Anlage 2 zum Vertrag zur Auftragsverarbeitung: Technische und organisatorische Maßnahmen beim Auftragsverarbeiter

hmd-software AG
Abt-Gregor-Danner-Straße 2
82346 Andechs

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.

---

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DS-GVO)

Zutrittskontrolle
(Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.)

Der Zutritt zu den Gebäuden bzw. Räumlichkeiten der hmd-software AG ist über ein mehrstufiges Sicherheitssystem je nach Bereich getrennt. Zutritt zu den unterschiedlichen Büroräumen, Serveranlagen, Archiven und Backupräumen können nur über bestimmte Sicherheitsfreigaben und Personen durchgeführt werden.

An allen externen Standorten der hmd-software AG befinden sich keine Datenbestände auf den lokalen Datenverarbeitungsanlagen. Der Zugriff der externen Standorte erfolgt über eigene Direktanbindungen und eigens dafür verwendeter Hardware mit der entsprechenden Verschlüsselung.

Die Zutrittskontrolle zu den Servern der hmd-software AG, die in den Rechenzentren der eurodata AG und der S.WERK AG untergebracht sind, sind nur durch ausgesuchte und autorisierte Mitarbeiter der hmd-software AG möglich. Die nötigen Sicherheitskontrollen beim Zugang zum Rechenzentrum werden von den Dienstleistern unter Berücksichtigung der derzeit höchst möglichen Sicherheitsstufen umgesetzt und ausgeführt.

Zugangskontrolle
(Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.)

Der gesamte Bereich von technischen Geräten, die Zugang zu Datenbeständen in den Räumen der hmd-software ag ermöglichen, ist mit personifizierten Schlüsseln zur Autorisierung geschützt. Zugänge zu den verschiedenen Räumen sind über verschiedenen Sicherheitsstufen und unterschiedlichen Autorisierungen an den Geräten mehrfach geschützt.

Externe digitale Zugänge von Mitarbeitern und Standorten werden über mehrstufige Zugangs- und Sicherheitskontrollen im Rahmen der technischen Möglichkeiten permanent durchgeführt. Externe Besucher, Kunden und Interessenten werden durch Personal am Empfang überprüft und eingetragen.

Alle externen digitalen Zugänge, die durch Telekommunikationsanbieter, einen Zugang zum Internet darstellen oder Daten aus dem Internet abrufen oder senden, werden mit entsprechenden Sicherungssystemen permanent mehrstufig auf Schadsoftware oder Kompromitierung der Daten geprüft., bevor diese durch Mitarbeiter der hmd-software AG verarbeitet werden können. Alle mehrstufigen Sicherungssysteme werden permanent von Mitarbeiter der IT geprüft und mit den neuesten Informationen versehen.

Zugriffskontrolle
(Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.)

Alle internen Zugriffsbereiche der hmd-software AG, egal ob es sich um Datenbestände der Entwicklung, von Test, Produktiv oder der internen Organisation handelt, sind strikt getrennt und auf verschiedenen Servern und/oder durch getrennten Benutzerzugriff vor falschem oder versehentlichem Zugriff geschützt. Automatisierte Sicherheitsrichtlinien und netzwerktechnische Grenzsysteme verstärken diese Sicherheitsfunktionen zusätzlich in allen Bereichen.

Der Zugriff auf externe Bereiche, wo Datenbestände in den Rechenzentren der hmd-software AG liegen, werden diese ebenso mit mehrstufigen Sicherheitsberechtigungen geschützt. Dabei werden wir durch technische Sicherheitsmaßnahmen der Rechenzentren unterstützt, um unsere Datenbestände zu schützen und Fremdzugriff zu unterbinden. Dies gilt sowohl für die Produktiv-, als auch für die Testsysteme der hmd-software AG.

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

Sämtliche Datenbestände, die sowohl in den Räumen der hmd-software AG, als auch in beteiligten Rechenzentren verarbeitet werden, sind durch unterschiedliche mehrstufige systemtechnische Abgrenzungen voneinander getrennt. Bei diesen Abgrenzungen handelt es sich sowohl um hardwaretechnische Trennungen, als auch um softwaregesteuerte technische Trennungen der Datenbestände. Dies gilt sowohl für Datenbestände auf Laufwerken, als auch für Datenbestände in Datenbanken.

Berechtigungskonzepte und Zutrittskontrollen zu den technischen Systemen und Datenbeständen, bzw. Lagerstätten, erhöhen die Sicherheit in diesem Bereich.

Pseudonymisierung
(Maßnahmen, die gewährleisten, dass Datenschutzgrundsätze, wie etwa Datenminimierung, wirksam umgesetzt und die notwendigen Garantien in die Verarbeitung aufgenommen werden, um den Anforderungen dieser Verordnung zu genügen.)

Dies trifft für Datenbestände der hmd-software AG nicht zu.

2. Integrität (Art. 32 Abs. 1 lit. b) DS-GVO)

Weitergabekontrolle
(Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung, während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Außerdem, um überprüfen und feststellen zu können, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.)

Alle Datenbestände, die im Rahmen des Austausches von Daten zwischen den lokalen Servern und den angeschlossenen Rechenzentren transportiert werden, werden mit einer derzeit aktuellen Verschlüsselungsmethode unkenntlich gemacht. Diese Methoden werden permanent überprüft, auf Schwachstellen getestet und an die neuesten technischen Möglichkeiten angeglichen, soweit das im Rahmen der finanziellen und organisatorischen Möglichkeiten der hmd-software AG machbar ist.

