Vereinbarung Auftragsverarbeitung

Diese Vereinbarung Auftragsverarbeitung regelt die Datenverarbeitung im Auftrag des Auftraggebers durch die symestic GmbH, Gewerbestraße 10-12, 69221 Dossenheim als Auftragnehmer.

Sie ist Teil des Hauptvertrages über die Zurverfügungstellung der SYMESTIC SaaS Lösung an den im jeweiligen Auftrag genannten Auftraggeber. Sie wird durch Bezugnahme in den AGB-Bestandteil des jeweiligen Vertrages.

1. Allgemeines
    a. Der Auftragnehmer stellt eine Softwareplattform zur Verfügung, um Produktionsprozesse in produzierenden Unternehmen digital abzubilden und mit bestehenden IT-Systemen zu verbinden. Die Parteien haben einen Vertrag geschlossen, der die Verarbeitung von personenbezogenen Daten im Auftrag durch den Auftragnehmer beinhaltet („Hauptvertrag“).
    b. Diese Vereinbarung Auftragsverarbeitung („AVV“) konkretisiert, als Teil des Hauptvertrages, die Verpflichtungen beider Parteien zur Einhaltung des anwendbaren Datenschutzrechts, insbesondere der Anforderungen der EU-Datenschutz-Grundverordnung („DSGVO“).

2. Anwendungsbereich
   Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind im Hauptvertrag und in Anlage 1 festgelegt. Die Laufzeit dieser AVV richtet sich nach der Laufzeit des Hauptvertrages.

3. Weisungsgebundenheit
    a. Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der dokumentierten Weisungen des Auftraggebers verarbeiten. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in Textform geändert, ergänzt oder ersetzt werden. Mündliche Weisungen sind vom Auftraggeber unverzüglich in Textform zu bestätigen.
    b. Falls der Auftragnehmer verpflichtet ist, personenbezogene Daten nach dem Recht der Union oder des Mitgliedstaates, dem der Auftragnehmer unterliegt, zu verarbeiten, wird der Auftragnehmer den Auftraggeber hierüber vor der jeweiligen Verarbeitung schriftlich informieren, es sei denn, das Gesetz verbietet solche Informationen aus wichtigen Gründen des öffentlichen Interesses. Im letztgenannten Fall wird der Auftragnehmer den Verantwortlichen unverzüglich informieren, sobald ihm dies rechtlich möglich ist.

c. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung so lange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

4. Technische und organisatorische Maßnahmen
   a. Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anwendbaren Datenschutzvorschriften erforderlich sind. Dies umfasst insbesondere die Anforderungen des Art. 32 DSGVO.

      Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist in Anlage 2 dokumentiert.

   b. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können.
      Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten. Der Auftragnehmer ist berechtigt, die Maßnahmen zu ändern oder durch gleichwertige oder wirksamere Maßnahmen zu ersetzen, sofern das vertraglich vereinbarte Schutzniveau hierdurch nicht unterschritten wird.
      Über wesentliche Änderungen der technischen und organisatorischen Maßnahmen, die das vereinbarte Schutzniveau oder die Sicherheit der Verarbeitung personenbezogener Daten erheblich betreffen, informiert der Auftragnehmer den Auftraggeber in angemessener Weise.
      Der Auftraggeber kann jederzeit eine aktuelle Übersicht, der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

5. Betroffenenrechte
   a. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO (insb. Auskunft, Berichtigung, Sperrung oder Löschung). Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.
   b. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

6. Sonstige Pflichten des Auftragnehmers

a. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, spätestens innerhalb von 48 Stunden, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.
b. Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie erforderlichenfalls bei Durchführung einer Datenschutzfolgenabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind dem Auftraggeber auf Anforderung unverzüglich zur Verfügung zu stellen.
c. Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Recht geltend, verpflichtet sich der Auftragnehmer, den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.
d. Die beim Auftragnehmer zur Verarbeitung eingesetzten Personen haben sich schriftlich zur Vertraulichkeit verpflichtet, wurden mit den relevanten Bestimmungen des Datenschutzes vertraut gemacht und werden hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht.
e. Der Auftragnehmer wird den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten unterstützen.
f. Der Auftraggeber kann sich bei Fragen zum Datenschutz beim Auftragnehmer jederzeit an der Datenschutzbeauftragten des Auftragnehmers wenden. Datenschutzbeauftragter des Auftragnehmers ist Wolfgang Knobloch, Tel. +49 6221 7 26 53-200, E-Mail privacy@symestic.com.

