Vertrag zur Auftragsverarbeitung (AVV) gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

zum Vertrag vom Klicken oder tippen Sie hier, um Text einzugeben.
zwischen Festo (Auftragsverarbeiter) und der Klicken oder tippen Sie hier, um Text einzugeben.
(Verantwortlicher)

zwischen dem Auftragsverarbeiter

Festo Didactic, (Straße), (Land, Ort) (der SE oder Landesgesellschaft)

– nachfolgend "Festo" genannt –

und dem Verantwortlichen

Firmierung Verantwortlicher, Adresse, Ort, Land

– nachfolgend „Verantwortlicher“ genannt –

– gemeinsam die „Parteien“ genannt –

Präambel
Der Verantwortliche erteilt Festo mit dem bestehenden Nutzungsvertrag („Hauptvertrag“) einen Auftrag zur Datenverarbeitung. Der vorliegende Auftragsverarbeitungsvertrag (AVV) konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien bei der Durchführung des Hauptvertrags und ersetzt etwaige bisherige zwischen den Parteien getroffene Vereinbarungen zur Auftragsverarbeitung.

1 Gegenstand und Dauer

1.1 Der Gegenstand des Auftrags zum Datenumgang ergibt sich aus dem Hauptvertrag vom Klicken oder tippen Sie hier, um Text einzugeben. und beinhaltet die Durchführung folgender Aufgaben:

- **Nutzung der Festo Learning Experience Plattform (Festo LX)**
- **Speicherung von Nutzungs- und Lernstandsdaten**

1.2 Die Dauer dieses AVV entspricht der Laufzeit des Hauptvertrags. Ändert sich der Umfang der gespeicherten personenbezogenen Daten bei einer Vertragsverlängerung nicht, gilt der AVV weiter.

2 Umfang, Art und Zweck der Datenverarbeitung sowie Kategorien betroffener Personen

Umfang, Art und Zweck der Datenverarbeitung sind im Hauptvertrag beschrieben und bestehen im Einzelnen aus:

2.1 Art der Daten:

Alle Anwender:
- Name, Vorname
- E-Mail-Adresse
- Stadt, Provinz/Staat, Land*
- Organisation
- Position*
- Primär-/Sekundärsprache*
- Interessenfelder*
- Tätigkeitsfelder*
- Abteilung*
- Titel*
- Fachkenntnisse*
- Zeitzone
- Elektrotechnische Einstellungen*

Lerner:
- Lernfortschritt
- Lernerfolge
- Antworten auf Testfragen
- Texte, Bilder, Videos
- Lernzeiten*

Lehrende:
- Selbsterstellte Lerninhalte inkl. Texte, Bilder, Videos*

*Optional

2.2 Kategorien betroffener Personen:

- **Beschäftigte**
- **Kunden, Interessenten o.ä.**

3 Technische und organisatorische Maßnahmen

3.1 Festo ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Verantwortlichen erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

3.2 Festo wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und gewährleistet, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Verantwortlichen gem. Art. 32 DSGVO, insbesondere mindestens die in Anlage 2 aufgeführten Maßnahmen getroffen hat. Festo legt auf Anforderung des Verantwortlichen die näheren Umstände der Festlegung und Umsetzung der Maßnahmen offen. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt Festo vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

4 Qualitätssicherung und sonstige Pflichten von Festo

Festo hat zusätzlich zur Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 EU-DSGVO. Er gewährleistet insbesondere die Einhaltung folgender Vorgaben:

4.1 Schriftliche Benennung eines Datenschutzbeauftragten:

Festo hat einen Datenschutzbeauftragten benannt.

4.2 Festo darf die Daten, die er im Auftrag verarbeitet, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Verantwortlichen berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich an Festo wendet, wird Festo dieses Ersuchen unverzüglich an die Datenschutzabteilung des Verantwortlichen weiterleiten.

