

Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Präambel

Zwischen dem Verantwortlichen (=Mieter oder Kunde) und dem Auftragsverarbeiter (=Gödde) besteht ein Auftragsverhältnis im Sinne des § 28 der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, „DSGVO“).

Dieser Auftragsverarbeitungsvertrag einschließlich aller Anlagen (nachfolgend gemeinsam als „**Vereinbarung**“ bezeichnet) konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien aus dem zugrundeliegenden Vertrag, der Leistungsvereinbarung und/oder Auftragsbeschreibung einschließlich aller Anlagen (nachfolgend gemeinsam als „**Hauptvertrag**“ bezeichnet). Sofern Bezug auf die Regelungen des Bundesdatenschutzgesetzes (nachfolgend „BDSG“) genommen wird, so ist damit das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 in der zum Zeitpunkt ab dem 25. Mai 2018 geltenden Fassung gemeint. Wird Bezug auf die Regelungen des Bundesdatenschutzgesetzes-alt („BDSG-alt“) genommen, so ist damit das Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66) gemeint.

Der Auftragsverarbeiter verpflichtet sich gegenüber dem Verantwortlichen zur Erfüllung des Hauptvertrages und dieser Vereinbarung nach Maßgabe der folgenden Bestimmungen:

§ 1 Anwendungsbereich und Begriffsbestimmungen

1. Die nachfolgenden Bestimmungen finden Anwendung auf alle Leistungen der Auftragsverarbeitung im Sinne des § 28 DSGVO, die der Auftragsverarbeiter auf Grundlage des Hauptvertrages gegenüber dem Verantwortlichen erbringt.
2. Sofern in dieser Vereinbarung der Begriff „Datenverarbeitung“ oder „Verarbeitung“ von Daten benutzt wird, ist darunter allgemein die Verwendung von personenbezogenen Daten zu verstehen. Datenverarbeitung oder das Verarbeiten von Daten bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.
3. Auf die weiteren Begriffsbestimmungen in § 4 DSGVO wird verwiesen.

§ 2 Gegenstand und Dauer der Datenverarbeitung

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag und nach Weisung des Verantwortlichen.
2. Gegenstand des Auftrags ist die Bereitstellung der Software „Connected Manufacturing“ im Rahmen des mit dem Auftragsverarbeiter vereinbarten Umfangs, gemäß dem Hauptvertrag.
3. Die Dauer dieser Vereinbarung entspricht der Laufzeit des Hauptvertrages.

§ 3 Art und Zweck der Datenverarbeitung

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter ergeben sich aus dem Hauptvertrag. Neben diesen werden die Daten insbesondere zu folgenden Zwecken verarbeitet:

- Durchführung von Fernwartung und Support

- Einpflege von Daten (Artikelstammdaten, Mitarbeiterdaten, Kostenstellen) in das System zur Vorbereitung der Inbetriebnahme oder im Zuge von Supportarbeiten
- Einrichtung von Schnittstellen und Installation der notwendigen Software
- Wiederaufspielen von Datensicherungen und Durchführung von etwaigen Datenanalysen zur Problemlösung von Hard- und Software im Rahmen des Kunden-Supports
- Durchführung von Software-Schulungen
- Weiterentwicklung der Software (z.B. Empfehlungssystem für die Nutzer) mittels Auswertung von Nutzeraktivitäten im System

§ 4 Kategorien betroffener Personen

Die Kategorien der durch den Umgang mit den personenbezogenen Daten im Rahmen dieser Vereinbarung betroffenen Personen umfasst:

- Kunden/Bestandskunden
- Mitarbeiter (Stammebelegschaft, Auszubildende, Leiharbeiter, freie Mitarbeiter) des Verantwortlichen

§ 5 Art der personenbezogenen Daten

Von der Auftragsverarbeitung sind folgende Datenarten betroffen:

- Personenstammdaten (Name, Anrede, Titel/akademischer Grad, Geburtsdatum)
- Elektronische Kommunikationsdaten (IP-Adresse, aufgerufene Internetseiten, Angaben zum verwendeten Endgerät, Betriebssystem und Browser)
- Login Daten (Benutzerkennung, E-Mailadresse)
- Protokolldaten (Änderungsnachverfolgung)

