# Allgemeine Einkaufsbedingungen

**1. Geltungsbereich und Vertragsschluss**

1.1 Für Lieferungen und Leistungen des Lieferanten gelten diese Allgemeinen Einkaufsbedingungen, soweit keine anderweitigen Vereinbarungen getroffen wurden. Andere Allgemeine Geschäftsbedingungen, insbesondere Allgemeine Lieferbedingungen des Lieferanten, gelten auch dann nicht, wenn ihnen im Einzelfall nicht ausdrücklich widersprochen wurde oder bestellte Waren/Leistungen vorbehaltlos angenommen wurden.

1.2 Diese Allgemeinen Einkaufsbedingungen gelten nur gegenüber Unternehmen gemäß § 310 Abs. 1 BGB.

1.3 Bestellung und Annahme der Bestellung („Auftragsbestätigung“) sowie alle Vereinbarungen, die zwischen dem Besteller und dem Lieferanten zwecks Ausführung des Vertrages getroffen werden, bedürfen der Schriftform. Zur Wahrung der Schriftform genügt die Übermittlung durch Telefax, Datenfernübertragung, Verwendung von elektronischen Signaturprogrammen wie DocuSign, AdobeSign oder E-Mail.

1.4 Der Lieferant ist verpflichtet, innerhalb einer Frist von 2 Wochen die Bestellung durch Rücksendung einer Auftragsbestätigung anzunehmen. Bei Fristüberschreitung ist der Besteller zum Widerruf der Bestellung berechtigt. Weicht die Auftragsbestätigung, wenn auch nur in unwesentlichen Punkten, von der Bestellung ab, so werden diese Änderungen nur Vertragsinhalt, wenn der Besteller ausdrücklich sein Einverständnis dazu erklärt.

**2. Lieferung, Erfüllungsort und Folgen von Terminüberschreitungen**

2.1 Vereinbarte Termine sind verbindlich. Umstände, die ihre Einhaltung unmöglich machen oder verzögern können, sind dem Besteller sofort mitzuteilen. Maßgebend für die Einhaltung des Liefer-/Leistungstermins ist der Eingang der Ware oder Vollendung der Leistung beim Besteller oder dem in der Bestellung genannten Liefer-/Leistungsort („Erfüllungsort“).

2.2 Teillieferungen bedürfen der Zustimmung des Bestellers.

2.3 Im Falle eines Liefer-/Leistungsverzuges ist der Besteller berechtigt, pauschalisierten Verzugsschaden in Höhe von 1% des Liefer-/Leistungswertes je vollendeter Woche des Lieferverzuges zu verlangen, insgesamt jedoch nicht mehr als 10% des im Liefer-/Leistungsverzuges befindlichen Vertragswertes. Weitergehende gesetzliche Ansprüche (Rücktritt und Schadensersatz statt der Leistung) bleiben vorbehalten. Die Geltendmachung eines nachgewiesenen höheren Schadens bleibt dem Besteller, der Nachweis eines wesentlich geringeren oder gar kein Schaden bleibt dem Lieferanten vorbehalten.

2.4 Die vorbehaltlose Annahme der verspäteten Lieferung oder Leistung enthält keinen Verzicht auf die dem Besteller wegen der verspäteten Lieferung oder Leistung zustehenden Ersatzansprüche.

**3. Ersatzteilversorgung**

Der Lieferant wird die Ersatzteilversorgung nach Auslaufen der Bauserie für das Lieferteil für mindestens 10 Jahre sicherstellen. Für diesen Zeitraum werden auch die zur Ersatzteilfertigung benötigten Mittel und Zeichnungen aufbewahrt. Die Aufbewahrungspflicht erlischt nach Ablauf dieser Frist und schriftlicher Zustimmung durch den Besteller. Diese darf nur aus wichtigem Grunde verweigert werden.

**4. Preise, Gefahrübergang und Zahlungsbedingungen**

4.1 Der in der Bestellung ausgewiesene Preis ist bindend. Die Preise verstehen sich frei genannter Lieferort DAP Incoterms 2020 einschließlich Verpackung. Die gesetzliche Mehrwertsteuer ist darin nicht enthalten. Der Lieferant trägt die Gefahr des Verlusts oder der Beschädigung der Ware bis sie, wie hierin beschrieben, geliefert ist.

4.2 Rechnungen sind unter Angabe der Bestellnummer an die in der Bestellung angegebene Adresse zu versenden. Solange die Bestellnummer fehlt, sind Rechnungen nicht zahlbar und werden an den Lieferanten zurückgeschickt; dadurch entstehende Verzögerungen sind nicht durch den Besteller zu vertreten. Für jede Bestellung ist eine gesonderte Rechnung zu erstellen. Die Rechnung ist entsprechend der Bestellung zu gliedern. Eventuelle Anzahlungs-, Teil- und Schlussrechnungen sind als solche zu bezeichnen. Im Falle von Werkleistungen sind den Rechnungen ein vom Besteller und vom Lieferanten unterschriebener Leistungsnachweis (Rapport) beizufügen.

4.3 Die Begleichung der Rechnung erfolgt innerhalb von 30 Tagen netto nach Lieferung bzw. Leistungserbringung und Rechnungseingang beim Besteller.

**5. Abnahme**

Schuldet der Lieferant eine Werkleistung, ist deren förmliche Abnahme durch den Besteller erforderlich. Die Abnahme erfolgt nach Wahl des Bestellers im Werk des Lieferanten oder am Erfüllungsort. Vorbehaltlose Zahlungen stellen weder eine Abnahme noch eine Genehmigung von Liefergegenständen oder einen Verzicht auf Mängelansprüche dar.

**6. Versand**

6.1 Der Versand der Ware ist spätestens bei Abgang der Lieferungen im Werk des Lieferanten anzuzeigen.

6.2 Der Lieferant ist verpflichtet, auf allen Versandpapieren und Lieferscheinen die Bestellnummer und die exakte Lieferanschrift des Bestellers anzugeben. Unterlässt er dies, so ist der Lieferant für die dadurch entstehenden Verzögerungen verantwortlich.

6.3 Sendungen, für die der Besteller die Frachtkosten ganz oder teilweise zu tragen hat, sind zu den günstigsten Frachttarifen bzw. nach den Versandvorschriften des Bestellers zu befördern.

6.4 Die geltenden Versandvorschriften werden in der Bestellung angegeben.

**7. Verpackungen**

7.1 Der Lieferant ist verpflichtet, die Verpackung für den erforderlichen Transport der Ware nach Maßgabe der Bestellung sowie der geltenden Vorschriften so vorzunehmen, dass Schäden bei normaler Behandlung der Ware vermieden werden.

7.2 Unabhängig davon, ob es sich bei den Verpackungen um Transport-, Verkaufs- oder Umverpackungen handelt, hat der Lieferant die Verpflichtungen nach dem deutschen Verpackungsgesetz einzuhalten. Der Lieferant hat Verpackungen nach Gebrauch auf Wunsch von Besteller kostenlos zurückzunehmen und einer erneuten Verwendung oder einer stofflichen Verwertung zuzuführen. Rücknahmeort der Verpackungen, wenn eine Rücknahme von Besteller gewünscht, ist das Besteller Werkstor.

**8. Mängelrüge**

Der Besteller wird eingehende Lieferungen auf Menge, Transportschäden und offensichtliche Sachmängel kontrollieren, soweit und sobald dies nach ordnungsgemäßem Geschäftsgang tunlich ist. Mängel werden gegenüber dem Lieferanten innerhalb einer Frist von 5 Arbeitstagen nach Entdeckung gerügt. Der Lieferant verzichtet insoweit auf den Einwand verspäteter Mängelrüge. Der Besteller behält sich das Recht vor, eine weitergehende Wareneingangsprüfung durchzuführen.

**9. Mängelhaftung**

9.1 Der Lieferant haftet dem Besteller dafür, dass die bestellte Ware bzw. Leistung zum Zeitpunkt des Gefahrüberganges den vertraglich vereinbarten und gewöhnlich vorausgesetzten Eigenschaften (das bedeutet die Einhaltung der für die Lieferung oder Leistung anwendbaren vertraglichen und gesetzlichen Vorschriften sowie der anwendbaren technischen Richtlinien und Normen und dem Stand der Technik) entspricht und frei von Sach- und Rechtsmängeln ist.

9.2 Teilt der Besteller dem Lieferanten den Einsatzzweck und den Einsatzort für die zu liefernde Ware / die durchzuführenden Leistungen mit, so sichert der Lieferant die Eignung seiner Lieferung und Leistung für diesen Zweck bzw. Ort zu.

9.3 Bei Vorliegen eines Sach- oder Rechtsmangels stehen dem Besteller die gesetzlichen Mängelansprüche ungekürzt zu.

9.4 Das Recht, die Art der Nacherfüllung zu wählen, steht grundsätzlich dem Besteller zu. Sollte der Lieferant nicht unverzüglich nach Aufforderung durch den Besteller mit der Nacherfüllung des Vertrages, d.h. der Mangelbeseitigung oder Ersatzlieferung, beginnen, so steht dem Besteller in diesen Fällen, sowie zur Abwehr von Gefahren oder zum Zwecke des Schadensvermeidung/-minderung das Recht zu, die vom Besteller gewählte Art der Nacherfüllung auf Kosten des Lieferanten selbst vorzunehmen oder durch Dritte vornehmen zu lassen. Das gleiche Recht hat der Besteller bei Fehlschlagen oder Verweigerung der Mangelbeseitigung bzw. der Ersatzlieferung.

9.5 Fallen im Zusammenhang mit dem Mangel bzw. der Durchführung der Nacherfüllung Kosten und/oder Aufwendungen für den Besteller an, das können insbesondere Aus- und Einbaukosten, Transportkosten zum und vom Einsatzort, Reisekosten, Sortierkosten, Reparatur- und Materialkosten und dafür erforderliche Arbeitsstunden, so ist der Lieferant verpflichtet, diese Kosten zu tragen, unabhängig davon, ob er den Mangel zu vertreten hat.

9.6 Wird der Besteller von Dritten in Anspruch genommen, weil im Zusammenhang mit der Lieferung/Leistung des Lieferanten Rechte Dritter verletzt werden, so ist der Lieferant verpflichtet, den Besteller auf erstes schriftliches Anfordern von diesen Ansprüchen freizustellen. Die Freistellungspflicht des Lieferanten bezieht sich auf alle Aufwendungen, die dem Besteller aus oder im Zusammenhang mit der Inanspruchnahme durch einen Dritten notwendigerweise erwachsen.
9.7 Mängelansprüche verjähren – außer in den Fällen der Arglist – in 30 Monaten ab Eingang der Ware am Erfüllungsort bzw. der Abnahme der Werkleistung. Erfüllt der Lieferant seine Nacherfüllungsverpflichtung durch Ersatzlieferung, so beginnt für die als Ersatz gelieferte Ware nach deren Ablieferung die Verjährungsfrist neu zu laufen.

## 10. Informationtechnologie

10.1 Für Software/Hardware und/oder OT & E/E-Systemlösungen einschließlich Dokumentation, die zum Lieferumfang gehört und die **nicht** im Auftrag von Voith entwickelt worden ist, gelten die Bedingungen von **Anhang 1** zu diesen Allgemeinen Einkaufsbedingungen.
10.2 Für alle Lieferungen und Leistungen im Bereich der Informationstechnologie (IT)/Operational Technology (OT) & E/E Systemen, die im Auftrag von Voith entwickelt bzw. angepasst worden ist oder es sich um den Einkauf von IT-Dienstleistungen oder Informationstechnologie, die nicht von 10.1 erfasst sind, handelt, gelten die Bedingungen von **Anhang 2** zu diesen Allgemeinen Einkaufsbedingungen.

## 11. Qualitätssicherung

11.1 Der Lieferant verpflichtet sich, die permanente Qualitätssicherung seiner Ware durch Anwendung eines geeigneten Qualitätssicherungssystems, z.B. DIN EN ISO 9001 ff oder gleichwertiger Art, und vom Besteller vorgegebene bzw. sonst geeignete Qualitätsprüfungen und -kontrollen während und nach der Fertigung seiner Waren zu gewährleisten. Über diese Prüfungen hat er eine Dokumentation zu erstellen und für einen Zeitraum von 10 Jahren aufzubewahren.
11.2 Der Besteller oder eine vom Besteller beauftragte Person hat das Recht, einen Nachweis über die vertraglich geschuldete Qualität des Liefergegenstandes sowie das Qualitätssicherungssystem des Lieferanten zu verlangen und sich jederzeit von der Qualität bzw. Art der Durchführung der Prüfungen und Kontrollen im Werk des Lieferanten oder seiner Unterlieferanten zu überzeugen sowie Abnahmen oder ein Audit im Werk des Lieferanten oder seiner Unterlieferanten auf Kosten des Lieferanten durchzuführen.
11.3 Der Lieferant hat dem Besteller unaufgefordert Änderungen in der Zusammensetzung des verarbeiteten Materials oder der konstruktiven Ausführung seiner Lieferungen oder Leistungen unverzüglich in Form von Ziffer 1.3 anzuzeigen. Die Änderungen bedürfen der schriftlichen Zustimmung des Bestellers.
11.4 Sofern der Lieferant beabsichtigt, Lieferungen oder Leistungen vollständig oder überwiegend durch einen Unterlieferanten durchführen zu lassen, hat er dies dem Besteller vorab anzuzeigen. Die Unterbeauftragung bedarf in diesem Falle der schriftlichen Zustimmung des Bestellers.
11.5 Die dem Lieferanten bekanntgegebenen Qualitätssicherungsleitlinien des Bestellers bzw. die mit dem Lieferanten getroffenen Qualitätssicherungsvereinbarungen sind Bestandteil des Vertrages.