7. Rechte und Pflichten des Auftraggebers
   a. Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.
   b. Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer, soweit erforderlich und möglich, Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind. Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt.

8. Unterauftragnehmer
    a. Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist nur mit Zustimmung des Auftraggebers zulässig.
    b. Der Auftraggeber stimmt der Beauftragung von Unterauftragnehmern gemäß der Übersicht Unterauftragsverarbeiter, anbei als Anlage 3, zu. In der Übersicht Unterauftragsverarbeiter ist auch der Prozess für zukünftige Änderungen der Unterauftragsverarbeiter definiert.
    c. Der Auftragnehmer hat die Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass diese die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten können. Der Auftragnehmer hat insbesondere zu kontrollieren, dass sämtliche Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen haben.
    d. Nicht als Unterauftragsverhältnisse im Sinne diese AVV sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen und Bewachungsdienste.
    e. Die Beauftragung von Unterauftragsverarbeitern lässt die vertraglichen und datenschutzrechtlichen Verpflichtungen des Auftragnehmers gegenüber dem Auftraggeber unberührt. Der Auftragnehmer haftet für eventuelle Schlechtleistungen eines Unterauftragsverarbeiters wie für eigenes Verschulden.

9. Datenübermittlung in Drittländer
   Die Auftragsverarbeitung kann auch in Drittländern stattfinden. Die Übermittlung personenbezogener Daten an ein Drittland durch den Auftragnehmer erfolgt dabei auf Basis eines Angemessenheitsbeschlusses gem. Art. 45 DSGVO und/oder auf Basis geeigneter Garantien gem. Art. 46 DSGVO (z.B. den von der Kommission erlassenen Standardvertragsklauseln, die zwischen Auftragnehmer und Unterauftragnehmern in Drittländern abgeschlossen wurden).

10. Löschung und Rückgabe von personenbezogenen Daten
    a. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
    b. Nach Beendigung des Hauptvertrages oder früher nach Aufforderung durch den Auftraggeber hat der Auftragnehmer die im Auftrag verarbeiteten personenbezogenen Daten dem Auftraggeber auszuhändigen oder datenschutzgerecht zu löschen.
    c. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den

Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

11. Trennungskonzept nach Beendigung des Vertrags
    a. Nach Beendigung des Vertragsverhältnisses werden auf Verlangen des Auftraggebers alle vom Auftragnehmer gespeicherten Anwendungsdaten im Standardformat ohne zusätzliche Kosten oder Aufwendungen zur Verfügung gestellt. Auf Wunsch des Auftraggebers können alle gespeicherten Daten im Standardformat auch durch den Auftragnehmer an einen Dritten übergeben werden. Der Auftraggeber ist verpflichtet alle hierfür anfallenden und schriftlich nachzuweisenden notwendigen Kosten zu erstatten.
    b. Auf Verlangen wird der Auftragnehmer, mit einem vom Auftraggeber benannten Dritten zusammenzuarbeiten, um das Vertragsverhältnis innerhalb eines festzulegenden Zeitraums und nach rechtmäßiger Beendigung dieser Vereinbarung abzuschließen. Die Zusammenarbeit ist beschränkt auf:
        i. Übertragung der von SYMESTIC gespeicherten Anwendungsdaten.
        ii. Übermittlung sonstiger den Kunden betreffender Daten, soweit diese nicht Geschäftsgeheimnisse der symestic GmbH betreffen.
        iii. Unterrichtung der bestellten Mitarbeiter des Dritten über Sachverhalte.

        Diese Mitwirkung ist gesondert zu vergüten. Die Vergütung erfolgt auf der Grundlage der zum Zeitpunkt der Beendigung des Vertrags gültigen Listenpreise der symestic GmbH.
    c. Auf Anfrage des Auftraggebers wird der Auftragnehmer den erforderlichen Nachweis erbringen, dass die Daten des Auftraggebers vollständig aus der dem Kunden zugeordneten Datenbank und der Anwendungsdaten gelöscht wurden.

12. Schlussbestimmungen
    a. Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.
    b. Für Nebenabreden ist die Schriftform erforderlich. Sollten einzelne Teile dieser AVV unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen der AVV nicht.