4.3 Festo verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Verantwortlichen die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrags fort. Festo setzt bei der Durchführung des Auftrags nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Festo und jede Festo unterstellte Person, die Zugang zu personenbezogenen Daten hat, darf diese Daten ausschließlich entsprechend der Weisung des Verantwortlichen einschließlich der in diesem AVV eingeräumten Befugnisse verarbeiten, es sein denn, dass sie gesetzlich zur Verarbeitung verpflichtet ist.

4.4 Festo und der Verantwortliche arbeiten bei Anfragen der Aufsichtsbehörde zusammen. Festo informiert den Verantwortlichen unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit diese personenbezogene Daten des Verantwortlichen betreffen. Festo informiert den Verantwortlichen unverzüglich, wenn die zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung bei Festo ermittelt. Wenn der Verantwortliche einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch ausgesetzt ist, hat ihn Festo nach besten Kräften zu unterstützen.

4.5 Festo kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

4.6 Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten des Verantwortlichen durch Festo, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird Festo den Verantwortlichen unverzüglich informieren.

4.7 Festo unterstützt den Verantwortlichen bei der Erstellung des Verfahrensverzeichnisses sowie bei der Erstellung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO und ggf. bei der vorherigen

Konsultation der Aufsichtsbehörden gemäß Art. 36 DSGVO, soweit personenbezogene Daten des Verantwortlichen betroffen sind.

5 Einsatz von Subunternehmern

5.1 Die vertraglich vereinbarten Leistungen werden unter Einschaltung der in Anlage 1 genannten Subunternehmer durchgeführt. Festo ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. Er setzt den Verantwortlichen hiervon unverzüglich in Kenntnis. Festo ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Festo hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Verantwortliche seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat Festo sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z.B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Festo wird dem Verantwortlichen auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

5.2 Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn Festo Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die Festo für den Verantwortlichen erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Verantwortlichen genutzt werden.

6 Kontrollrechte des Verantwortlichen

6.1 Der Verantwortliche überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen bei Festo. Hierfür kann er z.B. Auskünfte bei Festo einholen, sich vorhandene Testate von Sachverständigen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen bei Festo nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zu Festo steht. Der Verantwortliche wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe bei Festo dabei nicht unverhältnismäßig stören.

6.2 Festo verpflichtet sich, dem Verantwortlichen auf dessen schriftliche oder elektronische Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen bei Festo erforderlich sind.

6.3 Der Verantwortliche dokumentiert das Kontrollergebnis und teilt es Festo mit. Bei Fehlern oder Unregelmäßigkeiten, die der Verantwortliche insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er Festo unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Verantwortliche Festo die notwendigen Verfahrensänderungen unverzüglich mit.

6.4 Der Verantwortliche vergütet Festo den Aufwand, der ihm im Rahmen der Kontrolle entsteht.

7 Weisungsbefugnis des Verantwortlichen

7.1 Festo darf während des Auftragsverhältnisses personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen verarbeiten, berichtigen, sperren und löschen.

7.2 Weisungen werden vom Verantwortlichen grundsätzlich in Textform (z.B. per E-Mail) erteilt.

7.3 Festo wird den Verantwortlichen unverzüglich darauf hinweisen, wenn die Befolgung einer Weisung nach seiner Ansicht gegen eine datenschutzrechtliche Vorschrift verstößt.

8 Kopien, Löschung und Rückgabe personenbezogener Daten

8.1 Kopien oder Duplikate von personenbezogenen Daten werden ohne Wissen des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherungskopien, die zu einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

8.2 6 Monate nach Beendigung des Auftragsverhältnisses löscht Festo alle aus diesem Verhältnis mit der Kundenorganisation erlangten personenbezogenen Daten, es sei denn, Festo ist aufgrund gesetzlicher Aufbewahrungspflichten daran gehindert.

8.3 Nach Beendigung des Auftragsverhältnisses gibt Festo sämtliche in seinen Besitz gelangten Unterlagen und Datenträger an den Verantwortlichen zurück oder vernichtet sie nach vorheriger Zustimmung durch den Verantwortlichen datenschutzgerecht.

9 Haftung und Schadensersatz

9.1 Der Verantwortliche und Festo haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung. Festo stimmt eine etwaige Erfüllung von Haftungsansprüchen mit dem Verantwortlichen ab.

