# KOEPFER Anforderung an Lieferanten zur Sicherstellung der Informationssicherheit

Stand Januar 2024, FO.193

## Präambel

Als weltweit aufgestellter, unabhängiger Zulieferer ist die KOEPFER Group ein starker und verlässlicher Partner der Automobilindustrie. Als einer der führenden Hersteller von hochgenauen Zahnrädern für Motoren- und Getriebeanwendungen verbinden wir technologische Leistungsstärke mit Engagement, Kreativität und Motivation. Um unserem hohen Anspruch an Qualität gerecht zu werden, beschäftigen wir herausragende Spezialisten auf dem Gebiet der Metallbearbeitung.

Zur Erfüllung der aktuellen und künftigen Anforderungen unserer Kunden und Gesetzgeber sowie der Absicherung des Unternehmens gegen Cyberkriminalität sind Aspekte der Informationssicherheit immer stärker zu berücksichtigen. Diese Anforderung an Lieferanten bildet den verbindlichen Rahmen zwischen KOEPFER und dem Lieferanten, und dient dazu, den Anforderungen an den Schutz von Informationen hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit gerecht zu werden. Dieses Dokument ist Bestandteil unserer Einkaufsbedingungen und die Bestätigung durch den Lieferanten die Voraussetzung für die Belieferung an unseren Unternehmensverbund.

Um sicherzustellen, dass Sie die aktuellen und gültigen Dokumente verwenden, besuchen Sie bitte unsere KOEPFER-Homepage:
https://www.koepfer.com/unternehmen/einkauf/

Neuausgaben bzw. Änderungen werden allen Lieferanten der KOEPFER Group kommuniziert. Die Richtlinie ist zweisprachig deutsch / englisch. Die deutsche Ausgabe ist verbindlich.

i.V. M. Schweizer

Marcel Schweizer (Jan 16, 2024 15:53 GMT+1)

Marcel Schweizer
Head of Purchasing

i.V.

Lars Kammerer (Jan 16, 2024 17:10 GMT+1)

Lars Kammerer
Head of IT

| KOEPFER Anforderung an Lieferanten zur Sicherstellung der Informationssicherheit | FO.193 |
|---|---|

## 1. Informationssicherheit in Lieferantenbeziehungen

KOEPFER arbeitet ausschließlich mit Lieferanten zusammen, welche sich eigenständig zur grundlegenden Wahrung der Vertraulichkeit von Informationen und Geschäftsgeheimnissen verpflichten. In Einzelfällen, wenn die übergebenen oder geteilten Informationen einem gesteigerten Sicherheitsbedürfnis unterliegen, können darüber hinaus besondere Maßnahmen von Lieferanten gefordert werden, um dem gesteigerten Sicherheitsbedürfnis Rechnung zu tragen. Dies wird zumeist im Rahmen von Geheimhaltungsvereinbarungen geschehen.

## 2. Anforderungen an Lieferanten

### 2.1 Managementsystem

Der Lieferant wird aufgefordert sein Managementsystem, um die Grundsätze der Informationssicherheit zu erweitern. Dabei soll der Standard des TISAX-Assessment / TISAX Labels als Grundlage dienen. In Einzelfällen kann auch auf Zertifikate wie ISO/IEC 27001 oder VDA ISA Katalog zur Voraussetzung für bestimmte Geschäftsbeziehungen werden. Sollte der Lieferant keiner dieser obenstehenden Anforderungen erfüllen, gibt der Lieferant ein Maßnahmenplan zur Einführung der oben genannten Zertifikate und Stellungnahme im unten aufgeführten Fragenkatalog ab.

### 2.2 Interne Organisation

Es sind Richtlinien, Prozesse und Verantwortlichkeiten zu definieren, mit denen die Informationssicherheit implementiert und kontrolliert werden kann.
Dies beinhaltet insbesondere:

- Die Erstellung einer Informationssicherheitsrichtlinie.
- Anwenderrichtlinien zur Festlegung von Regeln für den Umgang mit Anwendungen, Systemen und IT-Endgeräten und dem Verhalten bei der Nutzung von Informationstechnologie
- Die Beschreibung von Prozessen für die Verwaltung von Datenträgern, Dokumenten und Informationen.
- Die Festlegung der Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit.
- Die Verpflichtung der Mitarbeiter auf Geheimhaltung und Wahrung des Datengeheimnisses.
- Die regelmäßige Durchführung von Schulungen und Awareness-Maßnahmen

Die Mindestanforderungen und zentralen Inhalte dieser obenstehenden Regelungen werden in den folgenden Kapiteln beschrieben.