Anlage 1: Beschreibung der Auftragsverarbeitung

Verantwortlicher

Der Auftraggeber ist Verantwortlicher und nutzt die SYMESTIC SaaS Lösung des Auftragnehmers, um seine Produktionsprozesse digital abzubilden, mit bestehenden IT-Systemen zu verbinden und Analysen der Arbeitsprozesse durchzuführen.

Auftragsverarbeiter

Der Auftragnehmer stellt als Auftragsverarbeiter eine Softwareplattform zur Verfügung, mit der der Auftraggeber Produktionsprozesse digital abbildet und Analysen seiner Arbeitsprozesse durchführt.

Betroffene Personen

Die im Auftrag verarbeiteten personenbezogenen Daten betreffen folgende Kategorien betroffener Personen:

- Nutzer der SYMESTIC SaaS Lösung (regelmäßig Mitarbeiter des Auftraggebers, die im Rahmen ihrer Tätigkeit auf die SYMESTIC SaaS Lösung zugreifen)

Kategorien von Daten

Die im Auftrag verarbeiteten personenbezogenen Daten gehören zu folgenden Datenkategorien:

- Benutzername;
- Passwort;
- Name und Vorname;
- E-Mail-Adresse;
- Bevorzugte Sprache;
- Daten zur Nutzung der Softwareplattform (z.B. Eingabewerte oder Zeitstempel bei der Nutzung von Fertigungssteuerung, Produktionskennzahlen, Prozessdaten, Alarme und Daten zur Bearbeitung von Aufgaben/Tasks);
- sonstige Daten, die dem Auftragnehmer vom Auftraggeber für die Durchführung seiner Leistungen zur Verfügung gestellt werden bzw. die im Rahmen der Durchführung der Leistungen des Auftragnehmers vom Auftragnehmer für den Auftraggeber erhoben werden.

Besondere Datenkategorien

Die im Auftrag verarbeiteten personenbezogenen Daten umfassen regelmäßig keine besonderen Kategorien personenbezogener Daten gem. Art. 9 DSGVO (z.B. Gesundheitsdaten), es sei denn, es werden dem Auftragnehmer solche besonderen Kategorien personenbezogener Daten vom Auftraggeber für die Durchführung der Leistungen des Auftragnehmers zur Verfügung gestellt bzw. vom Auftragnehmer im Rahmen der Durchführung seiner Leistungen auf Weisung und im Auftrag des Auftraggebers erhoben. Gegenstand und Dauer der Verarbeitung Die im Auftrag verarbeiteten personenbezogenen Daten werden verarbeitet zur Durchführung der im Hauptvertrag vereinbarten Leistungen des Auftragnehmers. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.

Anlage 2: Technische und organisatorische Maßnahmen

Beim Auftragnehmer sind nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO getroffen worden:

1. VERTRAULICHKEIT

   a. Zutrittskontrolle
   Das Hosting der SYMESTIC SaaS Lösung erfolgt in einem Rechenzentrum von Microsoft Azure in der EU. Eine ausführliche Dokumentation der von Microsoft Azure getroffenen technischen und organisatorischen Maßnahmen der Datensicherheit und der Zertifizierungen von Microsoft Azure aus dem Bereich der Informationssicherheit (einschließlich ISO 27001) findet sich hier: https://learn.microsoft.com/de-de/azure/security/fundamentals/overview

   Die Büroräume des Auftragnehmers befinden sich in einem Bürohaus in Dossenheim. Die Zugänge zum Bürohaus des Auftragnehmers sind Tag und Nacht verschlossen. Zugang zum Bürohaus haben nur der Mitarbeiter zudem haben Gäste Zutritt, die sich jedoch zuvor am Empfang anmelden müssen. Im Bürohaus kommt ein elektronisches Schließsystem zum Einsatz, das vom Auftragnehmer verwaltet wird. Die Schlüsselvergabe und das Schlüsselmanagement erfolgt nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug von Zutrittsberechtigungen für Räume regelt.
   Zutrittsberechtigungen werden einem Beschäftigten erst erteilt, wenn dies durch den jeweiligen Vorgesetzten angefordert wurde. Bei der Vergabe von Berechtigungen wird dem Grundsatz der Erforderlichkeit Rechnung getragen.
   Besucher dürfen sich nicht ohne Begleitung in den Büroräumen frei bewegen.

