**Verzeichnis**

**der technischen und organisatorischen Maßnahmen
nach Artikel 32 Datenschutz-Grundverordnung**

**(im Weiteren: DS-GVO)**

Nachfolgend werden die technischen und organisatorischen Maßnahmen (TOM) aufgelistet, die seitens des Verantwortlichen ergriffen worden sind, um die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten.

|  |
| --- |
| **A. Vertraulichkeit** |

1. **Zutrittskontrolle**

Maßnahmen, die gewährleisten, dass Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, verwehrt wird:

|  |  |  |
| --- | --- | --- |
| 1.1. | Alarmanlage | * Eingangsbereich
* …
 |
| 1.3. | Schließsystem | * Sicherheitsschlösser
* …
 |
| 1.4. | räumliche Abgrenzungen  | * Technikraum
* Arbeitszimmer
* …
 |
| 1.5. | Anwesenheitskontrolle | * Zeiterfassungssystem
* Protokollierung
* …..
 |

1. **Zugangskontrolle**

 Maßnahmen, die gewährleisten, dass Unbefugten die Nutzung von Datenverarbeitungssystemen, mit denen personenbezogene Daten verarbeitet werden, verwehrt wird:

|  |  |  |
| --- | --- | --- |
| 2.1. | Zugriffs-, Berechtigungs- und Rechtekonzept | * persönlicher und individueller User-Log-In
* Passwortrichtlinie
* Einrichtung mehrerer Benutzergruppen mit differenzierten Zugriffsrechten
* …
 |
| 2.2. | sichere Hard- und Software | * regelmäßige Anpassung an den aktuellen Stand der Technik/aktuelle Versionen der Software
* …
 |
| 2.3. | IT-Sicherheitsmaßnahmen | * Sperren von externen Schnittstellen (z. B. USB)
* Bildschirmsperren mit Passwortaktivierung
* Abschluss von Auftragsverarbeitungsverträgen
* …
 |

1. **Zugriffskontrolle**

 Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten nicht unbefugt verarbeitet werden:

|  |  |  |
| --- | --- | --- |
| 3.1. | Zugriffs-, Berechtigungs- und Rechtekonzept | * Einrichtung mehrerer Benutzergruppen mit differenzierten Zugriffsrechten
* Verwaltung der Rechte durch Systemadministrator
* Verschlüsselung von externen Datenträgern
* Zugriffsbeschränkungen durch:
	+ verschließbare Aktenschränke
	+ verschließbare Datentonnen
* …
 |
| 3.2. | Datenvernichtung | * datenschutzkonforme Löschung von Datenträgern vor Wiederverwendung
* Einsatz von Dienstleistern zur datenschutzkonformen Vernichtung von Datenträgern
* …
 |

|  |
| --- |
| **B. Integrität** |

1. **Weitergabekontrolle**

 Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übermittlung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt verarbeitet werden können und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

|  |  |  |
| --- | --- | --- |
| 1.1. | Übermittlungssicherheit | * Einsatz von VPN-Technologie
* Protokollierung von Datentransport
* Verschlüsselung von Datenträgern
* gesicherter Datentransport (z. B. SSL)
* …
 |
| 1.2. | nutzerbasierte Protokollierung der Verarbeitung | * von regelmäßigen Abruf- und Übermittlungsvorgängen
* …
 |

1. **Eingabekontrolle**

 Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen verarbeitet wurden:

|  |  |  |
| --- | --- | --- |
| 2.1. | Zugriffs-, Berechtigungs- und Rechtekonzept | * Erteilung von Zugangsberechtigungen durch mehrstufiges Freigabeverfahren
* Verwaltung der Rechte durch Systemadministrator
* Mehraugenprinzip
* …
 |
| 2.2. | nutzerbasierte Protokollierung der Verarbeitung | * der Eingabe, Änderung und Löschung von Daten
 |

1. **Kontrolle der Auftragsverarbeiter**

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Der Auftraggeber hat den Auftragsverarbeiter unter den folgenden Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) auszuwählen und zu beauftragen:

|  |  |  |
| --- | --- | --- |
| 3.1. | Geeignetheits- und Zuverlässigkeitsprüfung  | * datenschutzkonforme, insbesondere den Anforderungen des Art. 28 DS-GVO entsprechende Verarbeitung
* Verarbeitung nur innerhalb der EU
* …
 |
| 3.2. | Protokollierung | * des Auswahlverfahrens und der Vertragsgestaltung
 |

|  |
| --- |
| **C. Verfügbarkeit / Belastbarkeit** |

1. **Verfügbarkeitskontrolle**

Maßnahmen, die gewährleisten, dass personenbezogene Daten vor zufälliger Zerstörung oder Verlust geschützt sind:

|  |  |  |
| --- | --- | --- |
| 1.1. | Havarieschutz  | * unterbrechungsfreie Stromversorgung
* Feuer- und Rauchmeldeanlagen
* Rauchverbot im Gebäude
* …
 |
| 1.2. | Backup- und Recovery-System | * Backup- & Recovery-Konzept
* Testen der Datenwiederherstellung
* Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
* …
 |

1. **Trennungskontrolle**

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

|  |  |  |
| --- | --- | --- |
| 2.1. | Zugriffs-, Berechtigungs- und Rechtekonzept | * Erteilung von Zugangsberechtigungen durch mehrstufiges Freigabeverfahren
* Verwaltung der Rechte durch Systemadministrator
* verschließbare Aktenschränke
* …
 |
| 2.2. | Trennungsprinzip und Zweckzuordnung | * Trennung von Produktiv- und Testsystemen
 |

|  |
| --- |
| **D. Organisationskontrolle** |

Maßnahmen, die gewährleisten, dass die vorgenannten technischen und organisatorischen Maßnahmen eingehalten und regelmäßig evaluiert werden.

|  |  |  |
| --- | --- | --- |
| 1.1. | Datenschutzkonzept | * Konzept zur Überwachung und regelmäßigen Evaluierung
 |
| 1.2. | Fachbeauftragte | * Datenschutzbeauftragter
 |