

Informationen zum Datenschutz und zur Datenverarbeitung

TESCOBE Consultants
(asig-online.com)
Mainstrasse 6
65232 Taunusstein
Deutschland

Web:

<https://www.tescobe.de>
<https://www.asig-online.com>

eMail-Allgemein:

info@tescobe.de
info@asig-online.com

Erstellt am 24.10.2015

Update: 26.04.2020

asig-online.com
Ein Unternehmen der TESCOBE Consultants
Sitz: Mainstrasse 6
65232 Taunusstein
Telefon: +49 6128 936-5020
Fax: +49 6128 936-5021
Web: <https://www.asig-online.com>
EMail: info@asig-online.com
kundenservice@asig-online.com

Bankverbindung
Nassauische Sparkasse
IBAN: DE66 5105 0015 0189 0596 47
BIC: NASSDE55
USt-Id Nr.: DE207666415

Seite 1 von 11

Vertretungsberechtigt: Gerhard Hass

Inhalt

1. Grundsätzliches.....	3
1.1 Ziele des Dokumentes und der Auskunft	3
1.2 Hinweise.....	4
2. Gesetzliche Grundlagen.....	5
3. Auftragsdatenverarbeitung gem. §11 BDSG ³	5
4. Technische und organisatorische Maßnahmen gem. §9 BDSG.....	6
4.1 Zutrittskontrolle.....	7
4.2 Zugangskontrolle	7
4.3 Zugriffskontrolle	7
4.4 Weitergabekontrolle.....	7
4.5 Eingabekontrolle	7
4.6 Auftragskontrolle.....	7
4.7 Verfügbarkeitskontrolle ⁷	7
4.8 Trennungsgebot.....	7
4.9 Verschlüsselung.....	8
4.10 Berichtigung, Löschung und Sperrung.....	8
4.11 Unterauftragsverhältnisse	8
4.15 Rückgabe von Datenträgern und Löschung der Daten nach Beendigung	8
5. Quellen.....	9
6. Anlagen.....	10

1. Grundsätzliches

asig-online.com ist ein Service von TESCOBE Consultants und wird auch unter dem Begriff TESCOBE geführt.

asig-online.com stellt seinen Kunden eine webbasierte Software zur Verfügung, um die Kunden in die Lage zu versetzen, Unterweisungen ihrer Mitarbeiter und weitere Dokumentationen nachvollziehbar durchzuführen und zu archivieren.

Dieses Softwaresystem integriert auch die Erfolgskontrolle und eine Übersicht der vollzogenen Unterweisungen durch die jeweiligen Mitarbeiter des Kunden.

Da es sich hierbei um personenbezogene Daten handelt, bei denen allerdings eine Überprüfung von Fähigkeiten, Verhalten und Leistung des einzelnen Mitarbeiters durch seinen Vorgesetzten nicht möglich ist, ist im Sinne des BDSG eine Vorabkontrolle (gem. Art. 35 DSGVO) nicht erforderlich. asig-online.com ist in keinem Fall die verantwortliche Stelle im Sinne Art. 4 DSGVO. Die verantwortliche Stelle ist in diesem Zusammenhang immer der Kunde.

1.1 Ziele des Dokumentes und der Auskunft

Durch asig-online.com sollen in diesem Dokument die technischen und organisatorischen Maßnahmen für die Auftraggeber dokumentiert werden. Dieses Dokument soll darüber hinaus Audits der Auftraggeber ersetzen und die eventuell notwendigen Angaben für einen Vertrag über die Datenverarbeitung im Auftrag (Art. 26 DSGVO) beinhalten und/oder für einen solchen Vertrag als Anlage dienen, um eine gesetzeskonforme Umsetzung zu belegen. Die erforderliche, „sorgfältige Auswahl“¹ des Auftragnehmers durch den Auftraggeber wird hiermit dokumentiert.

Aus datenschutzrechtlicher Sicht sind für diesen Zweck hauptsächlich die folgenden Paragraphen des Bundesdatenschutzgesetzes (BDSG) relevant:

- §64 Anforderungen an die Sicherheit der Datenverarbeitung
- § 28 Abs. 1 Nr. 1 bis 3 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

Die Sensibilität der personenbezogenen Daten erfordert darüber hinaus die Begutachtung der technischen und organisatorischen Maßnahmen (vgl. §64 BDSG).