   b. Zugangskontrolle
   Um Zugang zu IT-Systemen zu erhalten, müssen Nutzer über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzerberechtigungen von Administratoren vergeben. Dies jedoch nur, wenn dies von dem jeweiligen Vorgesetzten beantragt wurde.
   Der Benutzer erhält dann einen Benutzernamen und ein Initialpasswort, das bei erster Anmeldung geändert werden muss. Die Passwortvorgaben beinhalten eine Mindestpasswortlänge von 8 Zeichen, wobei das Passwort auf Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen bestehen muss. Fehlerhafte Anmeldeversuche werden protokolliert. Bei 3-maliger Fehleingabe erfolgt eine kurzzeitige Sperrung der Anmeldemaske.
   Remote-Zugriffe auf IT-Systeme des Auftragnehmers erfolgen stets über verschlüsselte Verbindungen.
   Auf den Servern des Auftragnehmers ist ein Intrusion-Prevention-System im Einsatz. Alle Server- und Client Systeme verfügen über

Virenschutzsoftware, bei der eine tagesaktuelle Versorgung mit Signaturupdates gewährleistet ist.
Alle Server sind durch Firewalls geschützt, die stets gewartet und mit Updates und Patches versorgt werden.
Der Zugriff von Servern und Clients auf das Internet und der Zugriff auf diese Systeme über das Internet ist ebenfalls durch Firewalls gesichert. So ist auch gewährleistet, dass nur die für die jeweilige Kommunikation erforderlichen Ports nutzbar sind. Alle anderen Ports sind entsprechend gesperrt.
Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen. Passwörter werden grundsätzlich verschlüsselt gespeichert.

c. Zugriffskontrolle
Berechtigungen für IT-Systeme und Applikationen des Auftragnehmers werden ausschließlich von Administratoren eingerichtet.
Berechtigungen werden grundsätzlich nach dem Need-to-Know-Prinzip vergeben. Es erhalten demnach nur die Personen Zugriffsrechte auf Daten, Datenbanken oder Applikationen, die diese Daten, Anwendungen oder Datenbanken warten und pflegen bzw. in der Entwicklung tätig sind. Voraussetzung ist eine entsprechende Anforderung der Berechtigung für einen Mitarbeiter durch einen Vorgesetzten.
Es gibt ein rollenbasiertes Berechtigungskonzept mit der Möglichkeit der differenzierten Vergabe von Zugriffsberechtigungen, das sicherstellt, dass Beschäftigte abhängig von ihrem jeweiligen Aufgabengebiet und ggf. projektbasiert Zugriffsrechte auf Applikationen und Daten erhalten.
Alle Mitarbeiter des Auftragnehmers sind angewiesen, Informationen mit personenbezogenen Daten und/oder Informationen über Projekte in die hierfür ausgewiesenen Vernichtungsbehältnisse einzuwerfen.
Beschäftigten ist es grundsätzlich untersagt, nicht genehmigte Software auf den IT-Systemen zu installieren.
Alle Server- und Client-Systeme werden regelmäßig mit Sicherheits-Updates aktualisiert.

d. Trennung
Alle vom Auftragnehmer für Kunden eingesetzten IT-Systeme sind mandantenfähig. Die Trennung von Daten von verschiedenen Kunden ist stets gewährleistet.

e. Pseudonymisierung & Verschlüsselung
Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen.
Darüber hinaus werden Daten auf Server- und Clientsystemen auf verschlüsselten Datenträgern gespeichert. Es befinden sich entsprechende Festplattenverschlüsselungssysteme im Einsatz.

2. INTEGRITÄT

a. Eingabekontrolle
Die Eingabe, Änderung und Löschung von personenbezogenen Daten, die vom Auftragnehmer im Auftrag verarbeitet werden, werden mit Zeitstempel und Nutzeraccount protokolliert oder das letzte Ereignis festgehalten. Bspw.: “Auftrag zuletzt aktualisieret am AB von XY”.
Mitarbeiter sind verpflichtet, stets mit ihren eigenen Accounts zu arbeiten. Benutzeraccounts dürfen nicht mit anderen Personen geteilt bzw. gemeinsam genutzt werden.

