

AVV - Anlage 2 – Technische und organisatorische Maßnahmen des Auftragsverarbeiters nach Art. 32 DSGVO

Der Auftragsverarbeiter setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt und mit dem Auftraggeber abgestimmt.

1. Zweckbindung und Trennbarkeit

Folgende Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- Separierung von Datenbanken und logische Zweck- und Mandantentrennung
- Versehen der Datensätze mit Zweckattributen und Kontrolle der Zweckbindung

2. Zutrittskontrolle

Folgende Maßnahmen gewährleisten, dass Unbefugte am Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, gehindert werden:

- Manuelles Schließsystem und Schlüsselregelungen

3. Zugangskontrolle

Folgende Maßnahmen gewährleisten, dass Unbefugte die Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, nicht nutzen können:

- Kennwortverfahren (u.a. mit Sonderzeichen, Mindestlänge und regelmäßigem Wechsel)
- Anti-Viren-Software

4. Zugriffskontrolle

Folgende Maßnahmen gewährleisten, dass ausschließlich Berechtigte auf die Daten zugreifen und diese lesen, kopieren, verändern oder entfernen können:

- Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte (Profile, Rollen und Verwaltung der Rechte durch Systemadministrator), die auf das „Notwendigste“ reduziert sind.
- Regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte
- Benutzererkennung mit Passwort und Kennwortverfahren (u.a. mit Sonderzeichen, Mindestlänge und regelmäßigem Wechsel)

5. Eingabekontrolle

Mit Hilfe folgender Maßnahmen kann nachträglich überprüft und festgestellt werden, ob und wer personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt hat:

- Plausibilitätskontrollen und Sicherung von Daten gegen Verlust und Veränderung

6. Weitergabekontrolle:

Folgende Maßnahmen gewährleisten, dass Unbefugte bei der Weitergaben von personenbezogenen Daten keinen Zugriff darauf bekommen:

- Prüfung der Rechtmäßigkeit der Weitergabe von Dritten
- Weitergabe an Dritte in anonymisierter oder pseudonymisierter Form
- Verschlüsselung der Kommunikationswege und physischer Datenträger beim Transport

7. Auftragskontrolle

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

- Auswahl des Auftragsverarbeiters unter Sorgfaltsgesichtspunkten, schriftliche Weisung an den Auftragsverarbeiter in Form von Auftragsverarbeitungsverträgen

8. Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit der Systeme

Folgende Maßnahmen gewährleisten, dass die eingesetzten Datenverarbeitungssysteme einwandfrei funktionieren und personenbezogene Daten gegen zufällige Zerstörung und Verlust geschützt sind:

- Backup-Strategie (online und offline) und getrennte Aufbewahrung
- Virenschutz und Firewall

9. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen:

Der Auftragsverarbeiter wird die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen regelmäßig und anlassbezogen prüfen, evaluieren und bei Bedarf anpassen um eine unter Berücksichtigung des aktuellen Standes der Technik, angemessener Implementierungs und Wartungskosten sowie der Art, des Umfangs und der Zwecke der Verarbeitung, bestmögliche Eignung der Maßnahmen zum Schutz der personenbezogenen Daten zu gewährleisten.