# Deutsch

**Cybersecurity- und Betreiberpflichten**

**Präambel**
Dieses Dokument gilt als Vertragsbestandteil für sämtliche unsere Angebote und Auftragsbestätigungen. Durch Erteilung eines Auftrags an uns gelten diese Verpflichtungen seitens des Kunden als vorbehaltslos zur Kenntnis genommen. Ein entsprechender Verweis ist in unseren Angeboten und Auftragsbestätigungen vorhanden.

**1. Verantwortlichkeit des Betreibers**
Der Betreiber ist für den sicheren Betrieb der von ihm eingesetzten Informations-, Kommunikations-, Automatisierungs-, Steuerungs-, Maschinen-, OT- und Produktionssysteme verantwortlich. Dies gilt insbesondere für den laufenden Betrieb, die Administration, die Überwachung sowie die Einhaltung gesetzlicher und normativer Anforderungen.

Die Verantwortung des Betreibers umfasst insbesondere die Umsetzung und Aufrechterhaltung angemessener technischer und organisatorischer Maßnahmen nach dem Stand der Technik sowie die Einhaltung der Anforderungen der Normenreihe IEC 62443, des Cyber Resilience Act (CRA), der NIS-2-Richtlinie, der Maschinenverordnung (EU) 2023/1230 sowie sonstiger einschlägiger nationaler und europäischer Cybersecurity-Vorschriften, soweit diese auf den Betreiber Anwendung finden.

**2. Sicherheitsmaßnahmen des Betreibers**
Der Betreiber verpflichtet sich insbesondere,
- regelmäßige Risiko- und Bedrohungsanalysen durchzuführen,
- ein aktuelles Inventar aller relevanten Systeme, Komponenten und Softwarestände zu führen,
- geeignete Zugriffs-, Authentifizierungs- und Berechtigungskonzepte umzusetzen,
- Netzwerke angemessen zu segmentieren und zu schützen,
- Sicherheitsupdates, Patches und Herstellerinformationen regelmäßig zu bewerten und umzusetzen,
- Datensicherungen zu erstellen und Wiederherstellungstests durchzuführen,
- Sicherheitsereignisse und Cyberangriffe zu erkennen, zu dokumentieren und angemessen zu behandeln,
- ein Notfall-, Wiederherstellungs- und Business-Continuity-Konzept vorzuhalten,
- Mitarbeiter sowie beauftragte Dritte regelmäßig zu Cybersecurity-Themen zu schulen,
- Änderungen an Systemen kontrolliert und nachvollziehbar durchzuführen,
- die Wirksamkeit der Sicherheitsmaßnahmen regelmäßig zu überprüfen und zu verbessern.

**3. Pflichten des Betreibers hinsichtlich des Cyber Resilience Act (CRA)**
Soweit Produkte, Software, Maschinen, Komponenten oder Systeme eingesetzt werden, die unter den Anwendungsbereich des Cyber Resilience Act (CRA) fallen, ist der Betreiber insbesondere verpflichtet,
- vom Hersteller bereitgestellte Sicherheitsinformationen, Warnhinweise und Handlungsempfehlungen zu beachten,
- bereitgestellte Sicherheitsupdates innerhalb angemessener Fristen zu prüfen und einzuspielen,
- bekannte Schwachstellen und Sicherheitsrisiken angemessen zu behandeln,

- die Produkte ausschließlich entsprechend ihrer vorgesehenen Verwendung und Sicherheitsvorgaben einzusetzen,
- Veränderungen an Produkten nur unter Berücksichtigung der Herstellervorgaben und möglicher Auswirkungen auf Sicherheit und Konformität vorzunehmen,
- Prozesse zur Behandlung von Sicherheitsvorfällen und Schwachstellen einzurichten,
- bei Sicherheitsvorfällen die gesetzlich vorgeschriebenen Melde-, Mitwirkungs- und Dokumentationspflichten einzuhalten.

**4. Mitwirkung bei Cybersecurity-Maßnahmen**
Der Betreiber stellt sicher, dass dem Auftragnehmer die zur Leistungserbringung erforderlichen Informationen, Zugänge, Dokumentationen und Ansprechpartner rechtzeitig zur Verfügung stehen. Verzögerungen oder Einschränkungen, die aus einer fehlenden Mitwirkung resultieren, gehen nicht zu Lasten des Auftragnehmers.