## 12. Inverkehrbringen von Produkten und Produkthaftung

12.1 Der Lieferant verpflichtet sich, die an seinem Sitz und am Erfüllungsort anwendbaren Rechtsvorschriften einzuhalten.
12.2 Bei der Lieferung von Produkten, die dem Anwendungsbereich einer Binnenmarktrichtlinie der Europäischen Union für das erstmalige Inverkehrbringen unterfallen, wie z.B. EG-Maschinenrichtlinie, Druckgeräterichtlinie, EMV-Richtlinie usw., verpflichtet sich der Lieferant zur Einhaltung der dort maßgeblichen Sicherheits- und Gesundheitsschutzanforderungen und Verfahren sowie zur Ausstellung der darin vorgesehenen Dokumente. Bei unvollständigen Maschinen i.S. der EG-Maschinenrichtlinie Nr. 2006/42/EG hat der Lieferant dem Besteller eine Einbauerklärung nach Anhang II B der EG-Maschinenrichtlinie in der vom Besteller geforderten Form (erweiterte Einbauerklärung) sowie zusätzlich eine Betriebsanleitung nach Anhang I Ziffer 1.7.4. der EG-Maschinenrichtlinie auszuhändigen. Auf Verlangen und nach Wahl des Bestellers hat der Lieferant die von ihm erstellte Risikobeurteilung an den Besteller auszuhändigen bzw. Einblick in diese zu gewähren.
12.3 Soweit der Lieferant für einen Schaden außerhalb der gelieferten Ware verantwortlich ist und der Besteller aufgrund gesetzlicher Produkthaftung in Anspruch genommen wird, ist der Lieferant verpflichtet, den Besteller insoweit von Schadensersatzansprüchen Dritter auf erstes Anfordern freizustellen, als die Ursache des Schadens im Verantwortungsbereich des Lieferanten gesetzt ist und er im Außenverhältnis selbst haftet.
Im Rahmen seiner Haftung ist der Lieferant auch verpflichtet, etwaige Aufwendungen des Bestellers zu erstatten, die sich aus oder im Zusammenhang mit einer vom Besteller durchgeführten Warn- oder Rückrufaktion ergeben. Über Inhalt und Umfang der durchzuführenden Maßnahmen wird der Besteller den Lieferanten – soweit möglich und zumutbar – unterrichten bzw. mit ihm abstimmen. Unberührt bleiben sonstige gesetzliche Ansprüche aus Produkthaftung.
12.4 Der Lieferant verpflichtet sich, eine Produkthaftpflichtversicherung mit der Deckungssumme von mindestens 1.000.000,00 Euro je Schadensfall zu unterhalten. Stehen dem Besteller weitergehende Schadensersatzansprüche zu, so bleiben diese unberührt.

## 13. Arbeitssicherheit, Umweltschutz und Konfliktmineralien

13.1 Der Lieferant hat dafür zu sorgen, dass seine Lieferungen und Leistungen den auf dem Gelände des Bestellers oder an dem ihm bekannten sonstigen Erfüllungsort geltenden Umweltschutz-, Unfallverhütungs- und Arbeitsschutzvorschriften sowie sonstige sicherheitstechnischen/-relevanten Regeln genügen, so dass nachteilige Auswirkungen auf Mensch und Umwelt vermieden bzw. verringert werden. Hierzu wird der Lieferant ein Managementsystem, z.B. nach DIN EN ISO 14001 oder gleichwertiger Art einrichten und weiterentwickeln. Der Besteller hat das Recht, gegebenenfalls einen Nachweis über das vom Lieferanten betriebene Managementsystem zu verlangen, sowie ein Audit im Unternehmen des Lieferanten durchzuführen.
13.2 Der Lieferant sichert zu, dass er die Anforderungen der EU Chemikalienverordnung REACH (Verordnung (EG) Nr. 1907/2006) einhält, insbesondere die Registrierung der Stoffe erfolgt ist. Der Besteller ist nicht verpflichtet, im Rahmen der REACH-Verordnung eine Zulassung für einen vom Lieferanten gelieferten Liefergegenstand einzuholen.
Der Lieferant sichert weiterhin zu, keine Liefergegenstände zu liefern, die Stoffe enthalten gemäß der Anlagen 1 bis 9 der REACH-Verordnung, dem Beschluss des Rates 2006/507/EG (Stockholmer Übereinkommen über persistente organische Schadstoffe, der EG-Verordnung 1005/2009 über Ozonschicht abbauende Substanzen, der Global Automotive Declarable Substance List (GADSL) und der RoHS-Richtlinie (2002/95/EG) für Produkte gemäß ihres Anwendungsbereiches. Alle genannten Richtlinien in ihrer jeweils gültigen Fassung. Sollten die Liefergegenstände Stoffe enthalten, die auf der Candidate List of Substances of Very High Concern (SVHC-Liste) gemäß REACH gelistet sind, ist der Lieferant verpflichtet, dies unverzüglich mitzuteilen. Dies gilt auch, wenn bei laufenden Lieferungen, bislang nicht gelistete Stoffe in diese Liste aufgenommen werden. Die Liefergegenstände dürfen außerdem kein Asbest, Biozide oder radioaktives Material enthalten. Sollten Stoffe in den Liefergegenständen enthalten sein, so ist dies dem Besteller schriftlich vor der Lieferung unter Angabe des Stoffes, der Identifikationsnummer (z.B. CAS-Nr.) und einem aktuellen Sicherheitsdatenblatt mitzuteilen. Die Lieferung dieser Liefergegenstände bedarf einer gesonderten Freigabe durch den Besteller.
13.3 Der Lieferant verpflichtet sich, durch angemessene Maßnahmen in seiner Organisation und bezogen auf die eigene Lieferkette darauf hinzuwirken, dass sog. Konfliktmineralien im Sinne der Sektionen 1502 und 1504 des US-amerikanischen Dodd-Frank-Act (insbesondere aus der Demokratischen Republik Kongo und deren Nachbarstaaten stammendes Columbit-Tantalit (Coltan), Zinn, Wolframit und Gold sowie deren Derivate) in den an den Besteller zu liefernden Produkten nicht enthalten sind.
13.4 Der Lieferant ist verpflichtet, den Besteller von jeglicher Haftung im Zusammenhang mit der Nichteinhaltung der oben genannten Verordnungen durch den Lieferanten freizustellen bzw. den Besteller für Schäden zu entschädigen, die ihm aus der Nichteinhaltung der Verordnungen durch den Lieferanten entstehen oder mit ihr zusammenhängen. Der Lieferant hat ferner die für die Entsorgung von Abfällen und Reststoffen einschlägigen Vorschriften zu berücksichtigen und den Besteller auf eventuelle Produktbehandlungs-, -lagerungs und Entsorgungserfordernisse hinzuweisen.

## 14. Eigentumsvorbehalt, Modelle, Werkzeuge und Geheimhaltung

14.1 Eigentumsvorbehaltsrechte des Lieferanten werden nicht anerkannt.
14.2 Sofern der Besteller Stoffe, Teile, Behälter usw. dem Lieferanten beistellt, behält er sich hieran das Eigentum vor. Verarbeitung oder Umbildung dieser Teile erfolgen für den Besteller. Wird die Vorbehaltsware mit anderen, nicht dem Besteller gehörenden Gegenständen verarbeitet, so erwirbt der Besteller das Miteigentum an der neuen Sache im Verhältnis des Wertes der Sache des Bestellers zu den anderen verarbeitenden Gegenständen zur Zeit der Verarbeitung.
14.3 Modelle und Werkzeuge, die auf Kosten des Bestellers vom Lieferanten angefertigt werden, gehen nach Bezahlung in das Eigentum des Bestellers über. Sie sind vom Lieferanten sorgfältig zu behandeln, ausschließlich für die Herstellung der bestellten Waren einzusetzen, als Eigentum des Bestellers zu kennzeichnen und – soweit möglich – getrennt von den anderen Produkten des Lieferanten zu lagern sowie gegen Katastrophen wie Feuer, Wasser, Diebstahl, Verlust und sonstige Beschädigungen auf Kosten des Lieferanten zu versichern. Der Lieferant ist verpflichtet, an den Werkzeugen etwa erforderliche Wartungs- und Inspektionsarbeiten sowie alle Instandhaltungs- und Instandsetzungsarbeiten auf eigene Kosten rechtzeitig durchzuführen. Ein

Weiterverkauf der mit diesen Modellen und Werkzeugen hergestellten Teile ist ohne ausdrückliche schriftliche Genehmigung des Bestellers nicht gestattet.

14.4 Unterlagen, Zeichnungen, Pläne und Skizzen, sowie sonstiges Know-how des Bestellers, die der Besteller dem Lieferanten zur Anfertigung der bestellten Lieferung und/oder Leistung gleich in welcher Form überlässt, bleiben Eigentum des Bestellers. Sie sind Betriebsgeheimnisse des Bestellers und sind vertraulich zu behandeln. Der Lieferant verpflichtet sich, sie sorgfältig zu behandeln, sie nur solchen Mitarbeitern zur Verfügung zu stellen, die sie für die Ausführung des Vertrages benötigen und die ihrerseits zur Geheimhaltung verpflichtet sind, sie nicht Dritten zur Verfügung zu stellen, Kopien nur für den Zweck der Durchführung der Bestellung anzufertigen und nach Durchführung der Lieferung/Leistung alle Unterlagen einschließlich der Kopien dem Besteller zurückzusenden oder nach Wahl des Bestellers zu vernichten.

## 15. Datenschutz

Der Besteller ist berechtigt, personenbezogene Daten des Lieferanten zu erheben, zu speichern, zu nutzen oder (d.h. an Geschäftspartner, Behörden, Banken, Versicherungen, externe Berater, Dienstleistungsunternehmen) zu übermitteln, sofern dies zur Durchführung des Rechtsgeschäftes erforderlich ist oder betroffene Personen eingewilligt haben. Die Aufbewahrung von solchen personenbezogenen Daten erfolgt solange dies zur Erfüllung des Rechtsgeschäfts erforderlich ist, Rechtsansprüche aufgrund des Rechtsgeschäfts geltend gemacht werden können, für die Dauer gesetzlicher Aufbewahrungsfristen und solange behördliche Verfahren anhängig sind, in denen die Daten benötigt werden (können). Soweit die Verarbeitung von Daten auf der Einwilligung der jeweiligen betroffenen Person beruht, kann diese jederzeit widerrufen werden. Betroffene Personen haben das Recht, Auskunft über die zu ihrer Person gespeicherten Daten sowie deren Verarbeitungs- und Verwendungszweck zu erhalten. Etwaige Auskunftsersuchen oder die Geltendmachung weiterer Betroffenenrechte sind stets an den Besteller zu richten und werden im Rahmen nationaler Gesetze wahrgenommen.

## 16. Warenursprung und Exportkontrolle

16.1 Auf Anforderung des Bestellers ist der Lieferant zur Abgabe eines Ursprungsnachweises verpflichtet, welcher den zum Tag der Ausstellung gültigen rechtlichen Erfordernissen entspricht. Er stellt diese dem Besteller kostenfrei zur Verfügung. Werden Langzeitlieferantenerklärungen verwendet, hat der Lieferant Veränderungen der Ursprungseigenschaft dem Besteller mit der Annahme der Bestellung unaufgefordert mitzuteilen. Das tatsächliche Ursprungsland ist in jedem Fall in den Geschäftspapieren zu benennen, auch wenn keine Präferenzberechtigung vorliegt.

16.2 Der Lieferant ist verpflichtet, den Besteller über etwaige Genehmigungspflichten bei (Re-)Exporten seiner Waren gemäß deutschen, europäischen, US-amerikanischen und anderen anwendbaren Ausfuhr- und Zollbestimmungen zu unterrichten. Hierzu gibt der Lieferant, sofern nicht bereits in seinem Angebot enthalten, bei der Auftragsbestätigung und auf jeder Rechnung bei den betreffenden Warenpositionen folgende Informationen an: die statistische Warennummer, die AL-Nr. (Ausfuhrlistennummer) der EG-Dual-Use-Verordnung in der jeweils gültigen Fassung oder Teil I der Ausfuhrliste (Anlage AL zur deutschen Außenwirtschaftsverordnung) und die ECCN (Export Control Classification Number) nach US-Exportrecht.

16.3 Auf Anforderung des Bestellers ist der Lieferant verpflichtet, dem Besteller alle weiteren Außenhandelsdaten zu den Waren und deren Bestandteilen schriftlich mitzuteilen, sowie den Besteller unverzüglich über alle Änderungen der in den Ziffern 16.1 und 16.2 genannten Daten schriftlich zu informieren. Im Falle der Unterlassung oder der fehlerhaften Mitteilung vorstehender Angaben ist der Besteller unbeschadet weiterer Ansprüche berechtigt, vom Vertrag zurückzutreten.

## 17. Rücktritts- und Kündigungrechte

17.1 Der Besteller kann jederzeit den Vertrag schriftlich unter Einhaltung einer Frist von vier Wochen kündigen, ohne dass es hierfür eines Grundes bedarf. Dem Lieferanten steht in diesem Fall der Preis für die bis zum Datum der Kündigung vertragsgemäß erbrachten Leistungen gegen entsprechenden Nachweis zu, wobei ersparte Aufwendungen in Abzug gebracht werden müssen.

17.2 Der Besteller ist über die gesetzlichen Rücktritts- bzw. Kündigungsrechte hinaus zum Rücktritt bzw. Kündigung vom Vertrag berechtigt, wenn eine wesentliche Verschlechterung der Vermögensverhältnisse des Lieferanten eintritt oder einzutreten droht und hierdurch die Liefer- und Leistungsverpflichtung gefährdet ist. Der Besteller ist weiter zum Rücktritt bzw. zur Kündigung vom Vertrag berechtigt, wenn der Lieferant unter den beherrschenden Einfluss eines Wettbewerbers des Bestellers gerät.

17.3 Das Recht der Parteien zur Kündigung dieses Vertrags aus wichtigem Grund nach § 314 BGB bleibt unberührt. Als wichtiger Grund gilt insbesondere ein Fall, dass Lieferant, ein Organmitglied, ein Mitarbeiter oder ein sonstiger Erfüllungsgehilfe des Lieferantens oder eine Person, derer sich Lieferant zur Vermarktung seiner Produkte bedient, gegen die Vorgaben in Ziffer 18.1, den VOITH Code of Conduct oder die in Ziffer 18.3 genannten menschenrechts- und umweltbezogenen Vorgaben verstoßen hat oder ein entsprechender, durch Tatsachen erhärteter Verdacht besteht, es sei denn, der Verstoß ist unwesentlich und wird vom Lieferanten sofort und dauerhaft abgestellt.

