 4.2. Technische Maßnahmen

### 4.2.1. Zugriffs-und Transportsicherung

Grundsätzlich können auf die Systeme, die personenbezogene Daten verarbeiten, nur autorisierte Administratoren zugreifen. Die Übertragung von Daten erfolgt ausschließlich durch das System selbst an autorisierte Empfänger über kryptographisch gesicherte Wege. Die Übertragung wird in Logfiles protokolliert.

Der Zugriffsschutz auf Systeme mit sensiblen Informationen wird auf mehreren Ebenen realisiert - Auf Dateisystem-, auf Betriebssystem- und auf Netzwerkebene. Die Schutzmechanismen erlauben nur speziell autorisierten Administratoren den Zugriff auf die jeweilige Ebene. Um Datenverlust vorzubeugen, müssen alle arbeitsrelevanten Daten auf Servern gespeichert werden. Diese Daten werden regelmäßig nach definierten Backup-Konzepten gesichert, so dass ein Datenverlust dadurch weitestgehend ausgeschlossen ist.

### 4.2.2. Protokollierung

Der Zugriff und die Aktivitäten der Administratoren werden In speziellen Protokolldateien aufgezeichnet. Die Protokollierung der Zugriffe erfolgt direkt auf den Systemen. Der Zugriff auf die Protokolle ist geschützt und nur autorisienen Administratoren gestattet.

# 5. Eingabekontrolle

Um die Nachvollziehbarkeit und Dokumentation der Datenvenwaltung und -pflege sicherzustellen, werden Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder gelöscht worden sind, implementiert.

## 5.1. Protokollierungs- und Protokollauswertung

Durch die Einhaltung der oben aufgeführten Regeln zu Zutrittskontrolle, Zugangskontrolle und Zugriffskontrolle wurde die Grundlage für die Eingabekontrolle der Systeme geschaffen, die personenbezogenen Daten verarbeiten. Grundsätzlich wird im Rechte- und Rollen-Konzept zwischen Systemusern, Prozessusern und personalisierten Usern unterschieden. Angaben Zur Protokollierung sind in Kapitel 4.2.2 zu finden.

Protokollauswertungen werden stichprobenartig von den Systemadministratoren vorgenommen, insbesondere jedoch, wenn Auffälligkeiten oder der Verdacht auf eine Kompromittierung, z.B. durch eine Alarmierung/Triggering eines Events aufgetreten ist. Die Protokollauswertungen werden nur innerhalb von Gerst ITS verwendet.

# 6. Auftragskontrolle

Alle Weisungen des Auftraggebers zum Umgang mit personenbezogenen Daten werden dokumentiert und an zentraler Stelle für die mit der Datenverarbeitung bei Gerst ITS hinterlegt.

Gerst ITS verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen, siehe Anlage 2. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung erfolgt nur nach schriftlicher Einwilligung des Auftraggebers. Der Auftraggeber hat das jederzeitige Recht, nach Absprache die Umsetzung seiner Weisungen bei Gerst ITS zu kontrollieren. Gerst ITS wird den Auftraggeber bei der Durchführung von Kontrollen durch den Auftraggeber unterstützen und an der vollständigen Abwicklung der Kontrolle mitwirken.

Gerst ITS wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach ihrer Auffassung gegen gesetzliche Regelungen verstößt, sowie dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers unverzüglich mitzuteilen, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschfätigten Personen erfolgt ist.

Gerst ITS ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung des Datengeheimnisses im Sinne des §5 BDSG verpflichtet. Gerst ITS verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien werden erst nach vorheriger Zustimmung durch den Auftraggeber datenschutzgerecht vernichtet.

# 7. Verfügbarkeitskontrolle

Alle Dienste von Gerst ITS sind hochsensibel in Bezug auf deren Verfügbarkeit und müssen vor zufälliger Zerstörung oder Verlust geschützt werden. Die Kunden erwarten eine hochverfügbare Bereitstellung aller Netzwerk- und Rechenzentrumsdienstleistungen. In diesem Zusammenhang werden Maßnahmen zur Datensicherung und -erhaltung umgesetzt. Hierzu verwenden wir für die Auswahl des Rechenzentrums nur Unternehmen deren Rechenzentren mindestens Tier-3-Rechenzentrum und ISO-27001 klassifiziert sind.