Weitere Datenarten, die mittelbare Bezüge zu personenbezogenen Daten haben können und verarbeitet werden, sind:

- Werkzeugnutzungsdaten (Einsatzzeiten, Standzeiten, Verschleißdaten, Bestandsdaten etc.)
- Werkzeugstammdaten (kundenspezifische Werkzeugparameter, Stammdaten aus Werkzeugimporten etc.)
- Fertigungsdaten (Maschineneinschaltzeiten, Stillstandzeiten, Schnittdaten etc.)
- Auftragsdaten (Auftragsdaten, Qualitätsdaten, Bauteildaten, Positionsdaten etc.)

§ 6 Rechte und Pflichten des Verantwortlichen

1. Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie zur Wahrung der Rechte der Betroffenen ist allein der Verantwortliche zuständig und somit für die Verarbeitung Verantwortlicher im Sinne des § 4 Nr.7 DSGVO.
2. Der Verantwortliche ist berechtigt, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Mündliche Weisungen wird der Verantwortliche unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen.
3. Soweit es der Verantwortliche für erforderlich hält, können weisungsberechtigte Personen benannt werden. Diese wird der Verantwortliche dem Auftragsverarbeiter schriftlich oder in Textform mitteilen. Für den Fall, dass sich diese weisungsberechtigten Personen bei dem Verantwortlichen ändern, wird dies dem Auftragsverarbeiter unter Benennung der jeweils neuen Person schriftlich oder in Textform mitgeteilt.

4. Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter festgestellt werden.

§ 7 Pflichten des Auftragsverarbeiters

1. Datenverarbeitung

- a. Der Auftragsverarbeiter wird personenbezogene Daten ausschließlich nach Maßgabe dieser Vereinbarung und/oder des zugrundeliegenden Hauptvertrages sowie nach den Weisungen des Verantwortlichen verarbeiten.

2. Betroffenenrechte

- a. Der Auftragsverarbeiter wird den Verantwortlichen bei der Erfüllung der Rechte der Betroffenen, insbesondere im Hinblick auf Berichtigung, Einschränkung der Verarbeitung und Löschung, Benachrichtigung und Auskunftserteilung, im Rahmen seiner Möglichkeiten unterstützen. Sollte der Auftragsverarbeiter die in § 5 dieser Vereinbarung genannten personenbezogenen Daten im Auftrag des Verantwortlichen verarbeiten und sind diese Daten Gegenstand eines Verlangens auf Datenportabilität gem. Art. 20 DSGVO, wird der Auftragsverarbeiter dem Verantwortlichen den betreffenden Datensatz innerhalb einer angemessen gesetzten Frist, im Übrigen innerhalb von sieben Arbeitstagen, in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung stellen.
- b. Der Auftragsverarbeiter hat auf Weisung des Verantwortlichen die in § 5 dieser Vereinbarung genannten personenbezogenen Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder die Verarbeitung einzuschränken. Das Gleiche gilt, wenn diese Vereinbarung eine Berichtigung, Löschung oder Einschränkung der Verarbeitung von Daten vorsieht.
- c. Soweit sich eine betroffene Person unmittelbar an den Auftragsverarbeiter zwecks Anfragen und Ansprüchen als betroffene Person nach Kapitel III der DSGVO der Verarbeitung der in § 5 dieser Vereinbarung genannten personenbezogenen Daten wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich nach Erhalt an den Verantwortlichen weiterleiten.

3. Kontrollpflichten

- a. Der Auftragsverarbeiter stellt durch geeignete Kontrollen sicher, dass die im Auftrag verarbeiteten personenbezogenen Daten ausschließlich nach Maßgabe dieser Vereinbarung und/oder des Hauptvertrages und/oder den entsprechenden Weisungen verarbeitet werden.
- b. Der Auftragsverarbeiter wird sein Unternehmen und seine Betriebsabläufe so gestalten, dass die Daten, die er im Auftrag des Verantwortlichen verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind.
- c. Der Auftragsverarbeiter bestätigt, dass er gem. Art. 37 DSGVO und, sofern anwendbar, gemäß § 38 BDSG einen Datenschutzbeauftragten bestellt hat und die Einhaltung der Vorschriften zum Datenschutz und zur Datensicherheit unter Einbeziehung des Datenschutzbeauftragten überwacht. Datenschutzbeauftragter des Auftragsverarbeiters ist derzeit:

Thomas Boese
Gödde GmbH
Robert-Perthel-Straße 57-59, 50739 Köln
datenschutz@goedde.com

4. Informationspflichten

- a. Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darauf aufmerksam machen, wenn eine von dem Verantwortlichen erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.
- b. Der Auftragsverarbeiter wird den Verantwortlichen bei der Einhaltung der in den Artt. 32 bis 36 DSGVO genannten Pflichten unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützen.

5. Ort der Datenverarbeitung

- a. Die Verarbeitung der Daten findet grundsätzlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DSGVO erfüllt sind.

6. Löschung der personenbezogenen Daten nach Auftragsbeendigung

- a. Nach Beendigung des Hauptvertrages wird der Auftragsverarbeiter alle im Auftrag verarbeiteten personenbezogenen Daten nach Wahl des Verantwortlichen entweder löschen, sofern der Löschung dieser Daten keine gesetzlichen Aufbewahrungspflichten des Auftragsverarbeiters entgegenstehen. Die datenschutzgerechte Löschung ist zu dokumentieren und gegenüber dem Verantwortlichen auf Anforderung zu bestätigen.

§ 8 Kontrollrechte des Verantwortlichen

1. Der Verantwortliche ist berechtigt, nach rechtzeitiger vorheriger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Geschäftsbetriebes des Auftragsverarbeiters oder Gefährdung der Sicherheitsmaßnahmen für andere Verantwortliche und auf eigene Kosten, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang selbst oder durch Dritte zu kontrollieren. Die Kontrollen können auch durch Zugriff auf vorhandene branchenübliche Zertifizierungen des Auftragsverarbeiters aktuelle Testate oder Berichte einer unabhängigen Instanz (wie z.B. Wirtschaftsprüfer, externer Datenschutzbeauftragter, Revisor oder externer Datenschutzauditor) oder Selbstauskünfte durchgeführt werden. Der Auftragsverarbeiter wird die notwendige Unterstützung zur Durchführung der Kontrollen anbieten.
2. Der Auftragsverarbeiter wird den Verantwortlichen über die Durchführung von Kontrollmaßnahmen der Aufsichtsbehörde informieren, soweit die Maßnahmen oder Datenverarbeitungen betreffen können, die der Auftragsverarbeiter für den Verantwortlichen erbringt.

§ 9 Unterauftragsverhältnisse

1. Der Verantwortliche ermächtigt den Auftragsverarbeiter weitere Auftragsverarbeiter gemäß den nachfolgenden Absätzen in § 9 dieser Vereinbarung in Anspruch zu nehmen. Diese Ermächtigung stellt eine allgemeine schriftliche Genehmigung i. S. d. § 28 Abs. 2 DSGVO dar.
2. Der Auftragsverarbeiter arbeitet derzeit bei der Erfüllung des Auftrags mit den in der Anlage 2 benannten Unterauftragnehmern zusammen, mit deren Beauftragung sich der Verantwortliche einverstanden erklärt.
3. Der Auftragsverarbeiter ist berechtigt, weitere Auftragsverarbeiter zu beauftragen oder bereits beauftragte zu ersetzen. Der Auftragsverarbeiter wird den Verantwortlichen vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines weiteren Auftragsverarbeiters informieren. Der Verantwortliche kann gegen eine beabsichtigte Änderung Einspruch erheben.
4. Der Einspruch gegen die beabsichtigte Änderung ist innerhalb von 2 Wochen nach Zugang der Information über die Änderung gegenüber dem Auftragsverarbeiter zu erheben. Im Fall des Einspruchs kann der Auftragsverarbeiter nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder einen alternativen weiteren Auftragsverarbeiter vorschlagen und mit dem Verantwortlichen abstimmen. Sofern die Erbringung der Leistung ohne die beabsichtigte Änderung dem Auftragsverarbeiter nicht zumutbar ist – etwa aufgrund von damit verbundenen unverhältnismäßigen Aufwendungen für den Auftragsverarbeiter – oder die Abstimmung eines weiteren Auftragsverarbeiters fehlschlägt, können der Verantwortliche und der Auftragsverarbeiter diese Vereinbarung sowie den Hauptvertrag mit einer Frist von einem Monat zum Monatsende kündigen.
5. Bei Einschaltung eines weiteren Auftragsverarbeiters muss stets ein Schutzniveau, welches mit demjenigen dieser Vereinbarung vergleichbar ist, gewährleistet werden. Der Auftragsverarbeiter ist gegenüber dem Verantwortlichen für sämtliche Handlungen und Unterlassungen der von ihm eingesetzten weiteren Auftragsverarbeiter verantwortlich.

