Technische und organisatorische Maßnahmen
(Anlage 1 zur Auftragsverarbeitungsvereinbarung, Mai 2019)

1. Organisatorische Maßnahmen

a. Betrieblicher Datenschutzbeauftragter:

MORGENSTERN consecom GmbH
Jan Morgenstern
Große Himmelsgasse 1
67346 Speyer

E-Mail: dsb@epikur.de

b. Mitarbeiter werden nachweislich über Datenschutzrecht und Datensicherheit geschult.

c. Alle Mitarbeiter sind nachweislich auf das Datengeheimnis, ggf. auf das Fernmeldegeheimnis, mittels arbeitsvertraglicher Regelung verpflichtet.

d. Es existieren verfahrensunabhängige Plausibilitäts- und Sicherheitsprüfungen (z.B. technisch unterstützt oder durch Externe).

e. Datenkonzept,

f. Datensicherheitskonzept.

2. Vertraulichkeit gemäß Art. 32 Abs. 1 lit. b DS-GVO

a. Zutritts-, Zugangs-, Speicher- und Datenträgerkontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zugang zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet werden:

aa. Zutrittsregelungen zum Betreten der Räume mit DV-Anlagen,

bb. Schlüsselregelung (Schlüsselverwaltung mittels protokollierter Schlüsselausgabe/-rückgabe),

cc. Transponder-Schließsystem (Büroeingangstüren),

Epikur Software GmbH & Co. KG
Franklinstraße 26 a
10587 Berlin
USt-IdNr: DE281639000

Sitz der Gesellschaft:
Berlin Charlottenburg
Handelsregister:
Amtsgericht Charlottenburg
HRA 46263 B

Komplementärin:
Epikur Software Verwaltung GmbH
GF: Bernhard Hertel,
Dr. Krister Helbing
HRB 139118 B

Bankverbindung:
Deutsche Apotheker- und Ärztebank eG
IBAN: DE53300606010102617056
BIC: DAAEDEDDXXX

Kontaktdaten:
Telefon: +49 30 340 601 100
Telefax: +49 30 340 601 109
E-Mail: info@epikur.de
Internet: www.epikur.de

dd. manuelles Schließsystem,

ee. Zutritt für Betriebsfremde nur nach Klingelnutzung,

ff. Auswahl des Reinigungspersonals erfolgt sorgfältig,

gg. feuerfeste Türen,

b. Zugangs- und Benutzerkontrolle

Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

aa. Passworte mit Groß-, Kleinschreibung und Ziffern,

bb. Wechselfrist für Passworte: maximal drei Monate,

cc. Authentifikation mit Benutzername und Passwort,

dd. Einsatz von VPN-Technologie,

ee. Verschlüsselung von Datenträgern.

c. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass Personen nur im Rahmen ihrer Zugriffsberechtigung auf Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

aa. schriftliches Berechtigungskonzept,

bb. Zuordnung von Benutzerrechten/Erstellen von Benutzerprofilen,

cc. Verwaltung der Rechte durch System-Administrator,

dd. geringst erforderliche Anzahl von Personen mit Administratorrechten,

ee. Automatische Sperrung des Arbeitsplatzes,

ff. Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten,

gg. Einsatz von Aktenvernichtern DIN 66399,

hh. Verschlüsselung von Datenträgern,

ii. sichere Aufbewahrung von Datenträgern,

jj. ordnungsgemäße Vernichtung/Löschung von Datenträgern,

kk. Löschungskonzept für Daten,

ll. Protokollierung der Vernichtung/Löschung.

d) Transport- und Übertragungskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung ist.

aa. Die nach dem Stand der Technik erforderlichen Firewall-Technologien sind implementiert und werden auf dem aktuellen Stand gehalten,

bb. Weitergabe von Daten in verschlüsselter Form, z. B. mittels AES 256 Bit und PGP,

cc. Einrichtungen von Standleitungen bzw. VPN-Tunneln,

dd. E-Mail-Verschlüsselung,

ee. Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen,

ff. Protokollierung von Übermittlungen,

gg. Protokollierung Aus- und Eingang von Datenträgern,

hh. Beim physischen Transport sorgfältige Auswahl von Transportpersonal und Fahrzeugen.

e. Auftragskontrolle gemäß Art. 32 Abs. 1 lit. d DS-GVO i. V. m. Art. 25 Abs. 1 DS-GVO

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

aa. Vereinbarungen zur Auftragsverarbeitung,

bb. Kontrolle der Vertragsausführung,

cc. Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags,

dd. Regelung zu Wartungen (speziell Fernwartung).

3. Integrität gemäß Art. 32 Abs. 1 lit. b DS-GVO

a. Eingabekontrolle/Verarbeitungskontrolle

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

aa. Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen),

bb. Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind.

b. Dokumentationskontrolle

Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.

aa. Führung eines Verarbeitungsverzeichnisses,

bb. Dokumentation der eingesetzten IT- Systeme und deren Systemkonfiguration.

4. Verfügbarkeitskontrolle gemäß Art. 32 Abs. 1 lit. b DS-GVO

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und im Störfall wiederhergestellt werden können.

aa. Unterbrechungsfreie Stromversorgung (USV) der Server,

bb. Überspannungsschutz,

cc. Feuer- und Rauchmeldeanlagen,

dd. Testen von Datenwiederherstellung,

ee. Feuerlöschgeräte in Nähe der Server,

ff. tägliche/regelmäßige Backups (Server),

gg. Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort,

hh. Virenschutzsoftware,

ii. Spiegelung von Festplatten (RAID-Verfahren.

5. Trennungsgebot gemäß Art. 32 Abs. 1 lit. b DS-GVO

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

a. Versehen der Datensätze mit Zweckattributen/Datenfeldern,

b. Logische Mandantentrennung (softwareseitig),

c. Trennung von Produktiv- und Testsystem,

d. Trennung von Daten verschiedener Auftraggeber.