## 18. Unternehmerische Verantwortung

18.1 Der Lieferant bekennt sich im Rahmen seiner unternehmerischen Verantwortung dazu, dass bei oder im Zusammenhang mit der Herstellung und dem Vertrieb seiner Waren bzw. Erbringung seiner Leistungen die gesetzlichen Vorschriften, einschließlich der Gesetze zum Schutz der Umwelt gewahrt sind, arbeitsrechtliche Bestimmungen und Gesetze zur Gesunderhaltung der Mitarbeiter eingehalten, sowie Kinder- und Zwangsarbeit nicht geduldet werden. Der Lieferant bestätigt zudem mit Annahme der Bestellung, sich auf keinerlei Form von Bestechung und Korruption einzulassen, noch diese zu tolerieren. Der Besteller weist in diesem Zusammenhang auf den im VOITH-Konzern geltenden „VOITH Code of Conduct“ hin, der unter http://www.Voith.com eingesehen werden kann. Der Besteller erwartet vom Lieferanten, dass dieser sich zur Einhaltung der darin enthaltenen Regeln und Prinzipien bekennt und ihre Beachtung unterstützt.

18.2 Der Lieferant sichert insbesondere zu, die jeweils geltenden Gesetze zur Regelung des allgemeinen Mindestlohns einzuhalten und von ihm beauftragte Unterlieferanten in gleichem Umfang zu verpflichten. Ferner ist der Lieferant verpflichtet, die in Deutschland und der EU geltenden exportrechtlichen Bestimmungen zu beachten. Auf Verlangen des Bestellers weist der Lieferant die Einhaltung der vorstehenden Zusicherung nach. Bei Verstoß gegen vorstehende Zusicherung stellt der Lieferant den Besteller von Ansprüchen Dritter frei und ist zur Erstattung von Bußgeldern verpflichtet, die dem Besteller in diesem Zusammenhang auferlegt werden.

18.3 Lieferant verpflichtet sich insbesondere zur Einhaltung der folgenden menschenrechts- und umweltbezogenen Vorgaben:

- Verbot der Kinderarbeit betreffend Einhaltung des Mindestalters für die Zulassung zur Beschäftigung gemäß ILO-Übereinkommen Nr. 138 sowie betreffend das Verbot und unverzügliche Maßnahmen zur Beseitigung der schlimmsten Formen der Kinderarbeit gemäß Art. 3 ILO-Übereinkommen Nr. 182;
- Verbot der Beschäftigung von Personen in Zwangsarbeit gemäß ILO-Übereinkommen Nr. 29;
- Verbot aller Formen der Sklaverei, sklavenähnlicher Praktiken, Leibeigenschaft oder Unterdrückung im Umfeld der Arbeitsstätte;
- Einhaltung der geltenden Pflichten des Arbeitsschutzes gemäß Recht am Beschäftigungsort;
- Verbot der Missachtung der Koalitionsfreiheit;
- Verbot der Ungleichbehandlung in Beschäftigung aufgrund von nationaler, ethnischer Abstammung, sozialer Herkunft, Gesundheitsstatus, Behinderung, sexueller Orientierung, Alter, Geschlecht, politischer Meinung, Religion, Weltanschauung, sofern dies nicht in den Erfordernissen der Beschäftigung begründet ist;
- Verbot des Vorenthaltens eines angemessenen Lohns;
- Verbot der Umweltverschmutzung betreffend Boden, Gewässer, Luft, schädlicher Lärmemission oder übermäßigen Wasserverbrauchs;
- Verbot der widerrechtlichen Zwangsräumung sowie des widerrechtlichen Entzugs von Land, Wäldern und Gewässern bei dem Erwerb, der Bebauung oder anderweitigen Nutzung von Land, Wäldern und Gewässern, deren Nutzung der Lebensgrundlage einer Person sichert;
- Verbot der Beauftragung oder Nutzung privater oder öffentlicher Sicherheitskräfte zum Schutz des unternehmerischen Projekts, welche hierbei Folter und grausame, unmenschlicher oder erniedrigender Behandlung anwenden, dabei Leib oder Leben verletzen, oder die Vereinigungs- und Koalitionsfreiheit missachten;
- Verbot eines über die vorgenannten Verletzungshandlungen hinausgehenden Tuns oder pflichtwidrigen Unterlassens, das unmittelbar geeignet ist, in besonders schwerwiegender Weise eine geschützte Rechtsposition zu beeinträchtigen und dessen Rechtswidrigkeit offensichtlich ist;
- Verbot der Herstellung und Verwendung von Quecksilber und Quecksilberverbindungen sowie der Behandlung von Quecksilberabfällen gemäß den Bestimmungen des Minamata-Übereinkommens (Art. 4 Abs. 1 und Anlage A Teil I, Art. 5 Abs. 2 und Anlage B Teil I, Art. 11 Abs. 3);
- Verbot der Produktion und Verwendung von Chemikalien sowie der nicht umweltgerechten Handhabung, Sammlung, Lagerung und Entsorgung von Abfällen nach den Regelungen der anwendbaren Rechtsordnung gemäß Stockholmer Übereinkommen über persistente organische Schadstoffe (23.05.2001, 06.05.2005) und EU-Verordnung über persistente organische Schadstoffe 2021/277 (Art. 3 Abs. 1a und Anlage A, Art. 6 Abs. 1d (i), (ii));

- Folgende Verbote nach dem Basler Übereinkommen über die Kontrolle der grenzüberschreitenden Verbringung gefährlicher Abfälle und ihrer Entsorgung (22.03.1989 und 06.05.2014): Verbot der Ausfuhr gefährlicher und anderer Abfälle gemäß Art. 1 Abs. 1, 2 des) nach Art. 4 Abs. 1b, 1c, Abs. 5, Abs. 8 S.1, Art. 4A, und Art. 36 der Verordnung (EG) Nr. 1013/2006; Verbot der Einfuhr gefährlicher und anderer Abfälle aus einer Nichtvertragspartei des Basler Übereinkommens (Art. 4 Abs. 5).

Für den Fall, dass sich die menschenrechts- und umweltbezogenen Vorgaben für Besteller ändern, wird Lieferant einer Anpassung dieser Ziffer 3, die die Änderung der menschenrechts- und umweltbezogenen Vorgaben umsetzt, zustimmen. Besteller wird die Änderungen der menschenrechts- und umweltbezogenen Vorgaben jeweils unverzüglich in Schrift- oder Textform Lieferant mitteilen.

Lieferant wird gegenüber den eigenen Unterlieferanten und darüber hinaus entlang der ganzen eigenen Lieferkette die in dieser Ziffer 3 genannten menschenrechts- und umweltbezogenen Vorgaben in angemessener Weise adressieren und insbesondere deren Einhaltung durch die eigenen Unterlieferanten bzw. im Falle bestehender Verletzung menschenrechts- oder umweltbezogener Pflichten deren Beendigung im Wege geeigneter vertraglicher Regelungen sicherstellen. Dies umfasst im Rahmen des rechtlich Möglichen und des Zumutbaren auch die ernsthafte Bemühung um die Aufnahme einer Vereinbarung, die die Weitergabe dieser Verpflichtung durch die unmittelbaren Lieferanten des Lieferantens gegenüber den eigenen Lieferanten sicherstellt.

Lieferant verpflichtet sich ferner zur sorgfältigen Auswahl seiner Lieferanten insbesondere im Hinblick auf die menschenrechts- und umweltbezogenen Vorgaben gemäß dieser Ziffer 3 und wird Hinweisen auf Verstöße gegen die menschenrechts- und umweltbezogenen Vorgaben angemessen nachgehen und diese bei der Auswahl der Lieferanten berücksichtigen.

18.4 Besteller hat das Recht, durch Kontrollen beim Lieferanten vor Ort die Einhaltung der in Ziffer 3 genannten menschenrechts- und umweltbezogenen Vorgaben zu überprüfen (Audit-Recht). Das Audit-Recht kann Besteller durch eigene Mitarbeiter, durch einen durch Besteller beauftragten fremden Dritten (z.B. einen Rechtsanwalt oder Wirtschaftsprüfer) oder durch die Inanspruchnahme anerkannter Zertifizierungs- oder Audit-Systeme ausüben. Besteller wird die Ausübung des Audit-Rechts dem Lieferanten gegenüber grundsätzlich mit angemessener Frist ankündigen, es sei denn, es liegt Gefahr im Verzug vor oder die Ankündigung würde die Effektivität des Audits gefährden, erheblich mindern oder beseitigen. Die Ausübung des Audit-Rechts erfolgt grundsätzlich zu den üblichen Geschäftszeiten in den Geschäftsräumen des Lieferantens. Lieferant verpflichtet sich, von Besteller verlangte Dokumente, Unterlagen, Namen von Unterlieferanten innerhalb der Lieferkette und soweit bekannt („Lieferkettendokumentation“) zur Einsichtnahme durch Besteller für einen angemessenen Zeitraum, mindestens jedoch für [zehn] Arbeitstage, („Audit-Zeitraum“) bereitzustellen. Auf Anforderung von Besteller wird Lieferant auf eigene Kosten die Lieferkettendokumentation auch in einem geeigneten, den aktuellen IT-Sicherheitsstandards entsprechenden Online-Datenraum für den Audit-Zeitraum zur Verfügung stellen und Besteller Zugriff von den eigenen Geschäftsräumen aus gewähren. Außerdem wird Lieferant Besteller Zugang zu seinen Mitarbeitern und Organmitgliedern gewähren, z.B. um die Durchführung von Interviews zu ermöglichen, die der Wahrnehmung des Audit-Rechts dienen. Vorgaben des Datenschutzes sind bei Ausübung des Audit-Rechts durch Besteller einzuhalten, die Wahrung von Geschäftsgeheimnissen des Lieferants ist zu berücksichtigen, soweit dies nicht der Erfüllung gesetzlicher Pflichten durch Besteller entgegensteht.

18.5 Lieferant wird auf Verlangen von Besteller Schulungen und Weiterbildungen durch Besteller zur gemäß diesem Vertrag geschuldeten Einhaltung der in Ziffer 18.3 genannten menschenrechts- und umweltbezogenen Vorgaben unterstützen und ermöglichen, die eigenen relevanten Mitarbeiter benennen und deren Teilnahme an den Schulungen und Weiterbildungen im Rahmen der rechtlichen Möglichkeiten sicherstellen. Die Details der Organisation und Durchführung von Schulungen und Weiterbildungen gemäß dieser Ziffer 18.5 werden Besteller und Lieferant im Einzelfall in gegenseitigem Einvernehmen festlegen. Dabei werden die Interessen des Lieferantens im Hinblick auf die Art und Dauer der Schulungen, ihre Häufigkeit und den Kreis der Teilnehmer angemessen berücksichtigt, damit eine übermäßige Belastung des Lieferantens vermieden wird. Die Schulungen können sowohl als e-Learning, im Online-Format oder im Rahmen einer Präsenzveranstaltung erfolgen.

### 19. Allgemeine Bestimmungen

19.1 Personen, die zur Ausführung des Vertrages Arbeiten auf dem Gelände des Bestellers oder der mit dem Besteller verbundenen Unternehmen ausführen, haben die Bestimmungen der jeweiligen Betriebsordnung zu beachten. Die Haftung für Unfälle, die diesen Personen auf dem Werksgelände zustoßen, ist ausgeschlossen, soweit sie nicht durch vorsätzliche oder grob fahrlässige Pflichtverletzung unserer gesetzlichen Vertreter oder deren Erfüllungshilfen verursacht wurden.

19.2 Die Benutzung von Anfragen, Bestellungen und des damit verbundenen Schriftverkehrs zu Werbezwecken ist nicht gestattet. Der Lieferant darf nur mit vorheriger schriftlicher Zustimmung des Bestellers mit der Geschäftsbeziehung zu diesem werben oder sie als Referenz verwenden.

19.3 Forderungsabtretungen ohne ausdrückliche schriftliche Genehmigung des Bestellers sind ausgeschlossen.

19.4 Aufrechnungsrechte und Zurückbehaltungsrechte stehen den Parteien nur zu, wenn ihre Gegenansprüche rechtskräftig festgestellt oder unbestritten sind.

19.5 Für die vertraglichen Beziehungen gilt ausschließlich deutsches Recht unter Ausschluss des Kollisions- und des UN-Kaufrechts (CISG).

19.6 Gerichtsstand für beide Parteien ist das am Sitz des Bestellers zuständige Gericht. Der Besteller kann auch am Sitz des Lieferanten klagen.

19.7 Sollten einzelne Bestimmungen dieser Allgemeinen Einkaufsbedingungen ganz oder teilweise ungültig sein oder werden, so berührt dies die Wirksamkeit der übrigen Bestimmungen nicht.

| | |
|---|---|
| Anhang 1: | Bedingungen für die Lieferung von Software/Hardware und/oder OT & E/E Systemlösungen einschl. Dokumentation \| Version 2022 |
| Anhang 2: | Bedingungen für Lieferungen, Leistungen, Erstellung von Software/Hardware im Rahmen von IT & OT & E/E Systemen \| Version 2022 |

# Anhang 1: Bedingungen für Lieferungen von Software/Hardware und/oder OT & E/E Systemlösungen einschließlich Dokumentation

Die Allgemeinen Einkaufsbedingungen von Voith in ihrer jeweils gültigen Fassung werden durch die nachfolgenden Bedingungen ergänzt, die für alle Lieferungen von Software/Hardware und/oder OT & E/E Systemlösungen einschließlich Dokumentation im Bereich der Informationstechnologie (IT)/Operational Technology (OT) gelten.

Diese Bedingungen gelten zusätzlich und gehen im Falle von Widersprüchen den Allgemeinen Einkaufsbedingungen von Voith vor.