**5. Haftungsbeschränkung**
Der Auftragnehmer haftet nicht für Schäden, Sicherheitsvorfälle, Produktionsausfälle, Datenverluste oder sonstige Nachteile, die ganz oder teilweise darauf beruhen, dass der Betreiber

- die vorstehenden Pflichten nicht erfüllt,
- sicherheitsrelevante Empfehlungen des Auftragnehmers oder Herstellers nicht umsetzt,
- verfügbare Sicherheitsupdates nicht einspielt,
- erforderliche organisatorische Maßnahmen unterlässt,
- geltende gesetzliche Vorschriften oder anwendbare Normen nicht einhält.

Dies gilt insbesondere für Verstöße gegen Anforderungen der IEC 62443, des Cyber Resilience Act (CRA), der NIS-2-Regelungen oder vergleichbarer Vorschriften.

**6. Keine Übertragung gesetzlicher Betreiberpflichten**
Soweit nicht ausdrücklich schriftlich etwas anderes vereinbart wurde, führt die Lieferung von Produkten, Software, Maschinen, Dienstleistungen, Wartungsleistungen oder Supportleistungen durch den Auftragnehmer nicht zu einer Übertragung gesetzlicher, regulatorischer oder normativer Betreiberpflichten auf den Auftragnehmer.
Die Gesamtverantwortung für den rechtskonformen und sicheren Betrieb der Anlagen und Systeme verbleibt jederzeit beim Betreiber.

# English

**Cybersecurity and Operator Obligations**

**Preamble**

This document forms part of the contract for all of our offers and order confirmations. By placing an order with us, the customer acknowledges these obligations without reservation. Our offers and order confirmations contain a corresponding reference to this document.

**1. Operator Responsibility**
The operator is responsible for the secure operation of the information, communication, automation, control, machinery, OT, and production systems it uses. This applies in particular to ongoing operation, administration, monitoring, and compliance with statutory and normative requirements. The operator's responsibility includes, in particular, implementing and maintaining appropriate technical and organizational measures in line with the state of the art, and complying with the requirements of the IEC 62443 series, the Cyber Resilience Act (CRA), the NIS 2 Directive, Machinery Regulation (EU) 2023/1230, and other relevant national and European cybersecurity regulations, insofar as they apply to the operator.

**2. Operator Security Measures In particular, the operator undertakes to:**

- carry out regular risk and threat analyses,
- maintain a current inventory of all relevant systems, components, and software versions,
- implement suitable access, authentication, and authorization concepts,
- segment and protect networks appropriately,
- regularly assess and implement security updates, patches, and vendor information,
- create data backups and perform recovery tests,
- detect, document, and appropriately handle security incidents and cyberattacks,
- maintain an emergency, recovery, and business continuity plan,
- provide regular cybersecurity training to employees and commissioned third parties,
- carry out changes to systems in a controlled and traceable manner,
- regularly review and improve the effectiveness of security measures.
-

3. Operator Obligations under the Cyber Resilience Act (CRA)
Where products, software, machinery, components, or systems within the scope of the Cyber Resilience Act (CRA) are used, the operator is in particular obligated to:

- observe security information, warnings, and recommended actions provided by the manufacturer,
- review and install provided security updates within reasonable timeframes,
- address known vulnerabilities and security risks appropriately,
- use the products solely in accordance with their intended purpose and security specifications,
- make changes to products only with due regard to the manufacturer's specifications and possible effects on security and conformity,
- establish processes for handling security incidents and vulnerabilities,
- comply with statutory reporting, cooperation, and documentation obligations in the event of security incidents.

4. Cooperation in Cybersecurity Measures
The operator shall ensure that the information, access, documentation, and contact persons required by the contractor to perform the services are made available to the contractor in a timely manner. Delays or restrictions resulting from a lack of cooperation shall not be the contractor's responsibility.

**5. Limitation of Liability**
The contractor is not liable for damages, security incidents, production outages, data loss, or other disadvantages that are wholly or partly based on the operator:

- failing to fulfill the obligations above,
- failing to implement security-related recommendations from the contractor or manufacturer,
- failing to install available security updates,
- omitting required organizational measures,
- failing to comply with applicable statutory provisions or applicable standards.

This applies in particular to violations of requirements under IEC 62443, the Cyber Resilience Act (CRA), NIS 2 regulations, or comparable regulations.

**6. No Transfer of Statutory Operator Obligations**
Unless expressly agreed otherwise in writing, the delivery of products, software, machinery, services, maintenance, or support by the contractor does not transfer statutory, regulatory, or normative operator obligations to the contractor. Overall responsibility for the lawful and secure operation of the plants and systems remains at all times with the operator.