
| | | |
|---|---|---|
| **Titel:** | **TOMs** | |
| **Thema:** | **Technische und organisatorische Maßnahmen nach DSGVO** | |
| **Versionsnummer / Datum** | 1.0 | 05.05.2018 |
| **Verfasser / Co-Verfasser:** | DI Gerald KORTSCHAK | Andreas SENGER |
| **Zielgruppe:** | Fotografen | |

1 Präambel ..... 2
1.1 Erläuterung ..... 2
2 Begriffsdefinition TOM ..... 2
2.1 Stand der Technik ..... 4
3 Listung der bisher identifizierten TOMs ..... 5
4 Praxis-Beispiel ..... 9
5 Gruppe der Betroffenen ..... 11
6 Anhang – Auszüge der Art 32 DSGVO, § 54 DS-Anpassungsgesetz ..... 12
6.1 Art. 32 DSGVO – Sicherheit der Verarbeitung (Zitat): ..... 12
6.2 § 54 Datenschutz-Anpassungsgesetz 2018 (Zitat) ..... 13

**sevian7 IT development GmbH**
**Triesterstrasse 136**
**8020 Graz**
**www.sevian7.com / office@sevian7.com**

# 1 Präambel

Das gegenständliche Dokument enthält die Erstresultate der technischen und organisatorischen Maßnahmen im Zusammenhang mit der DSGVO.
Dieses Dokument ist ergänzend zu den Inhalten die im 001_Verfahrensverzeichnis angeführt sind.

## 1.1 Erläuterung

Gegenständliches Dokument stellt keine Rechtsberatung dar und stellt die Sichtweise der Unternehmensberatung zur Thematik dar.

# 2 Begriffsdefinition TOM

Art. 32 der DSGVO beinhaltet die technischen und organisatorischen Maßnahmen (TOM) die zur **Wahrung der** Sicherheit von Verarbeitungen zu ergreifen sind. Der § 54 Datenschutz-Anpassungsgesetz 2018 führt diese weiter aus.

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

- •die **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten;
- •die Fähigkeit, die **Vertraulichkeit, Integrität, Verfügbarkeit** und **Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- •die Fähigkeit, die **Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen** bei einem physischen oder technischen Zwischenfall **rasch wiederherzustellen**;
- •ein Verfahren zur **regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit** der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Eine nähere „Definition“ findet sich im § 54 Datenschutz-Anpassungsgesetz. Verkürzt definiert dieser wie folgt:

**sevian7 IT development GmbH**
**Triesterstrasse 136**
**8020 Graz**
**www.sevian7.com / office@sevian7.com**

| Maßnahme | Beschreibung |
|---|---|
| **Zugangskontrolle** | Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle) |
| **Datenträgerkontrolle** | Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern (Datenträgerkontrolle) |
| **Speicherkontrolle** | Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten |
| **Benutzerkontrolle** | Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle) |
| **Zugriffskontrolle** | Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben (Zugriffskontrolle) |
| **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 (Übertragungskontrolle) |
| **Eingabekontrolle** | Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind (Eingabekontrolle) |
| **Transportkontrolle** | Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle) |
| **Wiederherstellung** | Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellung) |
| **stabiles System / 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 (Datenintegrität). |

## 2.1 Stand der Technik

Der Begriff Stand der Technik ist in der Gewerbeordnung allgemein geregelt.

*§71 a GewO 1994*

*(1) Der Stand der Technik (beste verfügbare Techniken – BVT) im Sinne dieses Bundesgesetzes ist der auf den einschlägigen wissenschaftlichen Erkenntnissen beruhende Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen, Bau- oder Betriebsweisen, deren Funktionstüchtigkeit erprobt und erwiesen ist. Bei der Bestimmung des Standes der Technik sind insbesondere jene vergleichbaren Verfahren, Einrichtungen Bau- oder Betriebsweisen heranzuziehen, welche am wirksamsten zur Erreichung eines allgemein hohen Schutzniveaus für die Umwelt insgesamt sind; weiters sind unter Beachtung der sich aus einer bestimmten Maßnahme ergebenden Kosten und ihres Nutzens und des Grundsatzes der Vorsorge und der Vorbeugung im Allgemeinen wie auch im Einzelfall die Kriterien der Anlage 6 zu diesem Bundesgesetz zu berücksichtigen.*