DEFINITIONEN

| | |
|---|---|
| Informationstechnologie (IT) | Die Informationstechnologie (IT) umfasst die Entwicklung, Wartung und Nutzung von Computersystemen, Software und Netzwerken für die Verarbeitung und Verteilung von Daten; |
| Operationelle Technologie (OT) | Operationelle Technologie (OT) ist Hard- und Software, die durch die direkte Überwachung und/oder Steuerung von Industrieanlagen, Maschinen, Vermögenswerten, Prozessen und Ereignissen eine Veränderung feststellt oder bewirkt; |
| E/E-Systeme | Elektrische und elektronische Systeme |
| Daten der Kunden | bezeichnet alle Informationen und Daten (einschließlich Texten, Dokumenten, Zeichnungen, Diagrammen, Bildern oder Tönen), die Eigentum des Auftraggebers und/oder eines seiner Vertreter sind, an den Auftraggeber lizenziert wurden oder sich auf den Auftraggeber und/oder einen seiner Vertreter beziehen, unabhängig davon, ob sie in menschlicher oder maschinenlesbarer Form vorliegen, und die in jedem Fall vom Auftragnehmer oder einem seiner Unterauftragnehmer gemäß oder in Verbindung mit diesen Geschäftsbedingungen erzeugt, an ihn geliefert oder anderweitig aufbewahrt werden; |
| Sicherheitsvorfall | ein Ereignis, das den tatsächlichen oder versuchten unbefugten Zugriff auf und/oder die Nutzung der Systeme, die die Kundendaten enthalten, und/oder den unbefugten Zugriff auf, die Nutzung von, die Zerstörung, den Verlust oder die Veränderung von Kundendaten im Zusammenhang mit diesen Geschäftsbedingungen beinhaltet; solche Vorfälle können als kritischer Sicherheitsvorfall, schwerer Sicherheitsvorfall oder Sicherheitsvorfall niedriger Priorität eingestuft werden. |
| Kritischer Sicherheitsvorfall | ein Sicherheitsvorfall, der zu einer schwerwiegenden Unterbrechung der geleisteten Arbeit führt; |
| Großer Sicherheitsvorfall | ein Sicherheitsvorfall, der zu einer Minderung der Leistung der gelieferten Arbeit führt oder zu einer Offenlegung der Kundendaten oder anderer Daten, die vom Kunden oder dem Lieferanten im Zusammenhang mit diesen Bedingungen verwendet werden, in der Öffentlichkeit führen kann; |
| Sicherheitsvorfall mit niedriger Priorität | ein Sicherheitsvorfall, der keine wesentlichen Auswirkungen auf die Verfügbarkeit oder Leistung der gelieferten Arbeit hat; |
| Informationswert | jedes Informationssystem/IT-System, das Informationen enthält, die zu einer Organisation gehören |
| Informationssystem / IT-System | Ein Informationssystem ist eine Kombination aus Informationstechnologie, Prozessen, digitalen Informationen und Benutzeraktivitäten, die den Betrieb einer Organisation unterstützen; |
| Sicherheitsbedrohung | ist eine mögliche Gefahr, die eine Sicherheitslücke ausnutzen könnte, um einen Sicherheitsvorfall zu verursachen, der zu einem Schaden führen kann; |
| Sicherheitsschwachstelle | ist eine Schwachstelle in einem Informationssystem, die von einer oder mehreren Sicherheitsbedrohungen ausgenutzt werden kann; |
| Risikobewertung | Eine Risikobewertung ist ein Prozess, bei dem (a) die Risiken in Bezug auf ein Informationsgut und anerkannte Sicherheitsbedrohungen identifiziert werden und (b) die Gesamtwirkung der Wahrscheinlichkeit, dass die Risiken eintreten, und die Auswirkungen, wenn sie eintreten, bewertet werden; |
| Sicherheitsrisiko | Ein Sicherheitsrisiko ist die Wahrscheinlichkeit, dass etwas Schlimmes passiert, das einem Informationswert Schaden zufügt; |
| Bewertung des Sicherheitsrisikos | eine Bestimmung des quantitativen oder qualitativen Risikowertes in Bezug auf eine konkrete Situation und eine anerkannte Bedrohung für die Sicherheit der Kundendaten und/oder der Systeme; |
| Bewertung der Anfälligkeit | eine Sicherheitsrisikobewertung, die zur Identifizierung, Quantifizierung und Priorisierung (oder Rangfolge) der Schwachstellen in einem Computersystem, einschließlich der zugehörigen Netzwerke, Datenbanken und Softwareanwendungen, führt; |
| Verbundene Unternehmen | jedes Unternehmen, das als verbundenes Unternehmen des Kunden im Sinne der §§ 15 ff AktG anzusehen ist. Darüber hinaus kann der Kunde in einer Änderungsvereinbarung weitere Unternehmen als Verbundene Unternehmen des Kunden definieren; |
| Kundengruppe | bezeichnet den Kunden zusammen mit den mit ihm verbundenen Unternehmen; |

## 1 Open-Source-Software

Open-Source-Software ("OSS") ist Software, die im Allgemeinen kostenlos und quelloffen zur Verfügung gestellt wird und unter einer Lizenz verwendet werden kann, die die Weiterverbreitung der Software nicht einschränkt, Änderungen und abgeleitete Werke zulässt und deren Weiterverbreitung unter denselben Bedingungen wie die Lizenz der ursprünglichen Software erlauben muss ("OSS-Lizenz"). Zu den OSS-Lizenzen gehören unter anderem die "Berkeley Software Distribution License" (BSD), die "GNU General Public License" (GPL) und die "GNU Lesser General Public License" (LGPL). Copyleft-Lizenzen sind Lizenzen, die vorschreiben, dass alle abgeleiteten oder auf dem Programm basierenden Arbeiten nur unter den ursprünglichen Lizenzbedingungen verbreitet oder weitergegeben werden dürfen ("Copyleft-Lizenz").

1.1 Anforderungen

OSS kann in der vom Lieferanten gelieferten Software enthalten sein. Der Lieferant wird dem Auftraggeber alle Informationen und Materialien über die Verwendung von OSS in der Software zur Verfügung stellen. Dies umfasst:

(i) eine transparente und vollständige Liste aller unter einer OSS-Lizenz lizenzierten Komponenten,

(ii) den Lizenztext jeder OSS-Lizenz,

(iii) Urheberrechtshinweise,

(iv) die Ergebnisse einer dem Stand der Technik entsprechenden Sicherheits- und Schwachstellenüberwachung des gesamten verwendeten Open-Source-Codes und

(v) Eine klare Beschreibung und Dokumentation der verwendeten OSS-Komponenten.

Der Kunde wird die Genehmigung nach eigenem Ermessen erteilen. Eine erteilte Genehmigung ist zu widerrufen, wenn die bereitgestellten Informationen oder Materialien falsch oder unvollständig sind.

OSS-Lizenztexte und der dazugehörige Quellcode müssen separat zur Verfügung gestellt werden. Der Lieferant wird den gesamten Open-Source-Code zur Verfügung stellen, soweit dies von den geltenden Lizenzen verlangt wird.

Der Lieferant wird den Auftraggeber in die Lage versetzen, alle Anforderungen aus den geltenden OSS-Lizenzen jederzeit vollständig zu erfüllen.

Diese Anforderungen gelten auch für alle Updates, Patches, Upgrades oder neuen Versionen der Software.

1.2 Verantwortung
Der Lieferant ist sich seiner besonderen Verantwortung bewusst, den Auftraggeber vor Schäden zu schützen, die durch die Integration von OSS-Software in die vom Lieferanten gelieferte Software und die Nutzung dieser Software durch den Auftraggeber entstehen. In Anbetracht dessen wird der Lieferant besonders darauf achten, dass alle Rechte von 3rd Parteien nachgewiesen und gewährleistet sind.
1.3 Entschädigung
Der Lieferant wird den Kunden und die verbundenen Unternehmen, Mitarbeiter, Direktoren oder Vertreter des Kunden von allen Ansprüchen, Schäden, Ausgaben und Haftungen freistellen, die in direktem oder indirektem Zusammenhang mit der Verletzung einer der vorstehenden Verpflichtungen durch den Lieferanten entstehen, unabhängig von der Rechtsgrundlage.

## 2 Lebenszyklus der Softwareentwicklung

Für Lieferungen, die eine Softwareentwicklung beinhalten, muss der Lieferant einen Prozess zur sicheren Softwareentwicklung einrichten.
(i) ein Konzept für den Lebenszyklus der sicheren Softwareentwicklung gemäß den bekannten Normen wie IEC 62443 4-1 anwenden. Eine Zertifizierung wird erwartet.
(ii) den Nachweis erbringen, dass die ermittelten Sicherheitsanforderungen und die entsprechenden Sicherheitskontrollen entworfen und in der Software implementiert sind.
(iii) sicherzustellen, dass geeignete Sicherheitstests, einschließlich, aber nicht beschränkt auf statische und dynamische Codeprüfungen und kontinuierliche Schwachstellenbewertung, in den Entwicklungs- und Integrationsabläufen durchgeführt und alle aufgedeckten Probleme vor der Freigabe der Software behoben werden; und
(iv) dem Auftraggeber und/oder seinen Beauftragten die Durchführung von Schwachstellenanalysen der entwickelten Software ermöglichen. Wenn der Auftraggeber eine Schwachstelle mit einer Risikobewertung von "hoch" oder "kritisch" feststellt, wird der Lieferant Maßnahmen ergreifen, um die Risiken vor der Freigabe der Software zu mindern.

## 3 Schwachstellenmanagement

(i) Der Lieferant wird einen unabhängigen und vertrauenswürdigen Schwachstellenbewertungsdienst beauftragen und/oder mit einem vom Kunden benannten unabhängigen Dritten bei der Durchführung von Schwachstellenbewertungen zusammenarbeiten und diesen unterstützen.
(ii) Der Lieferant überprüft monatlich die Informationsquellen des Lieferanten für Bedrohungen und Schwachstellen auf die neuesten Schwachstellen, Bedrohungen und Abhilfemaßnahmen, die für die von ihm verwalteten Systeme relevant sind.
(iii) Der Lieferant muss einen Plan zur Behebung von Schwachstellen umsetzen, sobald eine Schwachstelle identifiziert wurde oder um zu verhindern, dass eine Schwachstelle auftritt, und er muss Prioritäten setzen und die Fortschritte des Plans verfolgen und überwachen. Alle Abhilfepläne sind für künftige Referenzzwecke zu dokumentieren. Schwachstellen, die erhebliche Auswirkungen auf die Sicherheit haben, müssen so schnell wie möglich behoben werden. Bei geringeren und mittleren Risiken ist der Zeitplan für die Behebung unter Berücksichtigung der Kosten, des Zeitaufwands und der Anstrengungen, die zur Minderung der Risiken erforderlich sind, festzulegen.
(iv) Der Lieferant benachrichtigt den Kunden unverzüglich, wenn er es versäumt, eine kritische oder hoch eingestufte Schwachstelle zu beheben, und schlägt dem Kunden die erforderlichen Sicherheitskontrollen vor.
(v) Der Lieferant stellt sicher, dass alle anpassbaren Produkte eine Dokumentation zur sicheren Parametrisierung enthalten.
(vi) Aktivitäten im Rahmen des Schwachstellenmanagements des Lieferanten, wie Schwachstellenbewertungen, unabhängig von Art oder Ziel, sowie alle Arbeiten und die Zeit, die zur Durchführung von Abhilfemaßnahmen erforderlich sind, gehen zu Lasten des Lieferanten und werden dem Kunden nicht in Rechnung gestellt.

## 4 Sicherheitsmanagement

(i) Der Lieferant wird eine Person (den "Sicherheitsbeauftragten des Lieferanten") ernennen, die folgende Aufgaben hat

- alle Aspekte der Sicherheit im Einklang mit dem Abkommen zu koordinieren und zu verwalten; und
- im Falle eines Sicherheitsvorfalls als einziger Ansprechpartner im Namen des Lieferanten und seiner Unterauftragnehmer zu fungieren.

(ii) Falls der Anbieter den Sicherheitsbeauftragten des Anbieters auswechseln möchte, wird er den Kunden schriftlich davon in Kenntnis setzen und ihm die Kontaktdaten der Ersatzperson mitteilen.

# Anhang 2: Bedingungen für Lieferungen, Leistungen, Erstellung von Software/ Hardware im Rahmen von IT & OT & E/E Systemen einschl. Dokumentation

Die Allgemeinen Einkaufsbedingungen von Voith in ihrer jeweils gültigen Fassung werden durch die nachfolgenden Bedingungen ergänzt, die für alle Lieferungen und Leistungen im Bereich der Informationstechnologie (IT)/Operational Technology (OT) & E/E Systemen (Teil A) und die Erstellung oder Anpassung von Software oder die Erbringung damit zusammenhängender Dienstleistungen (Teil B) gelten.

Diese Bedingungen gelten zusätzlich und gehen im Falle von Widersprüchen den Allgemeinen Einkaufsbedingungen von Voith vor.