9.2 Die Parteien stellen sich jeweils von der Haftung frei, wenn / soweit eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einer betroffenen Person eingetreten ist, verantwortlich ist. Im Übrigen gilt Art. 82 Absatz 5 DSGVO.

9.3 Sofern vorstehend nicht anders geregelt, entspricht die Haftung im Rahmen dieses Vertrages der des Hauptvertrages.

10 Schlussbestimmungen

10.1 Bei etwaigen Widersprüchen zwischen diesem AVV und dem Hauptvertrag gehen die Regelungen dieses AVV vor.

10.2 Sollten einzelne Regelungen dieses AVV unwirksam sein, berührt dies die Wirksamkeit des AVV im Übrigen nicht.

10.3 Jede Änderung dieses AVV bedarf der Schriftform, dies kann auch elektronisch erfolgen.

Festo
Datum: Klicken oder tippen Sie hier, um Text einzugeben.
Name: Klicken oder tippen Sie hier, um Text einzugeben.
Funktion: Klicken oder tippen Sie hier, um Text einzugeben.
Unterschrift:

Verantwortlicher
Datum: Klicken oder tippen Sie hier, um Text einzugeben.
Name: Klicken oder tippen Sie hier, um Text einzugeben.
Funktion: Klicken oder tippen Sie hier, um Text einzugeben.
Unterschrift:

Festo
Datum: Klicken oder tippen Sie hier, um Text einzugeben.
Name: Klicken oder tippen Sie hier, um Text einzugeben.
Funktion: Klicken oder tippen Sie hier, um Text einzugeben.

Verantwortlicher
Datum: Klicken oder tippen Sie hier, um Text einzugeben.
Name: Klicken oder tippen Sie hier, um Text einzugeben.
Funktion: Klicken oder tippen Sie hier, um Text einzugeben.

Unterschrift:	Unterschrift:

11 Übersicht Anlagen

Anlage	Inhalt
Anlage 1	Genehmigte Subunternehmer
Anlage 2	Technische und organisatorische Maßnahmen

Anlage 1: Weitere Auftragsverarbeiter

Vollständige Firmierung des weiteren Auftragsverarbeiters	Anschrift	Land	Beschreibung der Leistung
Microsoft Deutschland GmbH - Microsoft Azure West Europe	Walter-Gropius-Straße 5 80807 München	Deutsch-land	Azure Cloud Dienste ➢ Produktions-daten werden im Rechen-zentrum Amsterdam, NL, gehostet ➢ Backups werden im Rechen-zentrum Dublin, IRL, gehostet Anm.: Mit Microsoft ist über ein DPA sichergestellt, dass etwaige weitere Auftragsverarbeiter von MS auf die Einhaltung der Garantien aus Art. 46 DSGVO verpflichtet sind.
Festo-Didactic Ltd.	Rue du Carbone, Québec, QC G2N 2K7	Kanada	Entwicklung / Fehlerbehebung / dabei mögl. Zugriff auf Produktivdatenbank / Anm. zum Drittland: ➢ Kanada ist mit Angemessenheitsbe-schluss sicheres Drittland ➢ Festo-interne Binding Corporate Rules plus Konzern-Vertrag zur Verarbeitung personenbezogener Daten bestehen

Anlage 2: Gemäß Art. 32 DSGVO zu treffende technische und organisatorische Maßnahmen

Bearbeitungshinweis: Diese Anlage 2 ist von Festo ausgefüllt. Sie konkretisiert die von Festo ergriffenen technischen und organisatorischen Maßnahmen. Die Beurteilung des angemessenen Schutzniveaus obliegt dem Verantwortlichen.

Unter Berücksichtigung des
- Stands der Technik,
- der Implementierungskosten,
- 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

trifft Festo geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von bzw. unbefugten Zugang zu personenbezogene Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet werden.

