Vereinbarung zur Auftragsverarbeitung (ADV) – Anlage II

Nach Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO).

Stand des Dokumentes 14.05.2021

Wir Aktualisierungen die Inhalte der Anhänge laufend bzw. mind. Jährlich bei entsprechenden Änderungen. Sie können die neuen aktualisierten Anhänge von unserer Webseite laden, und ihrem bereits unterzeichneten ADV-Vertrag hinzufügen.

Technische und Organisatorische Sicherheitsmaßnahmen gemäß Art 32 DSGVO

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu Räumen zu verwehren, in denen Datenverarbeitungsanlagen untergebracht sind. Festlegung von Sicherheitsbereichen

- Realisierung eines Zutrittsschutzes
- Protokollierung des Zutritts
- Begleitung von Fremdpersonal
- Überwachung der Räume
- Festlegung Zutrittsberechtigter Personen
- Verwaltung von individuellen personengebundenen Zutrittsberechtigungen Dieser Punkt wird von unseren externen Dienstleistern erfüllt bzw. erbracht. Nach Vertragskontrolle hat die Götz & Oberhauser IT GbR sichergestellt, dass dies durchgeführt wird. (Anhang 1).

1.2 Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden.

- Zugangsschutz
- Monitoring bei kritischen IT-Systemen
- Meldung bei hoher Anzahl an Fehlversuchen
- Verbot Speicherfunktion für Passwörter und/oder Formulareingaben (Server/Clients)
- Festlegung befugter Personen
- Umsetzung sicherer Zugangsverfahren, starke Authentisierung
- Umsetzung einfacher Authentisierung per Username Passwort
- Protokollierung des Zugangs
- Verwaltung von personengebundenen Authentifizierungsmedien und Zugangsberechtigungen
- Automatische Zugangssperre und Manuelle Zugangssperre

1.3 Zugriffskontrolle

Es kann nur auf die Daten zugegriffen, für die eine Zugriffsberechtigung besteht. Daten können bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

- Erstellen eines Berechtigungskonzepts
- Verwaltung von personengebundenen Zugriffsberechtigungen
- Vermeidung der Konzentration von Funktionen
- Umsetzung von Zugriffsbeschränkungen
- Vergabe minimaler Berechtigungen

1.4 Verwendungszweckkontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Datensparsamkeit im Umgang mit personenbezogenen Daten
- Getrennte Verarbeitung verschiedener Datensätze
- Regelmäßige Verwendungszweckkontrolle und Löschung
- Trennung von Test- und Entwicklungsumgebung

1.5 datenschutzfreundliche Voreinstellungen

- Sofern Daten zur Erreichung des Verwendungszwecks nicht erforderlich sind, werden die technischen Voreinstellungen so festgelegt, dass Daten nur durch eine Aktion der Betroffenen Person erhoben, verarbeitet, weitergegeben oder veröffentlicht werden.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle Ziel der Weitergabekontrolle ist es, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Festlegung empfangs- /weitergabeberechtigter Instanzen/Personen
- Prüfung der Rechtmäßigkeit der Übermittlung ins Ausland
- Protokollierung von Übermittlungen gemäß Protokollierungskonzept
- Sichere Ablage von Daten, inkl. Backups
- Gesicherte Speicherung auf mobilen Datenträgern
- Sichere Übertragung zu externen Systemen
- Risikominimierung durch Netzseparierung
- Einführung eines Prozesses zur Datenträgerverwaltungen
- Prozess zur Sammlung und Entsorgung
- Sichere Datenübertragung zwischen Server und Client
- Sicherung der Übertragung im Backend
- Implementation von Sicherheitsgateways an den Netzübergabepunkten
- Datenschutzgerechter Lösch- und Zerstörungsverfahren
- Führung von Löschprotokollen

2.2 Eingabekontrolle

Zweck der Eingabekontrolle ist es, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Protokollierung der Eingaben
- Dokumentation der Eingabeberechtigungen

3. Verfügbarkeit, Belastbarkeit, Desaster Recovery
3.1 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)
• Brandschutz
• Redundanz der Primärtechnik
• Redundanz der Stromversorgung
• Redundanz der Kommunikationsverbindungen
• Monitoring
• Resourcenplanung und Bereitstellung
• Abwehr von systembelastendem Missbrauch
• Datensicherungskonzepte und Umsetzung
• Regelmäßige Prüfung der Notfalleinrichtungen Die Umsetzung der Hardware und Rechenzentren-Redundanz (wie Brandschutz, Stromversorgung) wird hierbei von externen Dienstleistern durchgeführt. Nach Vertragskontrolle hat die Götz & Oberhauser IT GbR sichergestellt, dass dies durchgeführt wird. (Anlage 1).

3.2 Desaster Recovery – Rasche Wiederherstellung nach Zwischenfall Zwischenfall (Art. 32 Abs. 1 lit. c DSGVO)
• Notfallplan
• Datensicherungskonzepte und Umsetzung

4. Datenschutzorganisation
• Festlegung von Verantwortlichkeiten
• Umsetzung und Kontrolle geeigneter Prozesse
• Melde- und Freigabeprozess
• Umsetzung von Schulungsmaßnahmen
• Verpflichtung auf Vertraulichkeit
• Regelungen zur internen Aufgabenverteilung
• Beachtung von Funktionstrennung und –zuordnung
• Einführung einer geeigneten Vertreterregelung

5. Auftragskontrolle
Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.
• Auswahl weiterer Auftragnehmer nach geeigneten Garantien
• Abschluss einer Vereinbarung zur Auftragsverarbeitung mit weiteren Auftragnehmern
• Abschluss einer Vereinbarung zur Auftragsverarbeitung mit der Götz & Oberhauser IT GbR 6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)
• Prozess zur Evaluation der Technischen und Organisatorischen Maßnahmen
• Prozess Sicherheitsvorfall-Management
• Durchführung von technischen Überprüfungen

[DIESER BEREICH IST ABSICHTLICH FREIGEHALTEN]