**sevian7 IT development GmbH**
**Triesterstrasse 136**
**8020 Graz**
**www.sevian7.com / office@sevian7.com**

# 3 Listung der bisher identifizierten TOMs

Die Maßnahmen sind immer nach dem Risiko und der Wirtschaftlichkeit zu bewerten und können daher von Unternehmen zu Unternehmen unterschiedlich sein. Es wird noch eine kleine Checkliste als Hilfestellung geben, anhand der eine grundsätzliche „Notwendigkeit“ einer Maßnahme beurteilt oder erkannt werden kann. Beispiel (Werte im Beispiel fiktiv): *Ein USB-Stick mit PIN-Eingabe kostet € 140,-- bto, personenbezogene Daten werden per USB-Stick ausgetauscht und darauf sind sensible Daten (Art. 9), ein Verlust verursacht einen Schaden von € 10.000,-- => Wirtschaflichkeit der Anschaffung ist wohl gegeben.*

| Maßnahme | technisch | organisatorisch |
|---|---|---|
| **Zugangsk.** | • Physischer Zutritt zum Objekt<br>• Alarmanlage<br>• Nach Notwendigkeit „Videoüberwachung“<br>• Absicherung des Zutrittes zu Räumlichkeiten mit personenbezogenen Daten<br>• Protokollierung des Zutrittes zu abgesicherten Räumlichkeiten<br>• Versperrmöglichkeiten für Ordner, Datenträger, Notebooks<br>• Firewall-Systeme | • Regelung des Zutrittes zu Räumen mit pers. Daten insbesonders für Fremdpersonal.<br>• Regelung zur Versperrung des Objektes<br>• Regelung zur Versperrung von Datenträgern (Ordner etc.) |
| **Datenträgerk.** | • Berechtigungssystem der Benutzer von digitalen Systemen (Lese, -Schreibrechte regeln)<br>• Anschluss von USB-Sticks technisch „kontrollieren“<br>• Bei „hohem“ Risiko sind entsprechende technische Lösungen grundsätzlich einzuführen, die Anschluss und Entfernung kontrollieren bzw. verhindern.<br>• techn. Verschlüsselung der Datenträger | • Mitnahme von USB-Sticks/Festplatten durch unbefugte regeln.<br>• Private USB-Sticks/Festplatten im Unternehmen regeln<br>• Private Speicherung von Daten auf Notebooks, Smartphones, Tablets regeln.<br>• Sichere Vernichtung von Datenträgern (Aktenvernichter, Festplatten, Geräte mit Speicher sicher entsorgen) |

**sevian7 IT development GmbH**
**Triesterstrasse 136**
**8020 Graz**
**www.sevian7.com / office@sevian7.com**

| | | |
|---|---|---|
| **Speicherk.** | • Eingabe-Kontrolle in Programmen – Veränderungskontrolle, Löschkontrolle<br>• Berechtigungsmanagement in Anwendungen und Systemen<br>• Protokollierung und Dokumentation von Veränderungen um eine Kontrollmöglichkeit sicher zu stellen.<br>• Antivirenlösungen (keine gratis Produkte) | • Regelung zur Eingabe von Daten, Kontrolle der gespeicherten Daten.<br>• Regelung der Frage „Wer darf in einem Ordner mit pers. Daten Änderungen ausführen?“ |
| **Benutzerk.** | • Benutzername und Kennwort für alle Systeme mit digitaler Verarbeitung von personenbezogenen Daten einführen (zB nicht nur für das Anmelden an Arbeitsstationen)<br>• Sicherstellung einer regelmässigen Änderung der Kennwörter<br>• technisch sichere Kennwörter voraussetzen<br>• | • Regelung dass Mitarbeiter nicht aus Bequemlichkeit Kennwörter untereinander tauschen<br>• Sicherstellen, dass es nicht einen Zugriff (Username, Passwort) für mehrere Personen in ein System gibt. |
| **Zugriffsk.** | • Usermanagement (Am Client oder Active Directory am Server)<br>• Je System mit pers. Daten eine Kennwort-Abfrage zur Kontrolle des Zugriffes nach Sicherheitsstufen.<br>• Berechtigungen auf Dateifreigaben (Berechtigungsmatrix)<br>• Applikationen die Daten an Dritte automatisiert synchronisieren prüfen oder ersetzen (zB WhatsApp durch Signal) | • Regelung, dass nur berechtigte Zugriff zu den pers. Daten haben.<br>• Regelung wie Dienstleister auf Daten zugreifen. (zB per Fernwartung)<br>• |