#### 2.2.1 Mobile Endgeräte

Der Einsatz von mobilen Endgeräten verlangt besonders sorgfältigen Umgang. Ein offener und unbeaufsichtigter Umgang, sowie Einblick für projektferner Personen muss verhindert werden. Mobile Endgeräte mit eingerichteten Firmen-Accounts (E-Mail, Kalender, etc.) dürfen nur vom Lieferanten selbst verwendet werden. Unbefugten Dritten ist die Benutzung verboten. Falls Daten von KOEPFER auf mobilen Systemen oder IT-Geräten gespeichert werden, sind diese mit dem aktuellen Stand der Technik entsprechender Hardware oder Software zu verschlüsseln. Die Entsorgung von mobilen Endgeräten, erfolgt durch die IT-Abteilung des Lieferanten. Eine eigenständige Entsorgung durch den jeweiligen Mitarbeiter ist verboten.

#### 2.2.2 Persönliche Logins- und Passwörter

Der Lieferant hat sicherzustellen, dass alle IT-Systeme ausreichend geschützt sind und entsprechende Regelungen in der Informationssicherheitsrichtlinie hierfür definiert werden.
Folgende Vorgaben müssen diese mindestens beinhalten:

- Die Weitergabe von Anmeldeinformationen ist nicht gestattet
- Anmeldeinformationen sind nur dem jeweiligen Benutzer bekannt (Initialpasswörter werden beim ersten Login geändert)
- Passwörter werden nicht unverschlüsselt notiert.
- Sollte der Verdacht auf Kompromittierung bestehen, muss das Passwort unmittelbar geändert werden
- Passwortlänge: mindestens 8 Zeichen; Empfehlung bezüglich Passwortlänge: 10 Zeichen
- Passwörter beinhalten eine Kombination aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen (mindestens 3 von 4 Kriterien müssen erfüllt sein)
- Passwörter dürfen nicht leicht zu erraten sein (Geburtsdatum). Trivialpasswörter (wie z.B. 1111, 1234, Passwort, etc.) dürfen nicht verwendet werden.
- Passwörter müssen regelmäßig gewechselt werden. Bereits genutzte Passwörter dürfen nicht erneut verwendet werden.
- Smartphones und Tablets sind mit einem vierstelligen Code ausgestattet.

2.2.3 Schwachstellen- und Patchmanagement

Eine Ausnutzung technischer Schwachstellen sind durch den Einsatz von aktueller Virenschutzsoftware und die Implementierung eines geregelten Patchmanagements zu verhindern. Es sind regelmäßige Überprüfungen zur Erkennung von Schwachstellen der IT-Struktur bei Bedarf auch durch externe IT-Berater durchzuführen. Beim Herunterladen sowie Speichern von Programmen o.ä. ist darauf zu achten, dass diese aus einer vertrauenswürdigen Quelle stammen. Das Herunterladen von offensichtlich rechtswidrigen Angeboten oder Plattformen im Rahmen von Aufträgen von KOEPFER ist unzulässig. Sollte sich der Verdacht eines IT-Sicherheitsvorfalls (Virenbefall, Verschlüsselung, unbefugtes Eindringen von außen,…) erhärten, ist dieser innerhalb von 24 Stunden nach Kenntnisnahme an KOEPFER unter der security@koepfer.com zu melden.

**2.3 Physische und umgebungsbezogene Sicherheit**

Der Lieferant hat dafür Sorge zu tragen, dass der unbefugte Zutritt in Räume, Büros und Einrichtungen, in denen Informationen von KOEPFER verarbeitet werden, ausgeschlossen ist. Dies gilt weiterhin auch für Anlieferungs- und Ladebereiche, über die unbefugte Personen die Räumlichkeiten betreten könnten. Von Seiten des Lieferanten sind Richtlinien zu erstellen, die aufgeräumte Arbeitsumgebungen sowie Bildschirmsperren bei Nichtbenutzung regeln. Es gilt Grundsätzlich, dass der Zugang zu und Zugriff auf Informationen auf einen eindeutig bestimmten Personenkreis und auf den jeweilig zur Aufgabenerfüllung erforderlichen Umfang zu beschränken ist. Gespeicherte Informationen müssen vor unberechtigtem Zugriff, unberechtigter Veränderung und vor Verlust geschützt werden.