DEFINITIONEN

| | |
|---|---|
| Informationstechnologie (IT) | Die Informationstechnologie (IT) umfasst die Entwicklung, Wartung und Nutzung von Computersystemen, Software und Netzwerken für die Verarbeitung und Verteilung von Daten; |
| Operationelle Technologie (OT) | Operationelle Technologie (OT) ist Hard- und Software, die durch die direkte Überwachung und/oder Steuerung von Industrieanlagen, Maschinen, Vermögenswerten, Prozessen und Ereignissen eine Veränderung feststellt oder bewirkt; |
| E/E-Systeme | Elektrische und elektronische Systeme |
| Kundendaten | bezeichnet alle Informationen und Daten (einschließlich Texten, Dokumenten, Zeichnungen, Diagrammen, Bildern oder Tönen), die Eigentum des Kunden und/oder eines seiner Vertreter sind, für die dieser eine Lizenz erteilt hat oder die sich auf den Kunden und/oder einen seiner Vertreter beziehen, unabhängig davon, ob sie in menschlicher Form oder in maschinenlesbarer Form vorliegen, und die in jedem Fall vom Lieferanten oder einem seiner Subunternehmer gemäß oder in Verbindung mit diesen Bedingungen erzeugt, an ihn geliefert oder anderweitig gespeichert werden; |
| Sicherheitsvorfall | ein Ereignis, das den tatsächlichen oder versuchten unbefugten Zugriff auf und/oder die Nutzung der Systeme, die die Kundendaten enthalten, und/oder den unbefugten Zugriff auf, die Nutzung von, die Zerstörung, den Verlust oder die Veränderung von Kundendaten im Zusammenhang mit diesen Geschäftsbedingungen beinhaltet; solche Vorfälle können als kritischer Sicherheitsvorfall, schwerer Sicherheitsvorfall oder Sicherheitsvorfall niedriger Priorität eingestuft werden. |
| Kritischer Sicherheitsvorfall | ein Sicherheitsvorfall, der zu einer schwerwiegenden Unterbrechung der geleisteten Arbeit führt; |
| Großer Sicherheitsvorfall | ein Sicherheitsvorfall, der zu einer Minderung der Leistung der gelieferten Arbeit führt oder zu einer Offenlegung der Kundendaten oder anderer Daten, die vom Kunden oder dem Lieferanten im Zusammenhang mit diesen Bedingungen verwendet werden, in der Öffentlichkeit führen kann; |
| Sicherheitsvorfall mit niedriger Priorität | ein Sicherheitsvorfall, der keine wesentlichen Auswirkungen auf die Verfügbarkeit oder Leistung der gelieferten Arbeit hat; |
| Persönliche Daten | hat die gleiche Bedeutung wie in der Allgemeinen Datenschutzverordnung 2016/679 festgelegt; |
| Informationswert | jedes Informationssystem/IT-System, das Informationen enthält, die zu einer Organisation gehören |
| Informationssystem / IT-System | Ein Informationssystem ist eine Kombination aus Informationstechnologie, Prozessen, digitalen Informationen und Benutzeraktivitäten, die den Betrieb einer Organisation unterstützen; |
| Sicherheitsbedrohung | ist eine mögliche Gefahr, die eine Sicherheitslücke ausnutzen könnte, um einen Sicherheitsvorfall zu verursachen, der zu einem Schaden führen kann; |
| Sicherheitsschwachstelle | ist eine Schwachstelle in einem Informationssystem, die von einer oder mehreren Sicherheitsbedrohungen ausgenutzt werden kann; |
| Risikobewertung | Eine Risikobewertung ist ein Prozess, bei dem (a) die Risiken in Bezug auf ein Informationsgut und anerkannte Sicherheitsbedrohungen identifiziert werden und (b) die Gesamtwirkung der Wahrscheinlichkeit, dass die Risiken eintreten, und die Auswirkungen, wenn sie eintreten, bewertet werden; |
| Sicherheitsrisiko | Ein Sicherheitsrisiko ist die Wahrscheinlichkeit, dass etwas Schlimmes passiert, das einem Informationswert Schaden zufügt; |
| Bewertung des Sicherheitsrisikos | eine Bestimmung des quantitativen oder qualitativen Risikowertes in Bezug auf eine konkrete Situation und eine anerkannte Bedrohung für die Sicherheit der Kundendaten und/oder der Systeme; |
| Bewertung der Anfälligkeit | eine Sicherheitsrisikobewertung, die zur Identifizierung, Quantifizierung und Priorisierung (oder Rangfolge) der Schwachstellen in einem Computersystem, einschließlich der zugehörigen Netzwerke, Datenbanken und Softwareanwendungen, führt; |
| Verbundene Unternehmen | jedes Unternehmen, das als verbundenes Unternehmen des Kunden im Sinne der §§ 15 ff AktG anzusehen ist. Darüber hinaus kann der Kunde in einer Änderungsvereinbarung weitere Unternehmen als Verbundene Unternehmen des Kunden definieren; |
| Kundengruppe | bezeichnet den Kunden zusammen mit den mit ihm verbundenen Unternehmen; |

## Teil A - Bedingungen für Lieferungen und Leistungen im Rahmen von IT/OT & E/E Systemen beim Lieferanten

### 1. Einhaltung und grundlegende technische Anforderungen

Der Auftragnehmer erbringt die Leistung unter Beachtung der Grundsätze ordnungsgemäßer Datenverarbeitung. Dazu gehören insbesondere die Einhaltung der gesetzlichen Datenschutzbestimmungen und die Umsetzung aller anerkannten, dem Stand der Technik entsprechenden Vorkehrungen und Maßnahmen.

Der Auftragnehmer hat geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein hohes Maß an IT-Sicherheit in Bezug auf die Leistungen und die vom Auftragnehmer für die Erbringung dieser Leistungen benötigten IT-Systeme zu gewährleisten. Soweit sie auf die Leistungen und die vom Auftragnehmer zur Leistungserbringung eingesetzten IT-Systeme anwendbar sind, wird der Auftragnehmer die Einhaltung der Mindeststandards der ISO/IEC 27001:2013 (oder einer ggf. später erschienenen Nachfolgeversion dieser Standards) oder der jeweils gültigen Versionen anderer ähnlicher, aber höherer Sicherheitsstandards, wie z.B. des BSI (Bundesamt für Sicherheit in der Informationstechnik) IT-Grundschutz, sicherstellen. Der Auftragnehmer wird diese Maßnahmen mit den entsprechenden Konzepten, Zertifikaten und Auditberichten auf Verlangen des Auftraggebers im Einzelnen offenlegen.

### 2. Schulung und Sensibilisierung im Zusammenhang mit der Informationssicherheit

Der Auftragnehmer informiert seine Mitarbeiter und die mit der Erbringung der Dienstleistungen betrauten Dritten regelmäßig über relevante Themen der Informationssicherheit, einschließlich der Pflichten, die ihnen im Zusammenhang mit der Erbringung der Dienstleistungen zur Gewährleistung der Informationssicherheit obliegen.

### 3. Schutz der Daten des Kunden vor Missbrauch und Verlust

Der Auftragnehmer verpflichtet sich, alle von ihm erhaltenen oder erzeugten Informationen und Daten des Auftraggebers unverzüglich, wirksam und dem Stand der Technik entsprechend gegen unbefugten Zugriff, Veränderung, Vernichtung oder Verlust, unerlaubte Weitergabe, sonstige unerlaubte Verarbeitung und sonstigen Missbrauch zu sichern. Bei der Sicherung der Daten des Auftraggebers hat der Auftragnehmer alle dem Stand der Technik ent-

sprechenden Vorkehrungen und Maßnahmen zu treffen, damit die Daten jederzeit verlustfrei archiviert und wiederhergestellt werden können. Ändert sich während der fortlaufenden Erbringung der Dienstleistungen der Stand der Technik hinsichtlich der Sicherheitsmaßnahmen, so verpflichtet sich der Lieferant, alle Maßnahmen zu ergreifen, um alle Informationen und Daten der Kundengruppe nach dem neuen Stand der Technik zu sichern.

**4. Eigentum an den Daten des Kunden**

Der Kunde und seine verbundenen Unternehmen besitzen und behalten alle Rechte, Titel und Interessen an ihren Daten, und der Lieferant ist ausschließlich im Namen des Kunden und/oder seiner verbundenen Unternehmen im Besitz dieser Daten.

**5. Schutz bei der Übermittlung von Informationen**

Alle Daten, die im Rahmen der Lieferungen und Leistungen physisch oder elektronisch übermittelt werden, müssen mit Mitteln (z. B. Einschreiben, Kurierdienst, E-Mail-Verschlüsselung) übermittelt werden, die dem Grad der Sensibilität dieser Daten angemessen sind.

**6. Schutz vor Malware**

Der Auftragnehmer wird alle Leistungen und Datenträger bzw. elektronisch (z.B. per E-Mail oder Datentransfer) übermittelte Leistungen vor deren Erbringung bzw. Nutzung nach dem Stand der Technik durch Test- und Analyseverfahren auf Schadprogramme (z.B. Trojaner, Viren, Spyware) untersuchen. Datenträger, auf denen Schadsoftware festgestellt wird, dürfen nicht genutzt werden. Der Anbieter wird den Kunden unverzüglich informieren, wenn er feststellt, dass der Kunde durch Schadsoftware kompromittiert ist. Die gleichen Verpflichtungen gelten für alle Formen der elektronischen Kommunikation.

**7. Transparenz bei Dienstleistungen und Verfahren**

Die Dienste dürfen keine undokumentierten Mechanismen oder Funktionen enthalten, die ihre Sicherheit beeinträchtigen könnten. Die automatische Übermittlung von Daten an den Anbieter oder an Dritte darf nur mit ausdrücklicher schriftlicher Zustimmung des Kunden erfolgen.

**8. Mitteilung im Falle von Mängeln oder Fehlern bei den erbrachten Dienstleistungen**

Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er Mängel oder Fehler in den für den Auftraggeber erbrachten Leistungen feststellt, die den Betrieb oder die Sicherheit des Auftraggebers beeinträchtigen können.

**9. Handhabung der dem Lieferanten zur Verfügung gestellten Hardware, Software, Zugangsmittel und Zugangsdaten**

Alle Hardware, Software, Zugangsmittel und Zugangsdaten, die der Auftraggeber dem Auftragnehmer zur Verfügung stellt, werden in Übereinstimmung mit den Nutzungsbedingungen des Auftraggebers verwendet. Der Lieferant wird alle ihm zur Verfügung gestellten Zugangsdaten und Zugangsmittel geheim halten und nach dem Stand der Technik vor dem unberechtigten Zugriff und der Nutzung durch Dritte schützen. Werden Hardware, Software, Zugangsmittel und Zugangsdaten, die dem Auftragnehmer zur Erbringung der Leistungen überlassen wurden, nicht mehr benötigt, sind sie unverzüglich an den Auftraggeber zurückzugeben. Ist die Rückgabe der überlassenen Software, Zugangsmittel und Zugangsdaten nicht möglich, so wird der Auftragnehmer die ihm überlassene Software, Zugangsdaten und Zugangsmittel löschen oder deinstallieren, jedoch nicht ohne vorher den Auftraggeber zu kontaktieren und um Zustimmung zur Löschung/Deinstallation zu bitten. Danach wird der Lieferant dem Auftraggeber die Löschung/Deinstallation schriftlich bestätigen. Der Lieferant darf seine eigene Hard- und Software nur dann mit oder auf den Systemen und Netzen des Auftraggebers im Zusammenhang mit der Erbringung einer Dienstleistung verwenden, wenn der Auftraggeber dies zuvor gestattet hat.

## Teil B - Bedingungen für die Bereitstellung von entwickelter Software/Hardware und/oder OT- & E/E-Systemlösungen einschließlich Dokumentation

**1. Grundsätzliche Verpflichtung des Lieferanten**

Hauptverpflichtung des Auftragnehmers ist es, im Rahmen des Dienstleistungsvertrages betriebsbereite Software entsprechend den in der überlassenen Softwarespezifikation festgelegten Spezifikationen und Funktionen, die zugehörige Dokumentation (wie z.B. das Benutzerhandbuch) und, sofern keine andere vertragliche Vereinbarung getroffen wurde, den Quellcode, jeweils entsprechend dem aktuellen Programm- und Updatestand, zu überlassen (nachfolgend "**Vertragsleistung**" genannt).

Der Lieferant wird die Betriebsbereitschaft der Software aufrechterhalten und sicherstellen, wenn dies gemäß einem separat oder im Rahmen des Vertrags über Software-Support und/oder Software-Pflege zu vereinbarenden Service Level Agreement vereinbart wird.

Der Auftragnehmer hat den Vertrag persönlich zu erfüllen. Eine Leistungserbringung durch einen Dritten ist ausgeschlossen, es sei denn, der Auftraggeber stimmt der Einschaltung eines Dritten im Rahmen einer vorherigen schriftlichen Mitteilung zu.

Nach Fertigstellung der vertraglichen Leistung teilt der Auftragnehmer dies dem Auftraggeber schriftlich oder in Textform mit und vereinbart einen Termin für die Präsentation der Arbeitsergebnisse. Der Auftragnehmer wird dem Auftraggeber Gelegenheit geben, vor der Abnahme der vertraglichen Leistung Funktionstests durchzuführen. Über die Einzelheiten dieser Tests werden sich die Parteien einvernehmlich verständigen.

Alle Abnahmen müssen nach einem förmlichen Verfahren erfolgen. Über die Abnahme ist ein von beiden Parteien zu unterzeichnendes Protokoll zu er- stellen. Ist die vertragliche Leistung nicht abnahmefähig, verpflichtet sich der Auftragnehmer, die Mängel unverzüglich zu beseitigen und die Leistung dem Auftraggeber erneut zur Abnahme vorzulegen.

**2. Nutzungsrechte**

2.1 Eigentum und ausschließliche Nutzungsrechte des Kunden

Eigentum an allen Ergebnissen und Zwischenergebnissen der vom Auftragnehmer im Rahmen des Vertrages erbrachten Leistungen bei der Entwicklung von Software/Hardware und/oder OT & E/E Systemen, z.B. Leistungsbeschreibungen, Spezifikationen, Studien, Konzepte, Dokumentationen einschließlich Installations-, Bedienungs- und Betriebsanleitungen sowie Dokumentationen zur Wartung, der Quellcode und Weiterentwicklungen, Berichte, Beratungsunterlagen, Grafiken, Diagramme, Bilder und Individualsoftware, Programme, angepasste Software (Customizing) und Parametrisierung sowie alle dabei entstehenden Zwischenergebnisse, Hilfsmittel und/oder sonstigen Leistungsergebnisse (zusammen: "**Arbeitsergebnisse**") gehen mit der Übergabe dieser Gegenstände auf den Auftraggeber über, soweit es sich um körperliche Gegenstände handelt.

Im Übrigen räumt der Lieferant dem Auftraggeber an den Arbeitsergebnissen mit deren Entstehung, spätestens jedoch mit deren Übergabe, ausschließliche, dauerhafte, unwiderrufliche, unterlizenzierbare und übertragbare Rechte ein. Der Betrieb der Software darf für den Auftraggeber und seine Verbundenen Unternehmen durch eines dieser Unternehmen durchgeführt werden.

