Marius Reichard WHI-Services
Am Bruchgraben 13, 31157 Sarstedt
info@whi-services.de | 0151-20151089
www.whi-services.de

Technische und organisatorische Maßnahmen gem. Art. 32 DSGVO

Einleitung

Der Auftraggeber hat die Möglichkeit von Marius Reichard WHI-Services als Auftragnehmer verschiedene Services in Anspruch zu nehmen. Die genauen Leistungen sind in den jeweiligen Hauptverträgen geregelt. Im Rahmen einer Auftragsverarbeitung wird ein Zusatzvertrag als Ergänzung zu den Hauptverträgen geschlossen. Die folgenden Erläuterungen sind wiederum eine vertragliche Ergänzung zu diesem Zusatzvertrag und beschreiben die technischen und organisatorischen Verantwortlichkeiten sowie Maßnahmen, die von Marius Reichard WHI-Services zum Schutz personenbezogener Daten ergriffen werden und deren Geltungsbereich.

Verantwortlichkeiten und Geltungsbereich

Der Auftraggeber ist für die Verarbeitung personenbezogener Daten verantwortlich und entscheidet allein über die Verarbeitungsweise personenbezogener Daten. Im Rahmen seiner Verantwortung kann sich der Auftraggeber auf die in diesem Dokument beschrieben technischen und organisatorischen Maßnahmen des Auftragnehmers verlassen. Der Auftragnehmer wendet diese konsequent an und stellt sicher, dass dadurch mindestens das in dem Zusatzvertrag zur Auftragsverarbeitung geregelten Schutzniveau eingehalten wird. Setzt der Auftragnehmer Subunternehmen ein, sind die Subunternehmen als Auftragsverarbeiter ebenfalls zur Ergreifung der beschriebenen Maßnahmen verpflichtet.

Beauftragt der Auftraggeber den Auftragnehmer mit dem vollständigen Betrieb einer Lösung, beispielsweise dem Betrieb einer Website oder App, greifen die beschriebenen Maßnahmen für den Betrieb dieser Lösung. Beauftragt der Auftraggeber den Auftragnehmer hingegen mit der Bereitstellung einzelner Services, greifen die beschriebenen Maßnahmen ausschließlich für diese Services. So hat der Auftragnehmer keinerlei Einfluss auf die Datenverarbeitung, wenn der Auftraggeber beispielsweise Hosting-Services ohne den Betrieb einer Lösung durch den Auftragnehmer in Anspruch nimmt. In diesem Fall kann der Auftragnehmer technische und organisatorische Maßnahmen ausschließlich bis zur Bereitstellung von Hosting-Kapazitäten ergreifen, nicht aber für die Bereitstellung von Lösungen, die der Auftraggeber eigenständig oder durch Dritte auf Basis dieser einzelnen Services betreibt. Insofern ergibt sich der Geltungsbereich der beschriebenen Maßnahmen durch die in den Hauptverträgen vereinbarten Leistungen.

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

- Zutrittskontrolle
  Es wird sichergestellt, dass kein unbefugter Zutritt zu physikalischen Datenverarbeitungsanlagen erfolgt. Hierzu sind die Gebäude durch Videoüberwachung und Einbruchmeldeanlagen geschützt. Schließsysteme regeln den Zutritt, indem sich befugte Personen beispielsweise durch Magnet- oder Chipkarte, Schlüssel, Transponder oder Video-Personenkontrolle ausweisen müssen.

- Zugangskontrolle
  Es wird sichergestellt, dass keine unbefugte Systembenutzung erfolgt. Hierzu sind die Systeme durch Firewalls sowie Passwörter mit Mindestanforderungen geschützt. Weiterhin werden Daten auf mobilen Datenträgern verschlüsselt.

- Zugriffskontrolle
  Es wird sichergestellt, dass kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems erfolgt. Hierzu werden nur befugten Personen die notwendigen Rechte zugeordnet. Diese Zuordnung erfolgt durch einen möglichst klein gehaltenen Kreis von Administratoren. Weiterhin werden Zugriffe in Log-Files protokolliert.

- Trennungskontrolle
  Es wird sichergestellt, dass eine getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, erfolgt. Hierzu wird der Zugriff auf Datenbestände auf die jeweils notwendigen Benutzer beschränkt und die Daten von Produktiv- und Entwicklungssystemen getrennt voneinander gespeichert.

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

- Weitergabekontrolle
  Es wird sichergestellt, dass kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport erfolgt. Hierzu werden personenbezogene Daten ausschließlich verschlüsselt übertragen.

- Eingabekontrolle
  Es wird festgestellt, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Hierzu werden Aktivitäten in Log-Files protokolliert.

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Verfügbarkeitskontrolle
  Es wird sichergestellt, dass ein Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust von Daten erfolgt. Hierzu wird eine unterbrechungsfreie Stromversorgung gewährleistet, Feuer- und Rauchmeldeanlagen sowie Monitoringsysteme ermöglichen die frühzeitige Erkennung Löschung von Bränden bzw. Eingreifen in die Systeme zur Sicherstellung der Verfügbarkeit.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- Datenschutz-Management
  Es ist ein Datenschutzmanagement etabliert.

- Incident-Response-Management
  Es erfolgt eine regelmäßige Überprüfung der IT-Infrastruktur.

- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
  Es werden nur Daten abgefragt, die für den jeweiligen Zweck erforderlich sind. Weiterhin sind beispielsweise Checkboxen zur Einholung von Einwilligungen initial deaktiviert und müssen durch den Benutzer aktiv angeklickt werden.

- Auftragskontrolle
  Es erfolgt keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers. Hierzu werden mit Subunternehmen Auftragsverarbeitungs-Verträge geschlossen, die mindestens dem Schutzniveau der hier beschrieben technischen und organisatorischen Maßnahmen entsprechen.

Version 2.0 vom 28.07.2018