| | | |
|---|---|---|
| **Übertragungsk.** | • Kontrolle der Übertragungen per Mail (zB Protokolle am Server oder Übermittlung an eine eigene „Kontroll-eMail-Adresse“ in Kopie)<br>• (Vorbild Faxprotokoll) | • Regelung der Dokumentation von postalischen Übertragungen<br>• Dokumentation und Kontrolle persönlicher Datenabholungen |
| **Eingabek.** | • Eingabekontrolle in Systemen – Protokollierung von Veränderungen und Eingaben im System (wer hat wann zuletzt)<br>• die techn. Lösung hierzu ist für die meisten Unternehmen wirtschaftlich nicht sinnvoll, wenn es nicht von Seiten des Software-Anbieters integriert ist. | • Veränderungsprotokoll in Papierablagen (zB Ordner-Deckblatt wer zuletzt welche Änderung durchgeführt hat)<br>• Bei Dateien kann dies im Dokument direkt eingetragen werden oder in einem separaten Dokument zur Datei protokolliert werden |
| **Transportk.** | • Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle)<br>• Einführung verschlüsselter USB-Sticks (zB mit PIN-Eingabe-Feld)<br>• Einführung von Passwort-geschützten Dokumenten (zB PDF mit Kennwort durch Adobe Acrobat) | • Verschwiegenheitsvereinbarungen mit Dienstleistern (auch Handwerk und Putzdienste mit Zugang zu Räumen in denen pers. Daten aufbewahrt werden regeln. zB Ein Ordner wird in einem Raum verwahrt, nicht separat versperrt, da Mitarbeiter diesen Raum beim Verlassen zusperren. Putzdienste oder Handwerker halten sich jedoch unkontrolliert in diesem Raum auf)<br>• Vertragl. Vereinbarung mit allen techn. Dienstleistern mit Fernwartungs- oder VorOrt Zugriff (zB Teamviewer)<br>• Regelung der Datenweitergabe an Dritte (Buchhaltung, Gemeinden, ...) |

| | | |
|---|---|---|
| **Wiederherstellung** | • techn. Backup-Konzept realisieren<br>• RAID (gespiegelte Festplatten) ist KEIN Backup<br>• Je nach Bedarf und Menge mit externen Festplatten, Netzwerk-Festplattensystemen (NAS), Bandlaufwerken, Online-Backup-Diensten odgl. vom techn. Dienstleister umsetzen lassen.<br>• techn. Lösung um IT-Systeme rasch wieder her zu stellen (zB Reserve-Smartphone, Notebooks die Aufgaben von StandPCs vorübergehend übernehmen können, Regelung bezüglich Austauschhardware am Server)<br>• Virtualisierung von Server-Systemen<br>• Kosten-Nutzen-Rechnung einer Lösung im Rechenzentrum<br>• techn. Überprüfung des Backup-Konzeptes mit Protokoll einführen<br>• techn. Prüfung lokaler Daten – Ist das Backup „vollständig“? | • Erstellung eines Backup-Konzeptes für Offline- und Online-Datenträger<br>• zB Papierordner kopieren, scannen und gesondert lagern<br>• Regelung in welchem Intervall eine Datensicherung erforderlich ist, um das System wieder her zu stellen.<br>• Prüfung der Regelung des externen Dienstleisters, wenn Systeme in einem Rechenzentrum stehen<br>• Faustregel 1: Eine Datei, eine E-Mail oder ein Dokument ist nicht mehr verfügbar, wird aber benötigt. Was ist die maximale Wartezeit, bis diese Datei wieder hergestellt ist, ohne wirtschaftlichen Schaden zu erleiden?<br>• Faustregel 2: Wenn ein ganzes System (zB E-Mail, , ...) nicht verfügbar ist, wie lange kann mein Betrieb ohne wirtschaftl. Schaden fortgeführt werden.<br>• Faustregel 3: Wenn meine gesamte IT (zB Server durch Verschlüsselungstrojaner) nicht mehr funktioniert, wie lange kann ich ohne diese Informationen arbeiten? (Tipp: Nutzen Sie und jeder Mitarbeiter für 1h keinen einzigen Rechner in Ihrem Unternehmen. Welche Probleme treten auf? Wie wäre dieser Zustand für 8, 16, 24 Stunden?<br>• Wenn Daten gm. „Recht auf Vergessen“ gelöscht wurden, Klärung ob Löschung im Backup möglich bzw. Verhinderung, dass bei Wiederherstellung diese Daten auch wiederhergestellt werden. |

**sevian7 IT development GmbH**
**Triesterstrasse 136**
**8020 Graz**
**www.sevian7.com / office@sevian7.com**

| | | |
|---|---|---|
| **stabiles System / Datenintegrität** | • Antiviren-Lösung<br>• Redundanzen für Strom (USV – Unabhängige Strom Versorgung), Festplatten, neuralgische Hardware<br>• Monitoring (techn. Überwachung) der Systeme um Ausfälle zu erkennen.<br>• Protokollierungen an Servern, Firewall etc. einführen und Warnsysteme (so vorhanden) aktivieren | • Vereinbarung mit Dienstleister „Konfiguration am Stand der Technik“<br>• Organisatorische Regelung der regelmäßigen Überprüfung von Redundanzen (Wie alt ist die USV? Wie lange hält sie die Stromversorgung aufrecht? Welche Systeme sind damit Verbunden?) |

Für sämtliche organisatorischen Maßnahmen gilt, dass eine nachweisliche Schulung und Einweisung der Mitarbeiter sowie schriftliche Vereinbarungen mit Dienstleistern als ganzheitliche organisatorische Maßnahme zu sehen sind, die es auszuführen gilt. Insbesonders sind Schulungen nicht durch Formulare mit Bestätigung oder durch zB Nebenverträge zum Dienstvertrag alleine zu regeln.