Der Kunde darf die Software - neben der eigenen Nutzung - seinen Verbundenen Unternehmen zur eigenen Nutzung nach Maßgabe der getroffenen Vereinbarungen überlassen und für diese Unternehmen nutzen. Dieses Nutzungsrecht ist zeitlich begrenzt; es endet sechs Kalendermonate nach dem Zeitpunkt, zu dem der Kunde und das nutzende Unternehmen nicht mehr miteinander verbunden sind.

Der Auftraggeber kann den Betrieb der Software durch ein Drittunternehmen durchführen lassen (z.B. als Outsourcing oder Hosting). Der Auftraggeber wird den Auftragnehmer hierüber vorab schriftlich informieren und dem Auftragnehmer auf dessen Verlangen die Erklärung des Dritten vorlegen, dass die Software geheim gehalten und ausschließlich für die Zwecke des Auftraggebers und der mit ihm verbundenen Unternehmen verwendet wird.

Außerhalb der Gewährleistungsrechte darf der Kunde die Software an Dritte zum Zwecke der Fehlerbeseitigung überlassen. Er darf die Software ein- schließlich der schriftlichen Unterlagen Dritten zur Schulung der Mitarbeiter des Kunden und der mit ihm verbundenen Unternehmen überlassen.

Diese Rechte sind räumlich, zeitlich und inhaltlich unbeschränkt und haben keine Einschränkung in der Nutzung und Verwertung.

Diese Nutzungsrechte umfassen alle Arten der Nutzung, insbesondere das Speichern, Laden, Ausführen und Verarbeiten von Daten, die Bearbeitung in jeglicher Form, einschließlich der Fehlerkorrektur, auch durch Dritte, auch in dauerhafter Verbindung mit den Leistungen des Anbieters, das Recht der Vervielfältigung und Verbreitung, das Recht der Aufführung und Vorführung, auch in der Öffentlichkeit, das Recht der Vermarktung, Veränderung, Umwandlung, Übersetzung, Ergänzung und Weiterentwicklung. Das Nutzungs- recht umfasst auch künftige neuartige Nutzungsformen. Hinsichtlich neuartiger Nutzungsformen stellt der Lieferant den Besteller von etwaigen Ansprüchen der Urheber gemäß §§ 31a Abs. 2, 32a UrhG frei.

Der Kunde darf Sicherungskopien im Rahmen einer dem jeweiligen Stand der Technik entsprechenden Nutzung erstellen.

Der Kunde kann das Benutzerhandbuch und andere Informationen ausdrucken und kopieren und sie auch den verbundenen Unternehmen zur Verfügung stellen.

Der Besteller ist berechtigt, sowohl unentgeltliche als auch entgeltliche Unterlizenzen und weitere Nutzungsrechte an diesen Nutzungsrechten einzuräumen und Nutzungsrechte an Dritte zu übertragen, ohne dass es einer weiteren Zustimmung des Lieferanten bedarf.

Der Auftragnehmer stellt sicher, dass die Personen, die er zur Erfüllung des

Auftrags heranzieht, auf folgende Rechte verzichten: auf die Nennung als Urheber und auf den Zugang zu Originalkopien von Software oder anderen Arbeiten wie Dokumentationen, Zeichnungen und anderen Arbeitsergebnissen, die urheberrechtlich geschützt sein können.

2.2 Die nicht ausschließlichen Nutzungsrechte des Kunden

Der Auftragnehmer räumt dem Auftraggeber und seinen Verbundenen Unternehmen hiermit ein nicht ausschließliches, unwiderrufliches, dauerhaftes Recht ein, Werke, sonstiges urheberrechtlich geschütztes Material und sonstiges ungeschütztes technisches Wissen ("Know-how"), das der Auftragnehmer bereits vor Vertragsbeginn entwickelt oder genutzt hat, sowie Know-how, Standardsoftware und Entwicklungswerkzeuge (zusammen "**Geistiges Eigentum des Auftragnehmers**"), die der Auftragnehmer und seine Erfüllungsgehilfen im Rahmen der Leistungserbringung erworben haben, unabhängig von der vertraglichen Leistung zu nutzen. Diese Rechte sind nicht auf ein bestimmtes geographisches Gebiet beschränkt, sondern es handelt sich um übertragbare, unterlizenzierbare und mit der vereinbarten Vergütung abgegoltene Nutzungsrechte, soweit dies für die Nutzung der vom Auftragnehmer gelieferten Arbeitsergebnisse durch den Auftraggeber und seine Verbundenen Unternehmen erforderlich ist, ohne dass es einer weiteren Zustimmung des Auftragnehmers bedarf. Dies umfasst auch die Vervielfältigung, Bearbeitung und Veränderung des geistigen Eigentums des Lieferanten durch den Kunden und seine Verbundenen Unternehmen oder Dritte, soweit dies zur Nutzung der Arbeitsergebnisse erforderlich ist.

Dieses Nutzungsrecht der Verbundenen Unternehmen ist zeitlich begrenzt; es endet sechs Kalendermonate nach dem Zeitpunkt, an dem der Kunde und das nutzende Unternehmen nicht mehr miteinander verbunden sind.

2.3 Nutzungsrechte für Customizing-Dienste

Soweit der Lieferant eigene Software oder Software Dritter für den Auftraggeber angepasst hat, räumt er dem Auftraggeber und seinen Verbundenen Unternehmen hieran Nutzungsrechte gemäß Ziffer 2.1 ein.

2.4 Meldepflicht

Der Auftragnehmer wird dem Auftraggeber vor Vertragsende alle im Rahmen der Erstellung der Arbeitsergebnisse zu verwendende Fremdsoftware, Standardsoftware, Entwicklungswerkzeuge und sonstige Werke (wie z.B. alle für die Weiterentwicklung und Bearbeitung der Leistungsergebnisse des Auftragnehmers erforderlichen Dokumentationen), einschließlich der vom Auftragnehmer in Lizenz genutzten Materialien, schriftlich mitteilen. Diese, einschließlich der Rechte des Auftragnehmers, sind im Vertrag aufzuführen. Soweit vertraglich nichts anderes vereinbart ist, räumt der Auftragnehmer dem Auftraggeber die Nutzungsrechte an Fremdsoftware, Standardsoftware, Entwicklungswerkzeugen und sonstigen Werken gemäß Ziffer 2.2 ein.

2.5 Mitverfasser

Soweit Mitarbeiter oder Erfüllungsgehilfen des Auftragnehmers Miturheber sind, sichert der Auftragnehmer zu, dass er von ihnen das Recht zur Einräumung der in Ziffer 2.1 und 2.2 genannten Nutzungs- und Verwertungsrechte erworben hat.

2.6 Rechte an Erfindungen

Enthalten Arbeitsergebnisse erfinderische Leistungen, so verpflichtet sich der Auftragnehmer, wenn die Erfindung von einem Arbeitnehmer gemacht wurde, diese rechtzeitig in Anspruch zu nehmen und die Erfindung auf den Auftraggeber zu übertragen. Der Besteller ist in der Entscheidung frei, ob er Erfindungen auf seinen Namen oder den Namen eines von ihm benannten Dritten für weltweite Schutzrechte anmelden will. Der Lieferant verpflichtet sich, alle Erklärungen abzugeben und Unterschriften zur Erlangung, Aufrechterhaltung und Verteidigung von Erfindungen zu leisten. Eine besondere Vergütung ist hierfür nicht vorgesehen.

2.7 Einräumung von Rechten zur Nachbesserung und Nacherfüllung

Updates, Upgrades, Ergänzungen, neue Versionen und ähnliches sowie die jeweils aktualisierte Dokumentation (zusammen "Updates" genannt), die dem Kunden vom Lieferanten zur Verfügung gestellt werden, unterliegen ebenfalls den Bestimmungen dieses Vertrages.

2.8 Fortgesetzte Anwendung

Werden Nutzungsrechte auf Dauer erworben und ist die vereinbarte Vergütung bezahlt, so werden die eingeräumten Nutzungsrechte durch Rücktritt vom Vertrag, dessen Kündigung oder sonstige Beendigung nicht berührt.

**3. Defekte und Leistungsunterbrechungen**

Der Lieferant wird besondere Sorgfalt darauf verwenden, dass die Vertragsleistung frei von Rechten Dritter ist, die die Nutzung entsprechend dem vertraglich festgelegten Umfang einschränken oder ausschließen, und dass Ansprüche Dritter, dass die dem Kunden einzuräumenden Nutzungsrechte die Rechte dieser Dritten verletzen, abgewehrt werden können. Sie werden ihre eigenen Beschaffungsvorgänge mit größter Sorgfalt dokumentieren, durch Vertragsgestaltung mit ihren Mitarbeitern für einen sicheren Rechtsübergang sorgen, Unterlieferanten mit größtmöglicher Sorgfalt auswählen, jedem Verdacht eines Rechtsmangels unverzüglich und intensiv nachgehen. Macht ein Dritter derartige Ansprüche geltend, so wird der Lieferant nach Mitteilung des Bestellers, dass seine Nutzungsrechte von einem Dritten angegriffen werden, dem Besteller diese Informationen und sein Fachwissen zur Aufklärung des Sachverhalts und zur Abwehr der behaupteten Ansprüche uneingeschränkt zur Verfügung stellen. Der Lieferant wird nach Möglichkeit mit seinen Unterlieferanten Vereinbarungen treffen, die eine umfassende Erfüllung dieser Verpflichtungen ermöglichen und sicherstellen. Im Falle eines Rechtsstreits mit dem Dritten hat der Lieferant den Nachweis in der für die jeweilige Verfahrensart richtigen Form (z.B. als eidesstattliche Versicherung oder als Originalurkunde) zu erbringen.

Der Auftragnehmer hat auch besonders darauf zu achten, dass die vertragliche Leistung den besonderen Anforderungen des Auftraggebers, den vor- gegebenen oder vereinbarten technischen oder sonstigen Spezifikationen entspricht und für die vorgesehene Nutzung geeignet ist, die mit den vereinbarten Leistungsanforderungen übereinstimmt.

Eine Abweichung der vertraglichen Leistung von der vereinbarten Beschaffenheit gilt stets als Sachmangel. Das Gleiche gilt, wenn sich die vertragliche Leistung nicht für die vertraglich vorgesehene Verwendung eignet.

Die Dokumentation ist mangelhaft, wenn ein sachkundiger Anwender mit dem für die Nutzung der Software üblichen Kenntnisstand nicht in der Lage ist, mit zumutbarem Aufwand mit Hilfe der Dokumentation einzelne Funktionen zu bedienen oder auftretende Probleme zu beheben.

Der Auftragnehmer erkennt an, dass das reibungslose Zusammenwirken der vertraglichen Leistungen mit den laufenden, zumindest aber den für den Vertragszweck vorgesehenen Programmen für den Auftraggeber von größter Bedeutung ist, um das Funktionieren des Geschäftsbetriebes des Auftraggebers zu gewährleisten, und dass der Auftraggeber den Auftragnehmer mit der Erbringung der vertraglichen Leistungen beauftragt hat und daher alles dafür tut, dass die vertraglichen Leistungen unter Verwendung der vertraglichen Leistung auf der Grundlage industrieller Standards störungsfrei betrieben werden können. Der Auftragnehmer erkennt darüber hinaus an, dass die Übereinstimmung der Vertragsleistung mit den zum Zeitpunkt der Abnahme geltenden gesetzlichen Bestimmungen für den Auftraggeber von größter Bedeutung ist und wird darauf besonders achten.

Die Verjährungsfrist für Sachmängel beträgt zwei Jahre ab Abnahme der vertraglichen Leistung. Die Verjährungsfrist für Rechtsmängel beträgt zwei Jahre und beginnt mit dem Schluss des Kalenderjahres, in dem der Anspruch entstanden ist und der Kunde von dem Rechtsmangel (insbesondere der Verletzung eines Schutzrechts) Kenntnis erlangt hat oder hätte erlangen müssen, es sei denn, es liegt grobe Fahrlässigkeit vor. Eine Mängelanzeige des Bestellers hemmt die Verjährung. Bis zum Eintritt der Verjährung auftretende Mängel hat der Besteller dem Lieferanten unverzüglich mitzuteilen. Der Besteller ist bei Bedarf und nach Rücksprache bei der Analyse und Beseitigung des Mangels in erforderlichem Umfang zu beteiligen.

3.1 Ergänzende Leistungen

Der Auftragnehmer wird Mängel unverzüglich und innerhalb einer angemessenen Frist während der Gewährleistungsfrist unter Berücksichtigung der Interessen des Auftraggebers beseitigen und entweder eine verbesserte Version der vertraglichen Leistung liefern oder die vertragliche Leistung neu erbringen. Führt die vertragsgemäße Nutzung zu einer Beeinträchtigung von Rechten Dritter, wird der Auftragnehmer entweder die Vertragsleistung so ändern, dass sie die Schutzrechte nicht verletzt, oder die Genehmigung erwirken, dass die Vertragsleistung uneingeschränkt und ohne zusätzliche Kosten für den Auftraggeber vertragsgemäß genutzt werden kann. Die Bereitstellung einer Ersatzlösung oder eines Workarounds kann als kurzfristige Maßnahme zur Überbrückung oder zur Umgehung der Auswirkungen eines

Mangels eingesetzt werden. Der Mangel gilt erst dann als behoben, wenn er innerhalb eines angemessenen Zeitraums vollständig behoben wurde.

Schlägt die Nachbesserung durch den Lieferer fehl und entsteht dem Besteller durch das Unterlassen der Nachbesserung ein im Verhältnis zum Nachteil des Lieferers unangemessen hoher Nachteil, so ist der Besteller berechtigt, auf Kosten des Lieferers den Mangel selbst zu beseitigen, beseitigen zu lassen oder Ersatz zu beschaffen. Die vom Lieferanten zu ersetzenden Kosten dürfen nicht unverhältnismäßig sein und sind auf den Betrag begrenzt, der dem Lieferanten entstanden wäre, wenn er den Mangel innerhalb der ihm zustehenden Nachbesserungsfrist selbst beseitigt hätte. Weitergehende gesetzliche oder vertragliche Ansprüche bleiben vorbehalten.