Festo ergreift folgende Maßnahmen:

A. Zutrittskontrolle

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

Betriebsgelände:

☐ vollständige Einfriedung des Betriebsgeländes

☒ Personenkontrolle beim Pförtner / Empfang

☒ Protokollierung der Besucher

☒ Ausgabe von Besucherausweisen und Beaufsichtigung von Besuchern auf dem Betriebsgelände

☒ Wachschutz außerhalb der Büroöffnungszeiten

Gebäude:

☒ Separate Zutrittsbeschränkung in sensiblen Bereichen (Personalabteilung, IT-Abteilung, etc.).

Rechenzentrum:

☐ Vorliegen einer gültigen Zertifizierung des Rechenzentrumsbetriebs nach DIN ISO 27001

☐ abgeschlossener Raum, der gegen unbefugten Zutritt besonders abgesichert ist (z.B. Lamperts-Zelle)

☒ Zutrittskontrolle mit Protokollierung der Zutritte (z.B. Chipkarten, Videoüberwachung, biometrische Authentifizierung)

☒ Vorhandensein von Klimaanlage, Brandmeldeanlage und Alarmanlage

Sonstiges / Spezifizierung der o.g. Maßnahmen: Klicken oder tippen Sie hier, um Text einzugeben.

B. Zugangskontrolle

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

Zugang von Intern:

- ☒ Dokumentierte Zuordnung von Benutzerrechten mittels Benutzername und Passwort
- ☒ Neuanlage und Sperrung von Benutzern anhand eines dokumentierten Prozesses
- ☒ Passwortsicherheitskonzept (mindestens 12 Zeichen und regelmäßige Änderung)
- ☒ Erzwungene Sperrung von Workstations nach wenigen Minuten
- ☐ Einsatz von Intrusion-Detection-Systemen
- ☒ Ordnungsgemäße Vernichtung von Datenträgern und Dokumenten (DIN 66399)

Zugang von Extern:

- ☒ Einsatz von VPN-Technologie mittels 2-Faktor-Authentifizierung
- ☒ Verschlüsselung von mobilen Datenträgern
- ☒ Verschlüsselung von Datenträgern in Laptops / Notebooks
- ☒ Einsatz einer Hard- und Software-Firewall
- ☒ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
- ☒ Einwahlversuche ins Netzwerk werden protokolliert.
- ☒ Sperrung des Benutzerkontos nach festgelegter Anzahl von Fehlversuchen.

Sonstiges / Spezifizierung der o.g. Maßnahmen: Klicken oder tippen Sie hier, um Text einzugeben.

C. 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.

- ☒ Vorliegen eines dokumentierten Berechtigungskonzepts
- ☒ Vergabe und Entzug von Berechtigungen anhand eines dokumentierten Prozesses
- ☒ Verwaltung der Rechte durch Systemadministrator
- ☒ Anzahl der Administratoren auf das „Notwendigste“ reduziert
- ☒ Protokollierung aller Anmeldungen am System
- ☐ Sonstiges / Spezifizierung der o.g. Maßnahmen: Klicken oder tippen Sie hier, um Text einzugeben.

D. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

☒ Zugriffe auf die Systeme von Festo von außen durch eigene Mitarbeiter müssen vor unbefugtem Zugriff besonders abgesichert werden (Standleitungen oder VPN-Tunnel)
☒ Die Weitergabe personenbezogener Daten an Dritte darf nur nach expliziter Genehmigung durch den Verantwortlichen erfolgen. Soweit möglich, erfolgt die Weitergabe nur in anonymisierter oder pseudonymisierter Form.
☒ Der Austausch personenbezogener Daten zwischen Verantwortlichem und Festo darf nur mittels verschlüsselter Verbindungen erfolgen (Austauschportale, E-Mail-Verschlüsselung).
☒ Vollständige Protokollierung aller Abruf- und Übermittlungsvorgänge
☒ Verschlüsselung von mobilen Datenträgern
☒ Verschlüsselung von Datenträgern in Laptops / Notebooks
☒ Beim physischen Transport: sichere Transportbehälter/-verpackungen
☒ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen in Abstimmung mit dem Verantwortlichen
☐ Sonstiges / Spezifizierung der o.g. Maßnahmen: Klicken oder tippen Sie hier, um Text einzugeben.