2.3.1 Umgang mit Betriebsmitteln und Datenträger

Um die Einsichtnahme durch Unbefugte zu verhindern, dürfen vertrauliche Dokumente niemals unbeaufsichtigt liegen gelassen werden. Ausgedruckte Dokumente mit personenbezogenen oder vertraulichen Daten müssen entsprechend sicher entsorgt werden z.B. mit einem Dokumentenschredder ab Sicherheitsstufe P4. Es werden ausschließlich unternehmenseigene Datenträger für den Austausch von Daten genutzt. Der Gebrauch von privaten USB-Sticks, Speicherkarten o. Ä. ist untersagt. Eine eigenständige Entsorgung durch den jeweiligen Mitarbeiter ist verboten. Die bereitgestellten Betriebsmittel dürfen nur für den entsprechenden Verwendungszweck eingesetzt werden.

2.3.2 Clean Desk

Beim Verlassen des Arbeitsplatzes ist dafür Sorge zu tragen, dass Unberechtigte keinen Einblick auf Informationen von der KOEPFER erlangen können. Es ist dafür Sorge zu tragen, dass Informationen auf Papier oder anderen Medien abgedeckt werden, wenn sich betriebsfremde Personen im Haus befinden. Auch nach Ende eines Meetings in einem Konferenzraum, sind alle Informationen aus Konferenzräumen sowie Inhalte auf Flipcharts, Whiteboards, etc. zu entfernen.

2.3.3 Arbeiten außerhalb der Organisation

Der Lieferant hat für seine Beschäftigten eine Richtlinie zu erstellen, welche das Arbeiten außerhalb der Organisation regelt. Der Fokus muss auf der Vertraulichkeit der Daten liegen und verhindern, dass Unbefugte Informationen abhören, erblicken, physisch stehlen oder elektronisch abgreifen können.

- Unterlagen von KOEPFER sollten in einem abschließbaren Schrank aufbewahrt werden.
- Personenbezogene, vertrauliche Papierdokumente sind gesichert zu entsorgen (z.B. Datenschutzcontainer oder Aktenvernichter). Alternativ ist eine papierlose Arbeitsweise zu empfehlen.
- Bei der Verwendung von Smartphone, Tablet und Laptop muss der Bildschirm bestmöglich vor Einsicht (z.B. durch die Verwendung einer Blickschutzfolie) geschützt werden (insbesondere, wenn Dritte nah sitzen, z.B. Flugzeug)
- Vertrauliche Gespräche, Telefonate und Videokonferenzen sollten nicht in öffentlichen Räumen, sondern nur an geschützten Plätzen geführt werden, wo kein Dritter zuhören kann.
- Hardware, Datenträger und geschäftliche Unterlagen dürfen nie unbeaufsichtigt gelassen werden und sollten immer persönlich mitgeführt oder sicher versperrt werden.
- Ein sicherer Zugriff auf das Firmennetzwerk außerhalb der Geschäftsräume ist, sofern möglich, über eine VPN-Verbindung (Virtual Private Network) herzustellen.

**2.4 Schutz von Informationswerten**

Der Lieferant ist aufgefordert seine Informationswerte zu erfassen, auf ihren Schutzbedarf zu bewerten und erforderliche Maßnahmen je nach Risikoklasse umzusetzen. KOEPFER verwendet eine Kennzeichnung seiner Informationswerte, Ein Leitfaden zur Klassifizierung von Informationen kann dem Lieferanten auf Anfrage ausgehändigt werden. Mit „vertraulich" gekennzeichnete Dokumente, als auch solche deren Inhalt in der üblichen Geschäftswelt von sensiblem Wert sind, dürfen nur ausgewählten Mitarbeitern zugänglich gemacht werden. Mit „intern" gekennzeichnete Dokumente sind für die Geschäftsbeziehung zwischen Lieferanten und KOEPFER bestimmt und im Unternehmen frei verteilbar.
Im Grundsatz gilt:

- Sowohl Daten als auch die Träger dieser Daten sind vor Verlust, Zerstörung, Manipulation und unberechtigten Zugriff zu schützen. Nicht mehr benötigte Datenträger sind nach sicheren Verfahren (z.B. Dokumentenschredder ab Sicherheitsstufe P4) zu vernichten.
- Der Datenaustausch darf nur über von KOEPFER freigegebenen Datenaustauschwegen durchgeführt werden. Die gewählten sicheren Datenaustauschwege müssen die Mindestanforderungen ISO27001 (wie z.B. SMIME) erfüllen.
- Der Lieferant hat sicherzustellen, dass keine unberechtigten Dritten vertrauliche Informationen mithören können oder Einsicht in diese erhalten. Beabsichtigt der Lieferant eine bewusste Weiterleitung ausgewählter Information an Dritte, so ist eine Freigabe von KOEPFER einzuholen. Dies gilt insbesondere für Informationen zu Projekten, die mit einer Geheimhaltungsvereinbarung verbunden sind. Beim Versand von E-Mails ist der Verteilerkreis auf das nötige Maß einzuschränken.