Werden Datenbestände von weiterführenden Organisationen (Finanzverwaltung, Banken und Sparkassen, Versicherungen, usw.) zur Pflichtweitergabe gefordert, werden diese durch die jeweils von den Organisationen bereitgestellten Schnittstellen und Softwaretechniken verschlüsselt transportiert.

Eine Weitergabe der Daten an Drittstaaten findet nicht statt und ist auch nicht geplant.

Eingabekontrolle
(Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.)

Für alle Datenbestände, die für die Verarbeitung und Speicherung von personenbezogenen Daten in Verbindung stehen, werden alle Maßnahmen, die der Eingabe, Kontrolle, Änderung und Löschung zur Verfügung stehen, umgesetzt. Daten die manuell oder automatisch aus Schnittstellen importiert werden, werden entweder markiert oder als Datei im System protokolliert.

Alle Programme verfügen über die Verwaltung von Zugriffsrechten, die Funktionen für die Nutzung und Kontrolle der Zugriffsrechte übernehmen. Über die Datenbankverwaltung stehen geeignete Maßnahmen zur Protokollierung und Wiederherstellung zur Verfügung

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle
(Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.)

An allen Standorten, sowohl am Standort der hmd-software AG, als auch in den benutzten Rechenzentren, stehen für die permanente Verfügbarkeit der Datenbestände die nötigen Maßnahmen gegenüber, die eine sehr hohe Verfügbarkeit gewährleisten. Dabei werden alle technischen Maßnahmen, die in angemessener und finanzieller Weise zur Verfügung stehen, umgesetzt.

Technische Konzepte werden regelmäßig überprüft und auf den neuesten technischen Stand gebracht.

Rasche Wiederherstellbarkeit
(Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.)

Sowohl die technische Basis, also auch die darin enthaltenen Datenbestände, werden nach Umfang und in angemessener finanzieller Weise umgesetzt. Alle nötigen Datenbestände werden regelmäßig gesichert. Dies wird durch ein Backup & Wiederherstellungskonzept sichergestellt. Wiederherstellungen von gelöschten Testdaten und ein Notfallplan für das Recovery - sowohl für die technische Basis, als auch für die Datenbestände - sichern die rasche Wiederherstellbarkeit ab. Dabei stellt die Virtualisierung von Produktivumgebungen einen großen Teil dar.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DS-GVO; Art. 25 Abs. 1 DS-GVO)

Datenschutz-Management
(Maßnahmen, die gewährleisten, dass die innerbetriebliche Organisation so gestaltet wird, dass sie den besonderen Anforderungen des Datenschützers gerecht wird.)

Die gesamte betriebliche Organisation für alle Mitarbeiter, stellt den Datenschutz, als Bestandteil der Firmenpolitik bei der Verarbeitung und Weitergabe der Daten in den Vordergrund. Mit der Bestellung eines Datenschutzbeauftragten und regelmäßigen Schulungen, wird die Umsetzung des erstellten Datenschutzkonzeptes permanent in allen Bereichen sichergestellt.

Basis ist in vielen technischen Bereichen der IT Grundschutz nach BSI, soweit dieser in Umfang und technischer Vorgabe umgesetzt, bzw. die Verhältnismäßigkeit dazu umgesetzt werden kann.

Incident-Response-Management
(Maßnahmen, die gewährleisten, dass im Falle einer Datenpanne eine unmittelbare Information an den Auftraggeber erfolgt.)

Alle Mitarbeiter aus den beteiligten Abteilungen werden regelmäßig unter Einbeziehung von externen Beratern und Schulungen bzw. Weiterbildungen auf die Erkennung von Datenabflüssen geschult. Ein Szenario zur Erkennung und Bewertung von Datenpannen, inkl. eines Vorfallreaktionsplans (Incident Response Plan - IRP) stehen zur Verfügung.

Datenschutzfreundliche Voreinstellungen
(Maßnahmen, die gewährleisten, dass den Vorgaben des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge getan wird.)

Die Maßnahmen sind aufgeteilt nach lokalen Softwarelösungen und dem Internetauftritt der hmd-software AG.

Im Internetauftritt der hmd-software AG und deren Folgeseiten werden keine Daten ohne Zustimmung der ausführenden Personen gespeichert. Jede Eingabe dient ausschließlich der Nutzung der Softwarelösung und wird durch den Benutzer mit dem Speichern explizit bestätigt.

In der lokalen Softwarelösung stehen alle Funktionen, die personenbezogene Daten speichern, in direktem Zusammenhang mit dem Mandantenverhältnis in der Steuerkanzlei, bzw. des Unternehmens, das die Software nutzt. Personenbezogene Daten werden nur für Fälle gespeichert, die zur Ausführung der übertragenen Aufgaben, sowohl im Mandantenverhältnis, als auch als Nutzer der Software, notwendig sind.

Auftragskontrolle
(Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.)

In Zusammenhang mit der Erfüllung der laufenden Tätigkeiten zur permanenten Verfügbarkeit und Sicherheit der Datenbestände, sind alle Sorgfaltsgesichtspunkte bei der Zusammenarbeit mit Unternehmen umgesetzt worden. Schriftliche Anweisungen und die Überprüfung der technisch organisatorischen Maßnahmen gehören ebenfalls dazu. Die Einhaltung der Vertraulichkeit im Umgang mit laufenden Informationen, sowie deren Vernichtung oder Unkenntlichmachung nach Beendigung des Auftrages sind im Anforderungsprofil umgesetzt. In der Vereinbarung sind Kontrollrechte und die laufende Überprüfung des Auftragnehmers mit eingebunden.

	Christian Heidler
Datum	Verantwortlicher für die Erstellung (in Druckbuchstaben)
	
	Unterschrift des Verantwortlichen