Die Geschäftsräume der TESCOBE Consultants (asig-online.com) in der Mainstrasse 6, 65232 Taunusstein, sind in diesem Zusammenhang nicht relevant, da innerhalb dieser Räumlichkeiten keine Daten der Kunden gespeichert oder verarbeitet werden.

Das Hosting des Softwaresystems wurde extern vergeben. Die Vertragsgestaltung im Unterauftragsverhältnis zwischen TESCOBE Consultants und dem Dienstleister (Rechenzentrum/RZ) ist für die Beurteilung ebenfalls von Bedeutung.

Zur besseren Beurteilung des Prozesses bzw. des Verfahrens wurde durch TESCOBE Consultants eine Prozessbeschreibung erstellt. Diese Prozessbeschreibung kann auf Verlangen vorgelegt werden.

¹ Vgl. §28 Abs. 1 Nr. 1 bis 3 BDSG

1.2 Hinweise

Grundlage für die erteilten Informationen sind die folgenden von asig-online.com bereitgestellten Informationen²:

- 1 - Informationen zum Datenschutz von asig-online.com
- 2 - Interne Verfahrensbeschreibung
- 3 - Öffentliches Verfahrensverzeichnis asig-online.com
- 4 - Internes Verfahrensverzeichnis asig-online.com
- 5 – Mitarbeiterverpflichtung auf das Datengeheimnis

² Informationsunterlagen der TESCOBE Consultants (asig-online.com)

2. Gesetzliche Grundlagen

Als Basis zur Beurteilung der datenschutzrechtlichen und –technischen Umsetzung wird das Bundesdatenschutzgesetz (BDSG) Ausfertigungsdatum 20.11.2019 zuletzt geändert durch Geändert durch Art. 12 G v. 20.11.2019 I 1626 herangezogen.

3. Auftragsdatenverarbeitung gem. §62 BDSG³

Eine Auftragsdatenverarbeitung im Sinne §62 BDSG liegt zwischen dem Betreiber des Rechenzentrums und TESCOBE Consultants (asig-online.com) nicht unmittelbar vor, da durch den Dienstleister keine Verarbeitung personenbezogener Daten im Sinne des BDSG erfolgt.⁴

Da in der Fachliteratur der Sonderfall der „Datenverarbeitung im Auftrag bei RZ-Dienstleistungen“ kontrovers diskutiert wird, wurde zwischen asig-online.com und dem Rechenzentrum die Vereinbarung geschlossen, dass die Speicherung der Daten ausschließliche in Deutschland bzw. im Geltungsbereich der EU erfolgt und dass diese Orte den entsprechenden Datenschutzregelungen des EU Raumes unterliegen.

³ Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

⁴ Vgl. BDSG Kommentar Gola, Klug, Körfner, 10. Auflage, Rn 14 zu §11 BDSG

4. Technische und organisatorische Maßnahmen gem. §64 BDSG

Werden personenbezogene Daten verarbeitet, so sind die technischen und organisatorischen Maßnahmen an dem Schutzbedarf auszurichten⁵.

Die zentrale Datenverarbeitung findet dabei auf Serversystemen statt, welche sich nach angemessenen Sicherheitsstandards im Rechenzentrum der Contabo GmbH, Aschauer Straße 32a, 81549 München, in Deutschland befinden.

Die technischen und organisatorischen Maßnahmen des Rechenzentrums wurden durch den Betreiber in Form eines aufgebauten Management-Systems zur Informationssicherheit (ISMS ISO 27001) belegt.

Die Möglichkeit eines unberechtigten Zugriffes kann demnach nur auf dem Übertragungsweg (Internetzugriff) stattfinden. Um diese Möglichkeit auszuschließen, wird durch asig-online.com grundsätzlich die Verschlüsselung der Datenübertragung eingesetzt. Diese ist mittels SSL⁶ realisiert. Auf diesem Wege stellt asig-online.com die maximale Sicherheit für den Auftraggeber dar. Kosten für die Verschlüsselung fallen für den Auftraggeber nicht an. Die Verschlüsselung der Daten wird ausschließlich im Zusammenhang mit dem Hosting durch asig-online.com bereitgestellt. Nutzt der Auftraggeber eigene Serversysteme (Hosting durch den Auftraggeber selber) ist dieser für die Sicherheit der Datenübertragung selber verantwortlich (Verantwortliche Stelle).