3.2 Ermäßigung des Preises, Rücknahme

Verweigert der Lieferant die Nachbesserung oder schlägt sie fehl oder verstreicht die ihm gesetzte Nachfrist fruchtlos, so kann der Besteller nach seiner Wahl die Vergütung mindern oder vom Vertrag ganz oder teilweise zurücktreten, wenn er den Mangel nicht selbst vorbehaltlich Ziffer 3.1 beseitigt hat.

3.3 Zurückhaltung von Zahlungen und Aufrechnung von Zahlungen

Kommt der Auftragnehmer seinen Verpflichtungen nicht nach, kann der Auftraggeber die Zahlung für die vertraglichen Leistungen zurückhalten, bis der Auftragnehmer seine Verpflichtungen vollständig erfüllt hat. Der Auftraggeber kann seine Forderungen gegen den Auftragnehmer von der dem Auftragnehmer wegen der Nichterfüllung seiner Verpflichtungen zustehenden Vergütung abziehen.

3.4 Erstattung von Kosten, Entschädigung

Weitergehende Ansprüche, auch in Bezug auf Schadensersatz und Aufwendungsersatz, bleiben unberührt.

**4. Open-Source-Software**

Open-Source-Software ("OSS") ist Software, die im Allgemeinen kostenlos und quelloffen zur Verfügung gestellt wird und unter einer Lizenz verwendet werden kann, die die Weiterverbreitung der Software nicht einschränkt, Änderungen und abgeleitete Werke zulässt und deren Weiterverbreitung unter denselben Bedingungen wie die Lizenz der ursprünglichen Software erlauben muss ("OSS-Lizenz"). Zu den OSS-Lizenzen gehören unter anderem die "Berkeley Software Distribution License" (BSD), die "GNU General Public License" (GPL) und die "GNU Lesser General Public License" (LGPL). Copyleft-Lizenzen sind Lizenzen, die vorschreiben, dass alle abgeleiteten oder auf dem Programm basierenden Arbeiten nur unter den ursprünglichen Lizenzbedingungen verbreitet oder weitergegeben werden dürfen ("Copyleft-Lizenz").

4.1 Anforderungen

OSS darf nur mit vorheriger schriftlicher Zustimmung des Auftraggebers in die vom Lieferanten gelieferte Software aufgenommen werden. Der Lieferant wird dem Auftraggeber alle Informationen und Materialien zur Verfügung stellen, die notwendig sind, um über die Verwendung von OSS in der Software zu entscheiden. Dies schließt ein:

(i) eine transparente und vollständige Liste aller unter einer OSS-Lizenz lizenzierten Komponenten,
(ii) den Lizenztext jeder OSS-Lizenz,
(iii) Urheberrechtshinweise,
(iv) die Ergebnisse einer dem Stand der Technik entsprechenden Sicherheits- und Schwachstellenprüfung des gesamten verwendeten Open-Source-Codes und
(v) eine klare Beschreibung und Dokumentation der technischen Integration der OSS-Komponenten.

Der Kunde wird die Genehmigung nach eigenem Ermessen erteilen. Eine erteilte Genehmigung ist zu widerrufen, wenn die bereitgestellten Informationen oder Materialien falsch oder unvollständig sind.

OSS-Lizenztexte und der dazugehörige Quellcode müssen separat zur Verfügung gestellt werden. Der Lieferant wird den gesamten Open-Source-Code zur Verfügung stellen, soweit dies von den geltenden Lizenzen verlangt wird.

Der Lieferant wird den Auftraggeber in die Lage versetzen, alle Anforderungen aus den geltenden OSS-Lizenzen jederzeit vollständig zu erfüllen.

Diese Anforderungen gelten auch für alle Updates, Patches, Upgrades oder neuen Versionen der Software.

4.2 Verantwortung

Der Lieferant ist sich seiner besonderen Verantwortung bewusst, den Auftraggeber vor Schäden zu schützen, die durch die Integration von OSS-Software in die vom Lieferanten gelieferte Software und die Nutzung dieser Software durch den Auftraggeber entstehen. In Anbetracht dessen wird der Lieferant besonders darauf achten, dass er:

(i) zu jeder Zeit die Lizenzanforderungen der anwendbaren OSS-Lizenzen erfüllt und dass der Kunde alle erforderlichen Lizenzen von den Autoren der in der Software enthaltenen OSS erhalten hat,
(ii) über ein Open-Source-Compliance-System verfügt, das den bewährten Verfahren der Branche entspricht,
(iii) nur OSS-Komponenten verwendet, die unter kompatiblen OSS-Lizenzen lizenziert sind,
(iv) keine Copyleft-Lizenz in die Software integriert hat,
(v) den gesamten in der Software verwendeten Open-Source-Code auf Sicherheitsrisiken überprüft hat.

4.3 Entschädigung

Der Lieferant wird den Kunden und die verbundenen Unternehmen, Mitarbeiter, Direktoren oder Vertreter des Kunden von allen Ansprüchen, Schäden, Ausgaben und Haftungen freistellen, die in direktem oder indirektem Zusammenhang mit der Verletzung einer der vorstehenden Verpflichtungen durch den Lieferanten entstehen, unabhängig von der Rechtsgrundlage.

**5. Lebenszyklus der Softwareentwicklung**

Bei Arbeiten, die eine Softwareentwicklung beinhalten, muss der Lieferant:

(i) ein Konzept für den Lebenszyklus der sicheren Softwareentwicklung nach bekannten Normen wie IEC 62443 4-1 anwenden. Eine Zertifizierung wird erwartet.
(ii) den Nachweis erbringen, dass die ermittelten Sicherheitsanforderungen und die entsprechenden Sicherheitskontrollen entworfen und in der Software implementiert sind.
(iii) sicherzustellen, dass geeignete Sicherheitstests, einschließlich, aber nicht beschränkt auf statische und dynamische Codeprüfungen und kontinuierliche Schwachstellenbewertung, in den Entwicklungs- und Integrationsabläufen durchgeführt und alle aufgedeckten Probleme vor der Freigabe der Software behoben werden; und
(iv) dem Auftraggeber und/oder seinen Beauftragten die Durchführung von Schwachstellenanalysen der entwickelten Software ermöglichen. Wenn der Auftraggeber eine Schwachstelle mit einer Risikobewertung von "hoch" oder "kritisch" feststellt, wird der Lieferant Maßnahmen ergreifen, um die Risiken vor der Freigabe der Software zu mindern.

**6. Schwachstellen-Management**

(i) Der Lieferant wird einen unabhängigen und vertrauenswürdigen Schwachstellenbewertungsdienst beauftragen und/oder mit einem vom Kunden benannten unabhängigen Dritten bei der Durchführung von Schwachstellenbewertungen zusammenarbeiten und diesen unterstützen.
(ii) Der Lieferant überprüft monatlich die Informationsquellen des Lieferanten für Bedrohungen und Schwachstellen auf die neuesten Schwachstellen, Bedrohungen und Abhilfemaßnahmen, die für die von ihm verwalteten Systeme relevant sind.
(iv) Der Lieferant führt sowohl auf Netzwerk- als auch auf Anwendungsebene Schwachstellenanalysen durch, um zu ermitteln, welche Kontrollen möglicherweise fehlen oder nicht wirksam sind, um ein Ziel vor potenziellen Bedrohungen zu schützen.
(v) Der Lieferant muss einen Plan zur Behebung von Schwachstellen erstellen, sobald eine Schwachstelle festgestellt wird oder um zu verhindern, dass eine Schwachstelle entsteht, und muss Prioritäten setzen sowie den Fortschritt des Plans verfolgen und überwachen. Alle Abhilfepläne sind für künftige Zwecke zu dokumentieren. Schwachstellen, die erhebliche Auswirkungen auf die Sicherheit haben, sind in Absprache mit dem Kunden so schnell wie möglich zu beheben. Bei geringeren und mittleren Risiken ist der Zeitplan für die Behebung unter Berücksichtigung der Kosten, des Zeitaufwands und der zur Risikominderung erforderlichen Anstrengungen festzulegen.
(vi) Der Lieferant muss alle Schwachstellen nach der Behebung erneut testen, um zu bestätigen, dass die Risiken auf ein akzeptables, vom Kunden festgelegtes Niveau reduziert wurden.
(vii) Der Lieferant stellt dem Abnehmer unverzüglich Folgendes zur Verfügung:

- die Berichte (im Originalformat) über die Ergebnisse und Empfehlungen der Gefährdungsbeurteilungen, die von den unabhängigen Anbietern von Gefährdungsbeurteilungen vorgelegt wurden; und
- die Pläne des Lieferanten zur Behebung der festgestellten Schwachstellen.

(viii) Der Lieferant benachrichtigt den Kunden unverzüglich, wenn er eine kritische oder hoch eingestufte Schwachstelle nicht behebt, und schlägt dem Kunden die erforderlichen Sicherheitskontrollen vor und vereinbart sie mit ihm.
(ix) Der Lieferant muss sicherstellen, dass alle Anwendungen, Middleware, Backend-Software, Systeme und Netze standardmäßig sicher erstellt und konfiguriert werden. Als Teil der Standard-Build-Implementierung werden für Technologiekomponenten Konfigurationseinstellungen verwendet, die den maßgeblichen Sicherheitsempfehlungen entsprechen, wie sie von Produkt-

lieferanten (z. B. Siemens, Microsoft) oder Branchengruppen (z. B. ISO, IEC, CIS, NIST, SANS, OWASP) bereitgestellt werden.
(x) Schwachstellenbewertungen, unabhängig von Art und Ziel, sowie alle Arbeiten und die Zeit, die für die Durchführung von Abhilfemaßnahmen erforderlich sind, gehen zu Lasten des Anbieters und werden dem Kunden nicht in Rechnung gestellt.

### 7. Sicherheits-Governance

(i) Der Lieferant wird eine Person (den "Sicherheitsbeauftragten des Lieferanten") ernennen, die folgende Aufgaben hat

- alle Aspekte der Sicherheit im Einklang mit dem Abkommen zu koordinieren und zu verwalten; und
- im Falle eines Sicherheitsvorfalls als einziger Ansprechpartner im Namen des Lieferanten und seiner Unterauftragnehmer zu fungieren.

(ii) Falls der Anbieter den Sicherheitsbeauftragten des Anbieters auswechseln möchte, wird er den Kunden schriftlich davon in Kenntnis setzen und ihm die Kontaktdaten der Ersatzperson mitteilen.
(iii) Wenn der Auftragnehmer Fragen in Bezug auf einen Aspekt der IT-Sicherheit oder die Umsetzung der Anforderungen in diesem Anhang hat, wird er sich mit dem Auftraggeber beraten.

### 8. Risikomanagement

(i) Auf angemessenes Verlangen des Auftraggebers wird der Auftragnehmer in den Fällen, in denen er mit dem IT-System des Auftraggebers in Berührung kommt, den Auftraggeber bei einer Sicherheitsrisikobewertung der Arbeiten unterstützen, die jederzeit während der üblichen Geschäftszeiten durchgeführt werden kann.
(ii) Für den Fall, dass bei einer Sicherheitsrisikobewertung Probleme festgestellt werden, die als hoch oder kritisch eingestuft werden, wird der Lieferant dem Kunden jede angemessene Unterstützung bei der Analyse der Risiken und der Identifizierung geeigneter Kontrollen gewähren, die vom Lieferanten zum Schutz der Daten oder des Dienstes des Kunden, die vom Lieferanten verwaltet werden oder in dessen Besitz sind, in Übereinstimmung mit den in diesem Dokument beschriebenen Anforderungen durchgeführt werden müssen.
(iii) Für den Fall, dass der Auftragnehmer beabsichtigt, seine Leistungen wesentlich zu ändern, oder der Auftraggeber eine wesentliche Änderung der Leistungen verlangt, wird der Auftragnehmer eine Sicherheitsrisikobewertung durchführen.
(iv) Der Lieferant stellt sicher, dass alle in einer Sicherheitsrisikobewertung ermittelten Risiken unverzüglich beseitigt, überwacht und bis zu ihrer Schließung verwaltet werden. Der Auftragnehmer hält den Auftraggeber über die Abhilfemaßnahmen für alle in der Sicherheitsrisikobewertung ermittelten Risiken auf dem Laufenden.

### 9. Personelle Sicherheit

(i) Der Lieferant stellt sicher, dass alle Lieferanten oder Mitarbeiter des Lieferanten, die Zugang zu den Kundendaten haben, in Übereinstimmung mit dieser Vereinbarung und/oder gemäß den Anweisungen des Kunden überprüft und kontrolliert wurden.
(ii) Der Lieferant und seine Unterauftragnehmer stellen sicher, dass das gesamte Personal des Lieferanten alle erforderlichen Schulungen erhält und sich seiner Verantwortung hinsichtlich der Sicherheitsbestimmungen dieser Vereinbarung bewusst ist.
(iii) Der Lieferant muss geeignete Kontrollen einführen und aufrechterhalten, um die Risiken von menschlichem Versagen, Diebstahl, Betrug oder Missbrauch von Einrichtungen durch das Personal des Lieferanten zu verringern.

### 10. Sicherheit im Rechenzentrum

(i) Der Auftragnehmer muss angemessene physische und umgebungsbezogene Sicherheitskontrollen einführen und aufrechterhalten, um unbefugten Zugang, Beschädigung und Beeinträchtigung von Datenzentren zu verhindern, die Kundendaten oder Informationen enthalten, die bei der Erbringung der Arbeiten verwendet werden.
(ii) Der Lieferant stellt sicher, dass alle Datenzentren nach ISO 27001 (oder einer anderen Norm, die ISO 27001 ersetzt oder ergänzt) zertifiziert sind.
(iii) Der Lieferant wird den Kunden mit angemessener Frist schriftlich über jede vom Lieferanten vorgeschlagene Änderung von Verfahren oder Richtlinien informieren, die für ein Datenzentrum gelten und von denen vernünftigerweise angenommen werden kann, dass sie das Risiko für die Sicherheit und Integrität von Kundendaten erhöhen.