§ 10 Vertraulichkeit

1. Der Auftragsverarbeiter ist bei der Verarbeitung von Daten für den Verantwortlichen zur Wahrung der Vertraulichkeit verpflichtet.
2. Der Auftragsverarbeiter verpflichtet sich bei der Erfüllung des Auftrags nur Mitarbeiter oder sonstige Erfüllungsgehilfen einzusetzen, die auf die Vertraulichkeit im Umgang mit überlassenen personenbezogenen Daten verpflichtet und in geeigneter Weise mit den Anforderungen des Datenschutzes vertraut gemacht worden sind. Die Vornahme der Verpflichtungen wird der Auftragsverarbeiter dem Verantwortlichen auf Nachfrage nachweisen.
3. Sofern der Verantwortliche anderweitigen Geheimnisschutzregeln unterliegt, wird er dies dem Auftragsverarbeiter mitteilen. Der Auftragsverarbeiter wird seine Mitarbeiter entsprechend den Anforderungen des Verantwortlichen auf diese Geheimnisschutzregeln verpflichten.

§ 11 Technische und organisatorische Maßnahmen

1. Die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen werden als angemessen vereinbart. Der Auftragsverarbeiter kann diese Maßnahmen aktualisieren und ändern, vorausgesetzt dass das Schutzniveau durch solche Aktualisierungen und/oder Änderungen nicht wesentlich herabgesetzt wird.
2. Der Auftragsverarbeiter beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung gemäß § 32 i.V.m § 5 Abs. 1 DSGVO. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen. Er wird alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Standes der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene ergreifen. Die zu treffenden Maßnahmen umfassen insbesondere Maßnahmen zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Maßnahmen, die die Kontinuität der Verarbeitung nach Zwischenfällen gewährleisten. Um stets ein angemessenes Sicherheitsniveau der Verarbeitung gewährleisten zu können, wird der Auftragsverarbeiter die implementierten Maßnahmen regelmäßig evaluieren und ggf. Anpassungen vornehmen.

§ 12 Haftung/ Freistellung

1. Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen gemäß den gesetzlichen Regelungen für sämtliche Schäden durch schuldhafte Verstöße gegen diese Vereinbarung sowie gegen die ihn treffenden gesetzlichen Datenschutzbestimmungen, die der Auftragsverarbeiter, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung verursachen. Eine Ersatzpflicht des Auftragsverarbeiters besteht nicht, sofern der Auftragsverarbeiter nachweist, dass er die ihm überlassenen Daten des Verantwortlichen ausschließlich nach den Weisungen des Verantwortlichen verarbeitet und seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus der DSGVO nachgekommen ist.
2. Der Verantwortliche stellt den Auftragsverarbeiter von allen Ansprüchen Dritter frei, die aufgrund einer schuldhaften Verletzung der Verpflichtungen aus dieser Vereinbarung oder geltenden datenschutzrechtlichen Vorschriften durch den Verantwortlichen gegen den Auftragsverarbeiter geltend gemacht werden.