Die Mitarbeiter der TESCOBE Consultants (asig-online.com) wurden auf das Datengeheimnis verpflichtet.

⁵ Vgl. §64 BDSG

⁶ Secure Sockets Layer / Transport Layer Security

4.1 Zutrittskontrolle

Da innerhalb der Geschäftsräume der TESCOBE Consultants (asig-online.com) weder Daten verarbeitet noch Entwicklungsleistungen gestellt werden, ist die Zutrittskontrolle für diese Bereiche ausreichend. Die Partner der asig-online.com haben durch entsprechende Maßnahmen und Zertifikate die Sicherheit der Systeme dokumentiert. Die eingerichteten Management-Systeme werden fortlaufend aufrechterhalten und stellen die Basis für die Zusammenarbeit der Partner dar.

4.2 Zugangskontrolle

Passwortschutz aller Computersysteme mit hinreichenden Komplexitätsanforderungen und Wechselintervallen.

4.3 Zugriffskontrolle

Audittrail (Nachvollziehbarkeit des Zugriffs) innerhalb des eLearning-Systems.

4.4 Weitergabekontrolle

TESCOBE Consultants (asig-online.com)

Unterweisungs-Tool, e-Learning-System: SSL-Datenübertragung zum Server.

Kunde – Unterweisungs-Tool, e-Learning-System: SSL-Datenübertragung zum Server.

4.5 Eingabekontrolle

Audittrail (Nachvollziehbarkeit der Änderungen) innerhalb des eLearning-Systems.

4.6 Auftragskontrolle

Vertragliche Regelung mit dem RZ-Betreiber und Vorbehalt der Prüfung der technischen und organisatorischen Maßnahmen beim RZ-Betreiber.

4.7 Verfügbarkeitskontrolle⁷

Die Daten von Mitarbeitern der Kunden über die zugewiesenen und absolvierten Unterweisungen sind auf dem jeweiligen Serversystem im Rechenzentrum hinterlegt. Das Rechenzentrum wird durch einen Wachschatz gesichert und mit Kameras überwacht. Eine Zutrittskontrolle ist eingerichtet. Die Stromversorgung ist trassenredundant ausgelegt und wird durch Dieselgeneratoren zusätzlich abgesichert. Das RZ verfügt über eine Klimatisierung mit Luftfeuchtekontrolle. Eine Brandmelde- und Brandschutzanlage ist installiert. Die Serversysteme sind redundant ausgelegt.

4.8 Trennungsgebot

Die Daten für unterschiedliche Kunden werden in getrennten Datenbankclustern hinterlegt. Hierdurch wird eine logische, virtuelle Trennung zwischen den Kundendaten sichergestellt.

4.9 Verschlüsselung

Die Datenübertragung zwischen Browser (des Kunden) und RZ wird mittels SSL verschlüsselt. Die Daten auf den mobilen Geräten der Mitarbeiter (Notebooks) werden verschlüsselt abgelegt.

4.10 Berichtigung, Löschung und Sperrung

Über Browser – Verwaltungsebene für die Nutzer, die über eine entsprechende Berechtigung verfügen, bzw. unmittelbar vom Auftraggeber selbst.

4.11 Unterauftragsverhältnisse

Es besteht ein Unterauftragsverhältnis zwischen asig-online.com und dem Betreiber des Rechenzentrums. Das Rechenzentrum ist entsprechend der Anforderungen nach ISO 27001 (Informations-Sicherheits-Management-Systeme, ISMS) zertifiziert und kommt somit den Forderungen des BDSG (Bundesdatenschutz-Gesetzes) nach.

4.15 Rückgabe von Datenträgern und Löschung der Daten nach Beendigung

Für die Löschung der Daten auf dem Server ist der Kunde selber verantwortlich, außer er beauftragt die asig-online.com mit der entsprechenden Durchführung.

Nach Beendigung des Vertrags werden die Daten innerhalb einer Karenzzeit von sechs Monaten in der kontinuierlichen, rollierenden Datensicherung im Backup-System vorgehalten. Danach werden die Daten automatisch überschrieben.