### 11. Zugangskontrolle

(i) Der Auftragnehmer stellt sicher, dass geeignete Zugangskontrollmechanismen eingesetzt werden, um alle Benutzer (oder Einrichtungen) zu überprüfen und zu authentifizieren, unabhängig davon, ob es sich um den Auftragnehmer, einen Dritten oder den Auftraggeber handelt, bevor der Zugang zum Werk gewährt wird.
(ii) Alle Nutzer (oder Stellen), die Zugang zu dem Werk haben oder beantragen, werden im Rahmen eines festgelegten Zugangsverwaltungsprozesses bereitgestellt, verwaltet und autorisiert.
(iii) Der Anbieter verwendet eine Authentifizierungsmethode, die mindestens eine Kombination aus Benutzerkennung und Passwort unterstützt, wobei die Benutzerkennungen und Passwörter eindeutig sind, nicht neu zugewiesen werden und nicht von einer Gruppe von Benutzern gemeinsam genutzt werden. Bei administrativen Konten verlangt der Anbieter einen zusätzlichen Faktor für die Authentifizierung.
(iv) Der Anbieter verlangt von allen Nutzern, die von einer niedrigeren auf eine höhere Berechtigungs- oder Sensibilitätsstufe wechseln, sich erneut zu authentifizieren.
(v) Der Lieferant muss Passwörter und andere Zugangsdaten bei der Speicherung und Übermittlung durch geeignete Kontrollen schützen. Der Lieferant darf Passwörter nicht im Klartext übermitteln oder speichern und Passwörter bei der Anmeldung in den Systemen nicht sichtbar anzeigen.
(vi) Der Anbieter darf Benutzerkennungen und Passwörter nicht in Skripten oder Klartextdateien wie Shell-Skripten, Batch-Konfigurationsdateien und Verbindungsstrings fest codieren.

### 12. Netzwerksicherheit

(i) Der Lieferant verwaltet die Übertragung der Kundendaten in einer Netzwerkumgebung unter der direkten Kontrolle des Lieferanten (oder eines Unterauftragnehmers). Das Netzwerk muss verwaltet und vor externen Bedrohungen geschützt werden, einschließlich, aber nicht beschränkt auf Zugangskontrollen auf der physischen, Netzwerk- und Anwendungsebene, um nur denjenigen Zugang zu den Kundendaten zu gewähren, die vom Lieferanten rechtmäßig autorisiert wurden. Das Netz ist abzutrennen, um den Zugang von öffentlichen oder nicht vertrauenswürdigen Netzen zu verweigern, einschließlich der Netze von Dritten, mit denen der Lieferant keinen Vertrag mit Klauseln, die den Klauseln in diesen Geschäftsbedingungen entsprechen, und keine separate Datenverarbeitungsvereinbarung (DPA) geschlossen hat.
(ii) Der Auftragnehmer stellt sicher, dass die Systeme regelmäßig und rechtzeitig mit der neuesten und relevanten Sicherheitssoftware sowie mit vorab getesteten und genehmigten Sicherheitssoftware-Patches und Korrekturen von anderen vom Auftragnehmer bereitgestellten Systemen aktualisiert werden. Der Auftragnehmer führt monatlich Schwachstellenbewertungen durch, um den Status der Konfiguration und der Softwarepatches der Systeme zu beurteilen.
(iii) Der Lieferant stellt sicher, dass alle Netzwerkverbindungen des Kunden zum Netzwerk des Lieferanten, die als "VERTRAULICH" eingestufte Kundendaten über ein nicht vertrauenswürdiges Netzwerk, wie z.B. das Internet, transportieren, über eine verschlüsselte Netzwerkverbindung in Übereinstimmung mit den Sicherheitsrichtlinien des Kunden oder veröffentlichten Standards wie ISO oder NIST erfolgen.
(iv) Der Lieferant stellt sicher, dass prüfbare Ereignisse erzeugt werden, einschließlich, aber nicht beschränkt auf sicherheitsspezifische Ereignisse, alle erfolgreichen und fehlgeschlagenen Zugriffsversuche auf das Netz, und führt ein Protokoll über alle Änderungen an den Sicherheitskonfigurationen des Netzes.
(v) Der Auftragnehmer muss Verfahren und ein Sicherheitsinformations- und Ereignisverwaltungssystem (Security Information and Event Management, SIEM) einrichten, umsetzen und verwalten, um die Sicherheit des Netzes bei Verdacht auf Eindringen oder unbefugten Zugriff zu überwachen.
(vi) Der Auftragnehmer muß sicherstellen, daß das Verfahren und die Kontrollen, die zur Durchführung der Sicherheitsüberwachung eingesetzt werden, so implementiert werden, daß die Integrität, Vertraulichkeit und Verfügbarkeit der gesammelten sicherheitsüberwachungsbezogenen Ereignisse gewahrt bleibt.
(vii) Der Lieferant muss die Trennung von Entwicklungs- und Testumgebungen von den Produktionsumgebungen aufrechterhalten. Alle Live-Kundendaten, die personenbezogene Daten enthalten, müssen anonymisiert werden (d.h. in eine Form umgewandelt werden, die keine Identifizierung von Personen ermöglicht oder die es erlaubt, Daten zur Erleichterung der Identifizierung wiederherzustellen), bevor sie für Tests verwendet werden, und müssen die ausdrückliche schriftliche Genehmigung des Kunden haben.
(viii) Wenn das System oder Netz eines Lieferanten mit dem Netz des Kunden verbunden ist, muss das System oder Netz des Lieferanten den Sicherheitsrichtlinien des Kunden entsprechen.

### 13. Unterauftragnehmer und Dritte

(i) Bei der Beauftragung eines Unterauftragnehmers hat der Lieferant dafür zu sorgen, dass der Unterauftragnehmer den gleichen Bedingungen zustimmt, wie sie in diesem Dokument in Bezug auf die Sicherheit von IT/OT & E/E-Systemen zum direkten Nutzen des Auftraggebers enthalten sind, und gegebenenfalls einen separaten Datenverarbeitungsvertrag (DPA) abzu-

schließen, wobei er es grundsätzlich für erforderlich hält, wenn Auftraggeber und Lieferant einen Datenverarbeitungsvertrag (DPA) abgeschlossen haben.
(ii) Auf Verlangen des Auftraggebers prüft der Auftragnehmer die Einhaltung der von seinen Unterauftragnehmern gemäß diesen Geschäftsbedingungen zu erfüllenden Sicherheitspflichten und legt einen detaillierten schriftlichen Bericht darüber vor.
(iii) Beauftragt der Lieferant einen Dritten mit der Lieferung der Arbeiten an den Kunden, so wird der Lieferant:

a) alle Drittsysteme mit Hilfe von Technologien und Verfahren zu authentifizieren, um eine Nichtabstreitbarkeit zu erzwingen;
b) Kontrollen zum Schutz des Netzes des Lieferanten vor unbefugtem Zugriff zwischen:
    1) das Netz eines Dritten und das Netz des Lieferanten;
    2) das Netz Dritter und etwaige Internet-Zugangspunkte; und
    3) das Netz eines Dritten und andere Netze Dritter, die mit dem Netz des Lieferanten verbunden sind;
c) alle ein- und ausgehenden Verbindungen zu oder von Netzen Dritter auf bestimmte Hosts und Ports zu beschränken und die Arbeit auf diesen Hosts auf das zur Erfüllung der Bedürfnisse des Kunden erforderliche Minimum zu beschränken;
d) alle Änderungen des Arbeitsumfangs, einschließlich Änderungen der Firewall-Regeln, dem Kunden auf Wunsch mitteilen;
e) eine Liste aller Personen führen, die Zugang zum Netz des Lieferanten haben, und diese Liste monatlich überprüfen;
f) alle erfolgreichen und fehlgeschlagenen Zugriffe Dritter zu protokollieren und dem Kunden bei Bedarf zur Überprüfung zur Verfügung zu stellen;
g) den Kunden unverzüglich über Sicherheitsverletzungen, einschließlich des tatsächlichen oder vermuteten unbefugten Zugriffs auf ein System oder dessen Beeinträchtigung, zu informieren und die entsprechenden Abhilfemaßnahmen gemäß diesen Bedingungen zu ergreifen; und
h) Überprüfung aller Netzverbindungen Dritter auf jährlicher Basis oder bei Änderungen der Verbindungen und der Anforderungen an die Zugangskontrolle und Beendigung veralteter oder nicht erforderlicher Verbindungen Dritter.

(iv) Der Lieferant haftet für Pflichtverletzungen seiner Unterlieferanten in gleichem Maße wie für eigene Pflichtverletzungen.

## 14. Management von Sicherheitsvorfällen

(i) Der Lieferant hat jederzeit zu überwachen und zu überprüfen, ob der Zugang zu den Kundendaten autorisiert ist und ob es Sicherheitsvorfälle gibt.
(ii) Im Falle eines kritischen Sicherheitsvorfalls oder eines schwerwiegenden Sicherheitsvorfalls, wie vom Kunden festgelegt, muss der Lieferant:

a) den Kunden spätestens vier Stunden nach dem Sicherheitsvorfall zu benachrichtigen (und diese Benachrichtigung erforderlichenfalls zu eskalieren);
b) unverzüglich und in angemessener Weise auf einen solchen Vorfall zu reagieren, und zwar in Übereinstimmung mit den Sicherheitsdienstleistungsstufen und dem im Plan zur Reaktion auf Sicherheitsvorfälle dargelegten Verfahren; und
c) dem Kunden und/oder seinen Vertretern sofortige Unterstützung bei der Untersuchung zu gewähren und alle Unterlagen im Zusammenhang mit solchen Untersuchungen aufzubewahren.

(iii) Der Lieferant darf die Einzelheiten eines Sicherheitsvorfalls oder einer Schwachstelle nicht ohne schriftliche Genehmigung des Kunden an Dritte weitergeben.
(iv) Der Lieferant sammelt und sichert bei der Untersuchung eines Sicherheitsvorfalls Beweise unter Verwendung forensischer Verfahren, wobei er eine Beweiskette und, soweit erforderlich, die Einhaltung gesetzlicher Vorschriften gewährleistet.
(v) Der Lieferant stuft alle Berichte über Sicherheitsvorfälle als "VERTRAULICH" in Übereinstimmung mit der Kundendaten-Klassifizierungspolitik ein und stellt sicher, dass angemessene Kontrollen zum Schutz dieser Informationen durchgeführt werden.
(vi) Der Lieferant muss im Falle eines Sicherheitsvorfalls Berichte über Sicherheitsvorfälle vorlegen. Diese Berichte müssen unter anderem Folgendes enthalten:

a) die Quelle und das Ziel des Ereignisses sowie die Uhrzeit, das Datum und die Art des Ereignisses;
b) eine Gewichtung der Kritikalität (niedrige Priorität, schwerer oder kritischer Sicherheitsvorfall);
c) einen Bericht über die Ursachenanalyse für jeden Sicherheitsvorfall; und
d) eine individuelle Referenznummer, die nachverfolgt werden kann.

(vii) Nach einem Sicherheitsvorfall oder auf Verlangen des Auftraggebers leitet der Auftragnehmer Abhilfemaßnahmen ein, um künftige Sicherheitsvorfälle im Zusammenhang mit dem Arbeitsumfang zu minimieren und zu verhindern.
(viii) Der Lieferant muss Sicherungs- und Wiederherstellungsverfahren anwenden, um auf Sicherheitsvorfälle zu reagieren, die zum Verlust oder zur Beschädigung von Informationen führen.

## 15. Sicherheitsprüfungen

(i) Der Lieferant gewährt dem Auftraggeber und/oder vom Auftraggeber beauftragten externen Prüfern (während der regulären Arbeitszeiten des Lieferanten) Zugang zu den Räumlichkeiten und/oder Aufzeichnungen des Lieferanten für die Zwecke:

a) die Überprüfung der Integrität, Vertraulichkeit und Sicherheit der Kundendaten und/oder des Arbeitsumfangs;
b) sich zu vergewissern, dass der Lieferant diese Bedingungen einhält; oder
c) die Durchführung einer Schwachstellenanalyse für alle Systeme, die Kundendaten enthalten.

(ii) Der Auftraggeber ist berechtigt, einmal in jedem Kalenderjahr während der Laufzeit des Vertrages ein Audit gemäß Absatz (i) durchzuführen, wobei der Auftraggeber berechtigt ist, jederzeit ein Audit durchzuführen, wenn er den begründeten Verdacht hat, dass der Lieferant gegen diese Geschäftsbedingungen verstößt.
(iii) Im Falle einer Untersuchung mutmaßlicher betrügerischer oder krimineller Handlungen im Zusammenhang mit der Sicherheit von IT/OT- und E/E-Systemen und/oder der Erbringung der Arbeiten durch den Auftragnehmer oder einen seiner Unterauftragnehmer gewährt der Auftragnehmer dem Auftraggeber, etwaigen gesetzlichen oder behördlichen Prüfern des Auftraggebers und ihren jeweiligen Bevollmächtigten zum Zwecke der Durchführung einer Prüfung unverzüglich Zugang zu den Geschäftsräumen und Aufzeichnungen des Auftragnehmers, und der Auftragnehmer leistet jederzeit während der Vertragslaufzeit oder zu einem beliebigen späteren Zeitpunkt jede erforderliche Unterstützung bei der Durchführung einer solchen Untersuchung.
(iv) Jede Partei trägt ihre eigenen Kosten und Auslagen, die ihr bei der Ausübung ihrer Rechte oder der Erfüllung ihrer Pflichten entstehen.
(v) Der Lieferant stellt dem Kunden (und/oder seinen Beauftragten oder Vertretern) Folgendes zur Verfügung und sorgt dafür, dass seine Unterauftragnehmer dies tun:

a) alle vom Kunden angeforderten Informationen im Rahmen des zulässigen Umfangs einer Prüfung;
b) Zugang zu allen vom Auftragnehmer kontrollierten Standorten oder Datenzentren, in denen Geräte des Auftraggebers bei der Ausführung der Arbeiten verwendet werden, zum Zwecke eines Audits;
c) Zugang zu den Aufzeichnungen in den Informationssystemen des Lieferanten für die Zwecke eines Audits; und
d) Zugang zum Lieferanten und zum Personal des Lieferanten für die Zwecke eines Audits.