## 7.1. Organisatorische Maßnahmen

### 7.1.1. Backup-Verfahren

Alle Systeme werden in regelmäßigen Abständen mittels Datensicherung und DisasterRecovery Backup gesichert, wobei die Sicherung auf einem separaten System als das zu sichernde System verwahrt wird. Die Backups verlassen jedoch nicht das Rechenzentrum von Gerst ITS. Zum Schutz der Archive und Backups sind die zuvor genannten Zutrittskontrollen implementiert. Der Zugang auf die Backupsoftware ist limitiert auf dedizierte Administratoren. Die Häufigkeit von Datenbackups richtet sich nach der Kritikalität der Informationen und ist individuell anpassbar.

Funktionalitätstests von Datenbackups werden stichprobenartig von den zuständigen Systemadministratoren vorgenommen. Die zum Backup benutzten Speichermedien werden nach einem sicheren Lösch- oder Überschreibungsverfahren wiederverwendet.

Der Wiederherstellungsprozess erfolgt nach Kritikalität der einzelnen Systeme. Alle Prozesse zur Wiederherstellung der Daten, der Wiederanlauf des Systems, sowie die Notfallsituation müssen in regelmäßigen Abständen in einer Übung durchgeführt und getestet werden. Die bei Notfällen und Incidents benötigten Eskalationspfade wurden im Praxisbetrieb erprobt.

## 7.2. Technische Maßnahmen

### 7.2.1. Firewall und Virenschutz

Die Netze und Systeme von Gerst ITS sind mit einer Firewall gegen Hackerangriffe geschützt, die regelmäßig von autorisierten Systemadministratoren gewartet und aktualisiert werden. Die Firewall- Regeln sind so ausgelegt, dass nur benötigte Dienste erlaubt sind und in der Grundeinstellung jeden Netzwerkverkehr blockieren. Alle Internetverbindungen

sind durch mindestens eine Firewall geschützt. Die Kontrolle sicherheitsrelevanter Konfigurationen erfolgt hierbei im Rahmen von Penetrationstests, die u.a. von der internen Sicherheitsabteilung des Rechenzentrums durchgeführt wird, Alle Netzwerkkomponenten werden einmal täglich, sowohl intern als auch extern, durch automatische Scanner geprüft.

Das Virenschutzkonzept sieht einen mehrstufigen Schutz vor Schadstoffsoftware über die Netzwerk-Gateways und Systeme von Gerst ITS vor. Der Schutz vor Schadstoffsoftware wird regelmäßig, mindestens einmal am Tag, aktualisiert. Alle Systeme sind mit einem fehlertoleranten Festplattenverbund (i.d.R. RAID 5, mindestens jedoch RAID 1) ausgestattet.

### 7.2.2. Hochverfügbarkeit und Stromversorgung

Aus der Hochverfügbarkeitsanforderung ergibt sich am Standort Offenbach am Main, an dem die Systeme aufgestellt sind, eine grundsätzliche hochredundant ausgelegte Netzwerkinfrastruktur, die Einzelfehler in fast allen Bereichen und Doppelfehler in vielen Bereichen abfangen kann. Die Stromversorgungen sind mehrfach unabhängig voneinander ausgelegt. Das Rechenzentrum ist mit einer unterbrechungsfreien Stromzufuhr und einem Notstromaggregat ausgestattet.

### 7.2.3. Brandschutz

Eine Löschanlage schützt die Sicherheitsräume im Brandfall. Die Server werden durch den Löschvorgang nicht beeintrachtigt und können normal weiter betrieben werden. Im Rechenzentrum sind Brandmelder installiert. Die Brandschutzsysteme unterliegen ständigen Kontrollen und werden durch den Betreibers des Rechenzentrums durchgeführt.

## 8. Trennungskontrolle

Durch die getroffenen Maßnahmen zur Trennungskontrolle sind der softwareseitige Ausschluss im Sinne einer Mandantentrennung, die Trennung von Test- und Routineprogrammen, die Trennung durch getroffene Zugriffs-regelungen, sowie Dateiseparierung.

Beispielsweise müssen alle Produktivsysteme getrennt von den Entwicklungs- und Testsystemen betrieben werden. Technisch wird das durch eine Segmentierung von Netzen mit einem aktivierten Firewall-Regelwerk, sowie gesonderte Testinstanzen und -systemen realisiert. Produktivdaten dürfen nicht als Kopie für Testzwecke verwendet werden, ebenso dürfen Testdaten nicht in Produktivumgebung eingesetzt werden.