ToM

zur Auftragsverarbeitung nach DS-GVO und BDSG

Berlin, den 01.04.2018

Inhaltsverzeichnis

Technische und organisatorische Maßnahmen....3
- Präambel....3
- Vertraulichkeit....3
  - Zutrittskontrolle....3
  - Zugangskontrolle....3
  - Zugriffskontrolle....3
  - Trennungskontrolle....4
- Pseudonymisierung....4
- Integrität....4
  - Weitergabekontrolle....4
  - Eingabekontrolle....4
- Verfügbarkeit und Belastbarkeit....4
  - Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit....4
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung....5
  - Datenschutz-Management und Incident-Response-Management....5
  - Datenschutzfreundliche Voreinstellungen....5
  - Auftragskontrolle....5

Weiterführende Informationen....5
- Mitgeltende Dokumente....5
- Datenschutzbeauftragter der managedhosting.de GmbH....5
- IT-Sicherheitsbeauftragter der managedhosting.de GmbH....5
- Ansprechpartner bei der managedhosting.de GmbH....5

Technische und organisatorische Maßnahmen

Präambel

Bei Abschluss eines Vertrags zur Auftragsverarbeitung sind auch die technischen und organisatorischen Maßnahmen, mit denen der Auftragnehmer die Einhaltung der vertraglichen Verpflichtungen sicherstellt, schriftlich festzulegen. Dazu werden hiermit folgende technische und organisatorische Maßnahmen verbindlich festgelegt.

Vertraulichkeit

Art. 32 Abs. 1 b) DS-GVO

Zutrittskontrolle

Unbefugte erlangen zu den technischen Einrichtungen keinen Zutritt. Die von der managedhosting.de GmbH betriebenen Rechenzentrumsstandorte mit der dazugehörenden Infrastruktur sind eine Hochsicherheitszone und entsprechen mindestens der Datacenter Tier III - Klassifikation.

Nur durch die Geschäftsleitung autorisierte Personen erlangen nach persönlicher und zeitlich exakter Legitimation bei Betreiber und/oder Wachschutz Zugang zu den technischen Einrichtungen. Der Zugang zum Datacenter und zu sämtlichen sensiblen Bereichen ist ausschließlich auf autorisiertes Fachpersonal der managedhosting.de GmbH beschränkt. Befugte werden entweder vom Sicherheitspersonal oder auch durch mehrere separate Kontrollsysteme eindeutig identifiziert. Der Zutritt zu operativen Bereichen ist nur nach Prüfung durch mehrstufige, unabhängig voneinander wirkende Authentifizierungs- und Autorisierungsmaßnahmen möglich. Ein unbefugter Zutritt wird dadurch praktisch unmöglich.

Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten sind:

- Personalisiertes Zutrittskontrollsystem,
  Ausweisleser, Magnetkarte, Chipkarte mit biometrischer Authentifizierung
- Interne Organisationsanweisung und Protokollierung von Zutrittsbeantragungen
- Türsicherungen (elektrische Türöffner, PIN-Schloss usw.)
- Identifizierung der zutrittsberechtigten Personen durch Wachschutz
- Genereller Einsatz von Überwachungseinrichtungen
  Alarmanlage, Videoüberwachung

Zugangskontrolle

Der administrative Zugang zu den für die Erbringung der in der Leistungsvereinbarung beschriebenen IT-Dienstleistung notwendigen Einrichtungen (Hardware, Betriebssysteme, Software) erfolgt grundsätzlich über ein personalisiertes, mindestens zweistufiges Authentifizierungsverfahren. Die Authentifizierungsregeln entsprechen dem derzeitigen Stand der Technik und werden regelmäßig auf Ihre Wirksamkeit hin überprüft.

Die organisatorischen Festlegungen sind im Detail u. a. in der Arbeitsplatzrichtlinie und in der Passwortrichtlinie der managedhosting.de GmbH festgelegt und für alle Mitarbeiter verbindlich. Die Passwortrichtlinie ist Bestandteil der ISO/IEC 27001 Zertifizierung und kann öffentlich eingesehen werden: https://go.managedhosting.de/iso27001.

Zugriffskontrolle

Die mit administrativen Tätigkeiten beauftragten Mitarbeiter haben nach erfolgreicher Authentifizierung lediglich die auf sie festgelegten Zugriffsrechte und Befugnisse (Autorisierung). Vertretungsregelungen sind definiert.

Maßnahmen, damit die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, sind z.Bsp.:

- Berechtigungsmechanismus mit Möglichkeit zur exakten Differenzierung
- Revisionssicheres, verbindliches Berechtigungsvergabeverfahren
- Revisionssicheres, verbindliches Verfahren zur Wiederherstellung von Daten aus Backup (Restore durch IT-Abteilung auf Anweisung von Projektleitung / Abteilungsleitung / Geschäftsleitung / Geschäftsführung)
- Trennung von Berechtigungsbewilligung (organisatorisch) durch Abteilungsleitung / Geschäftsleitung / Geschäftsführung und Berechtigungsvergabe (technisch) durch IT- Abteilung

Trennungskontrolle

Der Auftragnehmer stellt durch geeignete Maßnahmen sicher, dass die Daten des Auftraggebers auf den technischen Einrichtungen der managedhosting.de GmbH nicht anderweitig durch nicht autorisierte Dritte verarbeitet werden können. Art und Umfang der zur Verfügung stehenden Möglichkeiten sind in der Leistungsvereinbarung, den AGB und dem SLA festgelegt.