§ 13 Sonstiges

1. Im Falle von Widersprüchen zwischen den Bestimmungen in dieser Vereinbarung und den Regelungen des Hauptvertrages gehen die Bestimmungen dieser Vereinbarung vor.
2. Änderungen und Ergänzungen dieser Vereinbarung setzen die beidseitige Zustimmung der Vertragsparteien voraus unter konkreter Bezugnahme auf die zu ändernde Regelung dieser Vereinbarung. Mündliche Nebenabreden bestehen nicht und sich auch für künftige Änderungen dieser Vereinbarung ausgeschlossen.
3. Diese Vereinbarung unterliegt deutschem Recht.
4. Sofern der Zugriff auf die Daten, die der Verantwortliche dem Auftragsverarbeiter zur Datenverarbeitung übermittelt hat, durch Maßnahmen Dritter (z.B. Maßnahmen eines Insolvenzverwalters, Beschlagnahme durch Finanzbehörden, etc.) gefährdet wird, hat der Auftragsverarbeiter den Verantwortlichen unverzüglich hierüber zu benachrichtigen.

5. Die Einrede des Zurückbehaltungsrechts an den vertragsgegenständlichen Daten sowie an evtl. vorhandenen Datenträgern wird ausgeschlossen.
6. Sollten eine oder mehrere Bestimmungen dieses Vertrags rechtsunwirksam sein oder werden, so soll dadurch die Gültigkeit der übrigen Bestimmungen nicht berührt werden. Die ungültige Bestimmung wird schnellstmöglich durch eine andere Bestimmung ersetzt, die dem wirtschaftlichen Gehalt der rechtsunwirksamen Bestimmung am nächsten kommt.

Anlagen:

[Anlage 2.1.1 Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung](#)

[Anlage 2.1.2 Unterauftragsverhältnisse gemäß § 9 der Vereinbarung zur Auftragsverarbeitung](#)

Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung

Gödde sichert zu, folgende technische und organisatorische Maßnahmen getroffen zu haben:

A. Maßnahmen zur Pseudonymisierung

Maßnahmen, die den unmittelbaren Personenbezug während der Verarbeitung in einer Weise reduzieren, dass nur mit Hinzuziehung zusätzlicher Informationen eine Zuordnung zu einer spezifischen betroffenen Person möglich ist. Die Zusatzinformationen sind dabei durch geeignete technische und organisatorische Maßnahmen von dem Pseudonym getrennt aufzubewahren. Beschreibung der Pseudonymisierung:

- Pseudonymisierung von Kundendaten für den Test nichtproduktiver Systeme/Entwicklungen außerhalb der geschützten Datenbankumgebung

B. Maßnahmen zur Verschlüsselung

Maßnahmen oder Vorgänge, bei denen ein klar lesbarer Text / Information mit Hilfe eines Verschlüsselungsverfahrens (Kryptosystem) in eine unleserliche, das heißt nicht einfach interpretierbare Zeichenfolge (Geheimtext) umgewandelt wird:

- Festplattenverschlüsselung aller Fat Clients mittels Bitlocker
- Verschlüsselte Kennwortspeicherung in zentralem System

C. Maßnahmen zur Sicherung der Vertraulichkeit

1. Zutrittskontrolle

Maßnahmen, die unbefugten Personen den Zutritt zu IT-Systemen und Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, sowie zu vertraulichen Akten und Datenträgern physisch verwehren. Beschreibung des Zutrittskontrollsystems:

- Sicherheitsschlösser und/oder Chipkarte-/Transponder-Schließsystem
- Serverräume sind stets verschlossen, ein Zutritt mittels Schlüssel ist streng reguliert (begrenzter Personenkreis) 2-Faktor-Authentifizierung besonders schützenswerter Bereiche (Rechenzentrum) und Informationen
- Videoüberwachung an den Ein- und Ausgängen, in Durchgangsbereichen und im Hauptserverraum
- Alarmanlage und Raumüberwachung einstiegsgefährdeter Bereiche
- Tresore für besonders schützenswerte Informationen
- Kontrollierte Besucheranmeldung und -begleitung innerhalb der Schutzzonen (Besucherausweise inkl. Kontrolle der Rückgabe)

2. Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte datenschutzrechtlich geschützte Daten verarbeiten oder nutzen können. Beschreibung des Zugangskontrollsystems:

- Kennwortverfahren, d.h. persönlicher und individueller User Login bei Systemanmeldung (u.a. Sonderzeichen, Mindestlänge) sowie Anforderung verschiedener Passwörter für verschiedene Dienste und teils zusätzlich MFA (Multi Faktor Authentifizierung)
- Bereitstellung eines verschlüsselten Passwortmanagers
- Auto Lock bei Inaktivität innerhalb definiertem Zeitfenster
- Protokollierung der Anmeldeversuche und Abbruch des Anmeldevorgangs sowie Sperrung nach festgelegter Zahl von erfolgloser Zahl von Versuchen
- Zugangswege/Transportwege SSL-TLS oder AES-256 verschlüsselt
- Verzeichnisdienst zur zentralen Steuerung von Berechtigungen (Active Directory)
- Überwachung besonders schützenswerter Informationen (Active Directory)
Dabei Erkennung von unregelmäßigem Verhalten wie z.B.: Fehlversuche Anmeldung, Änderungen Gruppenzugehörigkeiten, etc.)
- Regelmäßig aktualisierte Antiviren- und Spywarefilter
- Rechtesystem: Begrenzung der Zahl der berechtigten Mitarbeiter auf das Notwendigste
- Netzwerksegmentierung (VLAN mit logisch getrennten Netzen)
- Separierte und abgesicherte WLAN Bereiche für Gäste, Firmennetzwerk, etc.
- Separate Rechtevergabe/Management für das ERP System
- Single Sign-on für verschiedene Applikationen (AD überwacht)
- Firewall Appliance

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, so dass Daten bei der Verarbeitung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Beschreibung des Zugriffskontrollsystems:

- Berechtigungskonzepte (Profile, Rollen, etc.) für zentrale Systeme (ERP, Produkte, CRM)
- Protokollierung wesentlicher Änderung der Berechtigungen innerhalb der Zielsysteme (Log Files) z.B. innerhalb des ERP
- Optionale Verschlüsselung (durch den User gesteuert) von externen Datenträgern, die an firmeneigene Rechner angeschlossen werden
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- Verschlüsselung von Datenträgern in Notebooks

4. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist. Beschreibung des Trennungskontrollvorgangs:

- Trennungsgebot von Verantwortlichkeiten/Rollen in den Berechtigungskonzepten verankert (ERP, Produktdaten)
 - Tätigkeitsspezifische Rollen für das Filesystem
 - Trennung von Entwicklungs-/Test-/Integrations-/Produktivumgebungen
- Eigenständige Systeme für Kunden- und Bestellmanagement (e-Shop und ERP)

D. Maßnahmen zur Sicherung der Integrität

1. Datenintegrität

Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden. Beschreibung der Datenintegrität:

- Geregelter Transport-Ablauf mit 4 Augen-Prinzip für Core Systeme (ERP, Produktdaten, CRM). Das Einspielen von Releases und Patches erfolgt gesteuert durch das Service Management mittels webbasierten Managementsystem. Neue Releases/Patches werden in Test-/Integrationsumgebung qualitätsgesichert, bevor sie in die Produktivumgebung fließen
- Geregelter Patch Management Prozess für wesentliche Services/Systeme inklusive zugehöriger Freigaben und Dokumentationen

2. Transportkontrolle

Maßnahmen, die gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden. Beschreibung der Transportkontrolle:

- VPN Tunnel zwischen Gödde und unserem ERP Dienstleister
- E-Mail TLS Verschlüsselung
- Https Verbindungen für Webzugriffe und Cloud basierte Anwendungen
- Datenübertragung schützenswerter Informationen mittels gesicherter Plattformen

3. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind. Beschreibung des Eingabekontrollvorgangs:

- Protokollierung (Log Files) von Systemänderungen in den wichtigsten Systemen (u.a. ERP, CRM, etc.)

E. Maßnahmen zur Sicherung der Verfügbarkeit und Belastbarkeit

1. Verfügbarkeitskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Beschreibung des Verfügbarkeitskontrollsystems:

- Redundante Auslegung wesentlicher Systeme und Server
- Betrieb wesentlicher IT-Systeme in einem IT-Safe. Dieser ist mit USV, Löschanlage, Klimatisierung, Monitoring, etc. ausgestattet.
- Virtualisierte Systeme mittels VMware
- Notfallplan (Notfallhandbuch, Rufbereitschaften)
- Monitoring von kritischen Datenverarbeitungssystemen
- Backup- und Recoverykonzept
- Regelmäßige Datenwiederherstellungstests
- Datensicherung in der Cloud
- Einsatz von Intrusion-Detection-Systemen
- Regelmäßige Aktualisierung der Systeme
- Feuer- und Rauchmeldeanlagen