E. 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.

☒ Revisionssichere und nutzerbezogene Protokollierung der Verarbeitung (Eingabe, Änderung und Löschung) von der Auftragsdatenverarbeitung betroffenen Daten
☒ Protokollierung der administrativen Zugriffe
☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
☐ Sonstiges / Spezifizierung der o.g. Maßnahmen: Klicken oder tippen Sie hier, um Text einzugeben.

F. Auftragskontrolle

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

☐ Vertrag zur Auftragsverarbeitung gemäß Art. 28 III EU-DSGVO mit Regelungen zu den Rechten und Pflichten von Festo und des Verantwortlichen
☐ Prozess zur Erteilung und / oder Befolgung von Weisungen
☒ Bestimmung von Ansprechpartnern und / oder verantwortlichen Mitarbeitern
☐ Kontrolle / Überprüfung weisungsgebundener Auftragsdurchführung
☒ Schulungen / Einweisung aller zugriffsberechtigten Mitarbeiter bei Festo
☐ Unabhängige Auditierung der Weisungsgebundenheit
☒ Verpflichtung der Mitarbeiter zur Vertraulichkeit
☐ Vereinbarung von Konventionalstrafen für Verstöße gegen Weisungen
☒ Sorgfältige Auswahl weiterer Auftragsverarbeiter, Einholung Zustimmung des Verantwortlichen, Übertragung der Pflichten von Festo an den weiteren Auftragsverarbeiter

☐ Sonstiges / Spezifizierung der o.g. Maßnahmen: Klicken oder tippen Sie hier, um Text einzugeben.

G. Verfügbarkeitskontrolle

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

☐ Vorliegen einer gültigen Zertifizierung des Rechenzentrumsbetriebs nach DIN ISO 27001

☒ Verfügbarkeit der auftragsbezogenen Anwendung über ein Spiegelrechenzentrum, so dass eine umgehende Ausfallsicherheit gewährleistet ist

☐ Dokumentiertes und gelebtes Desaster-Recovery und Backup-Konzept, sowie regelmäßige Tests von Datenwiederherstellungen, sowie ein dokumentierter Notfallplan

☒ Grundlegende Ausstattung der IT-Anlage (unterbrechungsfreie Stromversorgung (USV), Klimaanlage in Serverräumen, Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen, Feuer- und Rauchmeldeanlagen, Feuerlöschgeräte in Serverräumen,

☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

☐ Sonstiges / Spezifizierung der o.g. Maßnahmen: Klicken oder tippen Sie hier, um Text einzugeben.

H. Trennungsgebot

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

☒ Physikalische Trennung der auftragsbezogenen Daten (selbständiger physischer Server)

☒ Trennung von Produktiv- und Testsystem

☒ Ein Berechtigungskonzept regelt den Zugriff der Mitarbeiter auf die gespeicherten Kundendaten. Es wird sichergestellt, dass jeder Mitarbeiter nur auf Daten des Mandanten zugreifen kann, die er im Rahmen seiner Tätigkeit benötigt.

☐ Sonstiges / Spezifizierung der o.g. Maßnahmen: Klicken oder tippen Sie hier, um Text einzugeben.

I. Verfahren zur regelmäßigen Überprüfung

Maßnahmen, die gewährleisten, dass die oben genannten technischen und organisatorischen Maßnahmen regelmäßig auf Wirksamkeit und Stand der Technik überprüft werden.

☒ Verfahren für regelmäßige Kontrollen / Zyklische Audits (WP, ISAE, etc.)

☒ Sicherheits-Zertifizierungen nach ISO 27001, ISO/IEC 62443 o.ä.

☐ Zertifizierungen zur Sicherheit der Verarbeitung personenbezogener Daten, z.B.: ISO 27018, ISO 29100

☒ Externe technische Sicherheitsüberprüfungen (Penetrationstests) sowie RED Team Übungen

☐ K-Fall Übungen

☐ Sonstiges / Spezifizierung der o.g. Maßnahmen: Klicken oder tippen Sie hier, um Text einzugeben.