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken sind z. Bsp. aber nicht ausschließlich:

- Interne Mandantenfähigkeit / Zweckbindung
- Physikalische und logische Segmentierung der Datenverarbeitungseinrichtungen
- Private, nur für den Auftraggeber verfügbare Instanzen der Datenverarbeitungseinrichtungen
- Funktionstrennung zwischen Produktions- und Testumgebung

Pseudonymisierung

Art. 32 Abs. 1 a) DS-GVO; Art. 25 Abs. 1 DS-GVO

Eine Pseudonymisierung erfolgt durch den Auftragnehmer nicht.

Integrität

Art. 32 Abs. 1 b) DS-GVO

Weitergabekontrolle

Eine Weitergabe und Übermittlung personenbezogener Daten, die sich auf den technischen Einrichtungen der managedhosting.de GmbH befinden ist grundsätzlich nur im Rahmen vorliegender Weisung des Auftraggebers möglich und wird protokolliert. Eine Weitergabe zu Zwecken der Strafverfolgung ist nur bei Vorliegen eines richterlichen Beschlusses möglich. Der Auftraggeber wird darüber zeitnah informiert.

Weitere, nicht spezifische Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung von Datenträger (manuell oder elektronisch), sind in der Leistungsvereinbarung, den AGB und dem SLA festgelegt.

Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten. Der Einsatz und Umfang konkreter Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind, ist sind in der Leistungsvereinbarung, den AGB und dem SLA festgelegt.

Alle administrativen Tätigkeiten (z.b. Einrichtung und Änderung von Datensicherungen, Software-Updates u.a.), die der Auftragnehmer aufgrund organisatorischer Vereinbarungen bzw. auf Anweisung für den Auftraggeber ausführt, werden grundsätzlich protokolliert und sind über den vorgeschriebenen Zeitraum nachvollziehbar.

Verfügbarkeit und Belastbarkeit

Art. 32 Abs. 1 b) DS-GVO

Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit

Der Auftragnehmer trifft, soweit in der Leistungsvereinbarung festgelegt, geeignete Maßnahmen gegen Zerstörung oder Verlust von Daten.

- Datensicherung
- Replikationsverfahren

Art und Umfang der zur Verfügung stehenden Möglichkeiten sind in der Leistungsvereinbarung, den AGB und dem SLA festgelegt und müssen vom Auftraggeber im Rahmen der Auftragserteilung angewiesen werden.

Die Verfügbarkeit der technischen Einrichtungen gemäß der Vereinbarungen (SLA) wird nach derzeitigem Stand der Technik durch den Auftragnehmer gewährleistet. Die inhaltliche Verfügbarkeit der Daten obliegt dem Auftraggeber.

Darüberhinaus trifft der Auftragnehmer umfangreiche Maßnahmen, damit die innerbetriebliche Organisation den besonderen Anforderungen des Datenschutzes gerecht wird. Dies sind z. Bsp. aber nicht ausschließlich:

- Vollständiges Backup- und Recovery-Konzept mit mindestens täglicher Sicherung und katastrophensicherer Aufbewahrung der für die Aufrechterhaltung des Geschäftsbetriebes des Auftragnehmers notwendigen Daten
- Nachweis der sicheren und ordnungsgemäßen Archivierung in physisch geschütztem Archiv und verbindlicher Regelung der Zugriffsberechtigten
- Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter) und schriftliche Konzeption ihres Einsatzes (Virenschutzkonzept usw.)
- Umfassender Einsatz von Redundanz in allen für die Aufrechterhaltung des Geschäftsbetriebes des Auftragnehmers notwendigen technischen Systemen

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Art. 32 Abs. 1 d) DS-GVO; Art. 25 Abs. 1 DS-GVO

Datenschutz-Management und Incident-Response-Management

Der Auftragnehmer betreibt ein Information Security Management System (ISMS) nach den Richtlinien der Norm ISO/IEC 27001.

Datenschutzfreundliche Voreinstellungen

Art. 25 Abs. 2 DS-GVO

Es greifen die in den betreuten Anwendungen vom Auftraggeber vorgesehenen Mechanismen. Der Auftragnehmer verändert diesbezügliche Einstellung nur nach entsprechender Abstimmung mit dem Auftraggeber.

Auftragskontrolle

Die weisungsgemäße Auftragsverarbeitung wird gewährleistet. Konkrete Maßnahmen zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer sind in der Leistungsvereinbarung, den AGB und dem SLA festgelegt:

- Eindeutige Vertragsgestaltung
- Formalisierte Auftragserteilung (Auftragsformular) durch Auftraggeber
- Kontrolle der Vertragsausführung
- Pflicht der Schriftform bei Änderungswünschen und Anweisungen durch den Auftraggeber

Weiterführende Informationen

Mitgeltende Dokumente

Kontakt:	https://www.managedhosting.de/contact
SLA:	https://www.managedhosting.de/sla
AGB:	https://www.managedhosting.de/agb
Datenschutzerklärung:	https://www.managedhosting.de/privacy
TOM (öffentlich):	https://www.managedhosting.de/tom

Datenschutzbeauftragter der managedhosting.de GmbH

Ingenieurbüro für Datenschutz & Datensicherheit
Dipl.-Ing. Pierre-Gerard Große
Reichenbrander Str. 40

09117 Chemnitz

Telefon: +49 371 8579094
Telefax: +49 371 8579095
E-Mail: pierre.grosse@datenschutz-grosse.de

IT-Sicherheitsbeauftragter der managedhosting.de GmbH

Gesa Lütje
Die Strategisten GmbH
Kurze Mühren 1

20095 Hamburg

E-Mail: isms@managedhosting.de

Ansprechpartner bei der managedhosting.de GmbH

Marco Gregori

Telefon: +49 800 6737877
E-Mail: marco.gregori@managedhosting.de