2. Rasche Wiederherstellbarkeit

Maßnahmen, die die Fähigkeit sicherstellen, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Beschreibung der Maßnahmen zur raschen Wiederherstellbarkeit:

- Datensicherungsverfahren inklusive zugehöriger Test der Wiederherstellbarkeit (in Testsystemen)
- Gespiegelte Umgebungen
- Cloud Dienste für wesentliche Applikationen (HR Suite, MS Azure Cloud, CRM)
- Virtualisierte Systeme mittels VMware
- Monitoring von Kernsystemen und Services
- Wartungsverträge mit geeigneten Reaktionszeiten
- Nutzung virtueller Maschinen mit Offsitesicherung (Cloud)

3. Zuverlässigkeit

Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden. Beschreibung der Maßnahmen zur Zuverlässigkeit:

- Monitoring von Kernsystemen und Services
- Notfallpläne und definierte Verantwortlichkeiten
- Supporthotline
- Regelmäßige Datenwiederherstellungstests

F. Maßnahmen zur regelmäßigen Evaluation der Sicherheit der Datenverarbeitung

1. Überprüfungsverfahren

Maßnahmen, die die datenschutzkonforme und sichere Verarbeitung sicherstellen. Beschreibung der Überprüfungsverfahren:

- Kontinuierliche Steigerung der Informationssicherheit definiert über ein Reifegradmodell und unterstützt durch externe Berater
- Wiederkehrende Audits/Assessments zur Analyse und Beseitigung von Schwachstellen
- Überprüfung und Freigabe von Datenverarbeitungsprozessen mit personenbezogenen Daten durch den Konzern-Datenschutzbeauftragten
- Weisungen des Verantwortlichen werden dokumentiert

2. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Beschreibung der Maßnahmen zur Auftragskontrolle:

- Standardisierte und zentralisierte Vergabe von Dienstleistungsverträgen
- Standardisierte Vertragsvorlagen inklusive zugehöriger Datenschutzvereinbarung für Dienstleister Auftragsdatenverarbeitung

3. Reaktion auf Sicherheitsverletzung

- Implementierung eines formalisierten Prozesses und Verantwortlichkeiten, wodurch im Falle eines Datenschutzvorfalles die Betroffenen und die Aufsichtsbehörde informiert werden
- Definition von Eskalationswegen

4. Datenschutz-Management

- Bestellung eines Datenschutzbeauftragten
- Verzeichnis von Verarbeitungstätigkeiten
- Mitarbeitersensibilisierung und Schulungen
- Verpflichtung der Mitarbeiter auf Vertraulichkeit
- Arbeitsanweisungen

5. Richtlinien und Handlungsanweisungen für Mitarbeiter

Es existiert ein verbindliches Regelwerk für den Umgang mit personenbezogenen Daten und IT-Systemen. Hier wird u. a. Folgendes gesondert geregelt:

- E-Mail- und Internetnutzung
- Passwortrichtlinie
- Berechtigungsmanagement
- Vertraulichkeitsverpflichtung bei Umgang mit Firmen- und den Kundendaten
- Mobiles Arbeiten

Unterauftragsverhältnisse gemäß § 9 der Vereinbarung zur Auftragsverarbeitung

Der Auftragsverarbeiter arbeitet derzeit bei der Erfüllung des Auftrags mit den folgenden weiteren Auftragsverarbeitern zusammen, mit deren Beauftragung sich der Verantwortliche einverstanden erklärt.

1. Hoffmann Engineering Services GmbH

- Hoffmann Engineering Services GmbH, Haberlandstraße 55, 81241 München
 - Funktion/Tätigkeit: Sammeln von Nutzungsdaten zur Optimierung der eingesetzten Software im Sinne § 3 des Auftragsverarbeitungsvertrags

2. Hoffmann SE

- Hoffmann SE, Haberlandstraße 55, 81241 München
 - Funktion/Tätigkeit: Auftrag annehmen und an die Hoffmann Engineering Services weitergeben.