# 4 Praxis-Beispiel

- Einführung einer Firewall, um Fremdzugriffe von außen zu verhindern.
- Einführung eines NAS (Netzwerkfestplatten) die eine Sicherung der Daten mit Backupsoftware durchführt, löst bisherige Lösung gespiegelter Festplatten ab.
- USB-Sticks nur mehr mit PIN-Eingabe für den Transport sensibler Dateien
- Nutzung des E-Zustellungsdienstes der Post für einen gesicherten Datentransfer
- Schutz von Dokumenten (zB PDF) mit Kennwort, wenn diese per Mail übertragen werden.
- Regelung der Nutzung von WhatsApp am Firmentelefon (ablösen durch Signal)
- MitarbeiterInnen die Nutzung von WhatsApp für dienstliche Zwecke (Aufnahme von Bildern und Übermittlung in die Firma) „verbieten“ bzw. schulen, sensibilisieren und kontrollieren.
- MitarbeiterInnen kennen nicht mehr das Passwort der Chefetage
- Aktenvernichter wird zur Vernichtung von Dokumenten angeschafft
- Regelung der Verschwiegenheit und des vertraulichen Datenumganges mit Dienstleistern (IT, Wartungsverträge von Software, Handwerk, ...)
- Vergabe von neuen Passwörtern (12 34 56, qwertz, ... sind keine Kennwörter)
- Benutzerberechtigung auf Arbeitsstationen oder über einen Server steuern.
- Einführung eines kleinen Server-Systems (vor Ort oder Rechenzentrum) damit nicht alle Daten zentral auf einem Rechner liegen, der gleichzeitig eine Arbeitsstation ist.

**sevian7 IT development GmbH**
**Triesterstrasse 136**
**8020 Graz**
**www.sevian7.com / office@sevian7.com**

- Prüfen der USV, wie lange das dahinter liegende System wirklich noch mit Strom versorgt wird.
- Testen der eigenen Wiederherstellungsroutinen (Wie lange ohne IT? Welcher Aufwand muss betrieben werden, wenn die IT wieder da ist? zB nachträgliche Eingabe von Dokumenten, Terminen, Telefonaten, Routen, etc.)

**sevian7 IT development GmbH**
**Triesterstrasse 136**
**8020 Graz**
**www.sevian7.com / office@sevian7.com**

# 5 Gruppe der Betroffenen

Für die Bestimmung der Maßnahmen ist es erforderlich Kategorien der „Betroffenen“ in einem Unternehmen zu definieren.
Betroffene sind grundsätzlich alle Kunden und Mitarbeiter von denen personenbezogene Daten (Vorname, Nachname, ...) verarbeitet werden, beispielsweise für die Rechnungslegung. Dies gilt auch für personenbezogene Daten über den Geschäftsführer einer juristischen Person (zB. Vorname, Nachname, Geburtsdatum des Geschäftsführers einer GmbH).

Folgende Kategorien von Betroffenen wurden generell identifiziert:

**sevian7 IT development GmbH**
**Triesterstrasse 136**
**8020 Graz**
**www.sevian7.com / office@sevian7.com**

# 6 Anhang – Auszüge der Art 32 DSGVO, § 54 DS-Anpassungsgesetz

Nachstehend die Auszüge direkt zitiert aus RIS.BKA.GV.AT

## 6.1 Art. 32 DSGVO – Sicherheit der Verarbeitung (Zitat):

*(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:*

*a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;*

*b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;*

*c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;*

*d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.*

*(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.*

*(3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.*

*(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.*

**sevian7 IT development GmbH**
**Triesterstrasse 136**
**8020 Graz**
**www.sevian7.com / office@sevian7.com**

## 6.2 § 54 Datenschutz-Anpassungsgesetz 2018 (Zitat)

*(1) Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, unter Berücksichtigung der unterschiedlichen Kategorien gemäß § 37, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß § 39.*

*(2) Der Verantwortliche und der Auftragsverarbeiter haben im Hinblick auf die automatisierte Verarbeitung nach einer Risikobewertung Maßnahmen zu ergreifen, um folgende Zwecke zu erreichen:*

*Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle);*

*Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern (Datenträgerkontrolle);*

*Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle);*

*Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle);*

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

*6.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 (Übertragungskontrolle);*

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

**sevian7 IT development GmbH**
**Triesterstrasse 136**
**8020 Graz**
**www.sevian7.com / office@sevian7.com**

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

*Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellung);*

*10.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 (Datenintegrität).*