⁷ Informationen zu den technischen und organisatorischen Maßnahmen wurden durch den Betreiber des RZ zur Verfügung gestellt und sind Vertragsbestandteil im Auftragsverhältnis zwischen asig-online.com und dem RZ.

5. Quellen

- Bundesdatenschutzgesetz, zuletzt geändert 20.11.2019 | 1626
- BDSG Kommentar Gola, Klug, Körfer; 10. Auflage; Verlag C.H.Beck München
- BSI Grundschutz Baustein 1.5 - Datenschutz, Bundesamt für Sicherheit in der Informationstechnik
- Information Security Management; Burgartz, Röhrig; März; TÜV Media, März 2010

6. Anlagen

Datenschutz-Verfahrensbeschreibung (exemplarisch)

Datenschutz-Verfahrensbeschreibung

Zweckbestimmung

- Unterweisung von Mitarbeitern und Fremdfirmen

Rechtsgrundlage(n)

- Datenverarbeitung für eigene Zwecke gem. §62 BDSG
- DGUV bzw. DGUV V1 "Grundsätze der Prävention" gem. §§15ff SGB VII
- Arbeitsschutzgesetz/ArbSchG

Kreis der Betroffenen

- Eigene Mitarbeiter
- Mitarbeiter von Fremdfirmen
- Zeitarbeiter; Besucher

Art der Daten

- Name
- Personalnummer
- eMail-Adresse (Firmenadresse)
- Zugewiesene Unterweisungen(en)
- Zieldatum der Unterweisung
- Abschluss der Unterweisung
- Firmenanschrift (Strasse, Nummer, Plz, Ort)
- Telefon, Fax, Mobil-Nummer (nicht zwingend erforderlich und werden im Normalfall nicht erfasst)

Empfänger

Kunden-Intern

- Vorgesetzte
- Mitarbeiter (Unterweisungsdurchführender)
- Personalabteilung

Extern (TESCOBE Consultants/asig-online.com)

- keine

Herkunft der Daten (auch intern)

- Grunddaten d. Mitarbeiter (Name, Personalnummer, Abteilung) aus der Personal bzw. IT-Abteilung, der entsprechende ERP-Systeme siehe „Art der Daten“

Gesetzliche Aufbewahrungspflichten

- Je nach Unterweisung bis zum Ende des Beschäftigungsverhältnisses oder bis zur Außerbetriebnahme der Einrichtung
- Gem. Gefahrstoff-VO ggf. längere Aufbewahrungszeiten

Regelfristen für die Löschung

- Abhängig vom Kunden bzw. Auftraggeber. Daten die TESCOBE Consultants (asig-online.com) zum Erfassen übergeben sind, werden nach abgeschlossener Arbeit im Rahmen der gesetzlichen Löschfristen gelöscht, bzw. vernichtet.

Eingesetzte Hardware

- Eigene IT als "Frontend" für die Online-Unterweisung
- Webserver im Rechenzentrum des Unterauftragnehmers von asig-online.com

Eingesetzte Software

- Softwaresystem "e-Learning-System"

Zutritts und Zugangskontrolle

- Abhängig vom Kunden bzw. Auftraggeber

Zugriffskontrolle

- Protokollierung im eLearning-System

Weitergabekontrolle

- SSL-Verschlüsselung des Übertragungswegs zwischen Eingabestelle und Verarbeitender Stelle
Für die interne Weitergabe (Hosting beim Kunden) ist der Kunde verantwortliche Stelle

Eingabekontrolle

- Keine manuelle Dateneingabe durch asig-online.com außer bei expliziter Beauftragung durch den Kunden. Die Richtigkeit der Daten ist durch den Kunden zu überprüfen, eine Haftung wird durch asig-online.com ausgeschlossen

Auftragskontrolle

- Weisungsgebundenheit gem. DV im Auftrag mit asig-online.com

Verfügbarkeitskontrolle

- Redundante Webserver im Rechenzentrum

Trennungsgebot

- Dedizierte Datenbanken pro Kunde

Art der Verschlüsselung

- TLS/SSL

Hinweis:

Diese Verfahrensbeschreibung soll als Orientierungshilfe dienen. Die tatsächliche Datenverwendung kann je nach Auftraggeber in einzelnen Punkten variieren.