b. Weitergabekontrolle
Eine Weitergabe von personenbezogenen Daten, die vom Auftragnehmer im Auftrag von Kunden erfolgt, darf jeweils nur in dem Umfang, wie erfolgen, wie dies mit dem Kunden abgestimmt und soweit dies zur Erbringung der vertraglichen Leistungen für den Kunden erforderlich ist.
Alle Mitarbeiter, die in einem Kundenprojekt arbeiten, werden im Hinblick auf die zulässige Nutzung von Daten und die Modalitäten einer Weitergabe von Daten instruiert.
Soweit möglich werden Daten verschlüsselt an Empfänger übertragen.
Die Nutzung von privaten Datenträgern ist den Beschäftigten des Auftragnehmers im Zusammenhang mit Kundenprojekten untersagt.
Alle Mitarbeiter des Auftragnehmers werden regelmäßig zu Datenschutzthemen geschult. Alle Mitarbeiter sind auf zu einem vertraulichen Umgang mit personenbezogenen Daten verpflichtet worden.

3. VERFÜGBARKEIT UND BELASTBARKEIT
Daten auf Serversystemen des Auftragnehmers werden mindestens täglich inkrementell und wöchentlich „voll“ gesichert. Die Sicherungsmedien sind verschlüsselt.
Das Einspielen von Backups wird regelmäßig getestet.
Die IT-Systeme verfügen über eine unterbrechungsfreie Stromversorgung. Im Serverraum befindet sich eine Brandmeldeanlage sowie eine CO2-Löschanlage.
Alle Serversysteme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst.
Der Auftragnehmer hat einen Notfallplan implementiert, der auch einen Business Continuity Prozess und Wiederanlaufplan beinhaltet.

4. AUFTRAGSKONTROLLE
Beim Auftragnehmer ist ein betrieblicher Datenschutzbeauftragter benannt. Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben jeweils anzuwendenden Datenschutzrechts ein Auftragsverarbeitungsvertrag nach zuvor durchgeführtem Audit durch den Datenschutzbeauftragten des Auftragnehmers abgeschlossen. Auftragnehmer werden auch während des Vertragsverhältnisses regelmäßig kontrolliert.

5. PRIVACY BY DESIGN UND PRIVACY BY DEFAULT
Es wird schon bei der Entwicklung der Software sorge dafür getragen, dass dem Grundsatz der Erforderlichkeit schon im Zusammenhang mit Benutzer-Interfaces

Rechnung getragen wird. So sind z.B. Formularfelder, Bildschirmmasken flexibel gestaltbar. So können Pflichtfelder vorgesehen oder Felder deaktiviert werden.

6. VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

   Der Auftragnehmer hat ein umfassendes Datenschutzmanagementsystem implementiert. Es gibt eine Leitlinie zu Datenschutz und Datensicherheit und Richtlinien, mit denen die Umsetzung der Ziele der Leitlinie gewährleistet wird.
   Es ist Datenschutz- und Informationssicherheits-Team (DST) eingerichtet, das Maßnahmen im Bereich von Datenschutz und Datensicherheit plant, umsetzt, evaluiert und Anpassungen vornimmt.
   Die Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst.
   Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich dem Datenschutz- und Informationssicherheits-Team (DST) gemeldet werden. Dieses wird den Vorfall sofort untersuchen. Soweit Daten betroffen sind, die im Auftrag von Kunden verarbeitet werden, wird Sorge dafür getragen, dass diese unverzüglich über Art und Umfang des Vorfalls informiert werden.
   Bei der Verarbeitung von Daten für eigene Zwecke wird im Falle des Vorliegens der Voraussetzungen des Art. 33 DSGVO eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Kenntnis von dem Vorfall erfolgen.

Anlage 3: Übersicht Unterauftragsverarbeiter

Der Auftragnehmer setzt bei der Erbringung der Leistungen aus dem Hauptvertrag folgende Unterauftragsverarbeiter ein:

Unterauftragsverarbeiter	Leistungen des Unterauftragsverarbeiter	Ort der Daten-verarbeitung	Geeignete Garantien (Art. 46 DSGVO)
Microsoft Deutschland GmbH, Deutschland	Hosting der SYMESTIC SaaS Lösung („Azure“)	EU	EU-Standardvertragsklauseln (Standard Contractual Clauses – SCC), ergänzt durch das Microsoft Data Protection Addendum (DPA) und technische Zusatzmaßnahmen (z. B. EU Data Boundary, Verschlüsselung).
HubSpot	Support-Ticketsystem und Knowledge-Base-Zugang (Anlage 2): Kontakt- und Zugangsdaten der benannten Key-User sowie Ticketinhalte, soweit diese personenbezogene Daten enthalten	EU	EU-US Data Privacy Framework (DPF) (Zertifizierung von HubSpot, Inc. aktiv) in Kombination mit den EU-Standardvertragsklauseln (Standard Contractual Clauses – SCC) gemäß Art. 46 Abs. 2 lit. c DSGVO, die im HubSpot Data Processing Agreement (DPA) standardmäßig verankert sind. Flankiert von technischer EU-Datenresidenz (Speicherung in Westeuropa).
Benachrichtigungsdienst E-Mail/SMS: Deutsche Telekom (Infrastruktur), Microsoft (Applikation)	Versand von System-, Ticket- und Alarm-Benachrichtigungen	EU	EU-US Data Privacy Framework (DPF) / Angemessenheitsbeschluss (Art. 45 DSGVO) als primäre Grundlage für Microsoft; flankiert von EU-Standardvertragsklauseln (SCC) gemäß Art. 46 Abs. 2 lit. c DSGVO für die Applikationsebene.

Der Auftragnehmer kann die Beauftragung einzelner Unterauftragsverarbeiter beenden oder zusätzliche Unterauftragsverarbeiter beauftragen. Der Auftragnehmer wird den Auftraggeber bei der Beauftragung zusätzlicher Unterauftragsverarbeiter auf elektronischem Wege mindestens 30 Tage vor Einsatz des zusätzlichen Unterauftragsverarbeiters über dessen geplanten Einsatz informieren. Ausgenommen hiervon sind Notfallersetzungen wie weiter unten definiert. Sollte der Auftraggeber einen wesentlichen Grund haben, dem Einsatz eines Unterauftragsverarbeiters zu widersprechen, wird der Auftraggeber dies dem Auftragnehmer spätestens 15 Tage nach der Information über den geplanten Einsatz des Unterauftragsverarbeiters schriftlich und unter Nennung des wesentlichen Grundes mitteilen. Sollte der Auftraggeber innerhalb dieser Zeitspanne nicht widersprechen, so wird der Einsatz des zusätzlichen Unterauftragsverarbeiters als vom Auftraggeber genehmigt angesehen.
Sollte der Auftraggeber widersprechen, kann der Auftragnehmer den Widerspruch wie folgt heilen: (1.) Der Auftragnehmer wird den zusätzlichen Unterauftragsverarbeiter für die Verarbeitung personenbezogener Daten des Auftraggebers nicht einsetzen, oder (2.)

der Auftragnehmer wird Maßnahmen ergreifen, um den wesentlichen Grund für den Widerspruch des Auftraggebers auszuräumen, oder (3.) der Auftragnehmer kann die Erbringung des von dem Einsatz des zusätzlichen Unterauftragsverarbeiters betroffenen Aspekts der Leistung gegenüber dem Auftraggeber vorübergehend oder dauerhaft einstellen und dem Auftraggeber die für die Erbringung des Aspekts der Leistung eventuell bereits vorab gezahlte Vergütung zurückerstatten. Sollte keine dieser drei Optionen machbar sein und wurde dem Widerspruch nicht innerhalb von 15 Tagen nach Zugang des Widerspruchs abgeholfen, kann jede Partei den Vertrag mit angemessener Frist außerordentlich kündigen.
Notfallersetzungen eines Unterauftragsverarbeiters können erforderlich werden, wenn die Erforderlichkeit des sofortigen Einsatzes eines zusätzlichen Unterauftragsverarbeiters außerhalb der Kontrolle des Auftragnehmers liegt, beispielsweise wenn ein Unterauftragsverarbeiter überraschend den Geschäftsbetrieb einstellt oder seine wesentlichen Vertragspflichten gegenüber dem Auftragnehmer verletzt, so dass es dem Auftragnehmer nicht mehr möglich ist/wäre, die gegenüber dem Auftraggeber geschuldete Leistung zu erbringen. In einem solchen Fall wird der Auftragnehmer den Kunden unverzüglich über den zusätzlichen Unterauftragsverarbeiter informieren und der Widerspruchsprozess, wie oben definiert, wird mit der Information des Auftraggebers eingeleitet.