**2.5.Sicherheitsrelevante Vorfälle**

Es sind konsistente und wirksame Maßnahmen für das Management von Informationssicherheitsvorfällen (Diebstahl, Systemausfall, Datenverlust etc.) mit potenziell negativem Effekt zu implementieren.
Dies beinhaltet insbesondere:

- Die unverzügliche Meldung von Informationssicherheitsvorfällen an den Auftraggeber, insbesondere bei Bekanntwerden sogenannter Cyberangriffe.
- Die Protokollierung von Sicherheitsvorfällen.
- Die Implementierung von Prozessen zur Einleitung von Maßnahmen zur Verhinderung / Wiederholung von Informationssicherheitsvorfällen

Bei Bekanntwerden von Ereignissen, die zu einer Verletzung der Informationssicherheit oder des Datenschutzes führen können, ist der Lieferant innerhalb von 24 Stunden zur Meldung an security@koepfer.com verpflichtet.

**2.6 Datensicherungen**

Es sind Maßnahmen umzusetzen, die gewährleisten, dass schutzbedürftige Informationen und Daten / personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

2.6.2.Kryptographie

Der Einsatz von Verschlüsselungsverfahren für die Sicherstellung des ordnungsgemäßen und wirksamen Schutzes der Vertraulichkeit, Verfügbarkeit oder Integrität von personenbezogenen Daten bzw. schutzbedürftigen Informationen. Der Einsatz der kryptographischen Absicherung der Kommunikation ist insbesondere notwendig, wenn Daten mit hohem Schutzbedarf über öffentliche oder als nicht ausreichend sicher geltende Netzwerke übertragen werden.

2.6.2. Schutz personenbezogener Daten

Nach der EU-Datenschutz-Grundverordnung (EU-DSGVO) ist es untersagt, personenbezogene Daten zu einem anderen als dem zugewiesenen zur jeweiligen regelmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekannt zu geben, zugänglich zu machen oder sonst zu nutzen. Die EU-DSGVO schützt alle Daten natürlicher Personen, die aufgezeichnet oder verarbeitet werden. Hierzu zählen auch Aufzeichnungen auf mobilen, personenbezogenen Speicher- und Verarbeitungsmedien sowie Angaben auf Formularen. Diese Verpflichtung besteht auch nach Beendigung der Tätigkeit fort.

**2.7. Notfallmanagement**

Die Systemverfügbarkeit muss in schwierigen Situationen, wie Krisen- oder Schadensfällen, aufrechterhalten bzw. schnellstmöglich wiederhergestellt werden. Der Lieferant muss für die kritischen Informationswerte und IT-Systeme Notfallpläne erstellen, um die weitere Geschäftstätigkeit zu gewährleisten. Diese Notfallpläne müssen regelmäßig auf ihre Wirksamkeit getestet und ggf. optimiert werden.

## 3. Besonderheiten für Organisationen mit Zugang zum Netzwerk

### 3.1.Umgang mit Anmeldeinformationen und -medien

Anmeldedaten dürfen an unautorisierte Personen nicht weitergegeben werden. Bereits beim Verdacht der Kompromittierung sind die Zugangsdaten zu ändern und der Vorfall zu melden. Solange ein Zugriff auf das KOEPFER Netzwerk besteht, ist ein Verlassen des Arbeitsplatzes verboten.

### 3.2.Zugriffsrechte

Zugriffsrechte auf Systeme von KOEPFER müssen beantragt werden. Zugriff auf Daten von KOEPFER dürfen den Mitarbeitern nur nach dem Need-to-Know-Prinzip zugänglich gemacht werden.

### 3.3.Umgang mit Informationen

Alle Informationen sind unter der grundsätzlichen Annahme, dass diese streng vertraulich sind zu behandeln. Eine lokale Speicherung von Informationen und Daten ist verboten. Anpassungen und Updates an Software und IT-Systemen müssen bei den Ansprechpartnern von KOEPFER angemeldet und freigegeben werden.

## 4. Besonderheiten für Softwarelieferanten

Die gelieferte Software darf keine Funktionen erhalten, die die Schutzziele der Daten als auch der Software selbst gefährden insbesondere dem unerwünschten Ein- und auch Ausleiten von Daten und Funktionen oder der unerwünschten Veränderung von Daten bzw. der Ablauflogik. Der Lieferant hat nach Stand der Technik zu überprüfen, dass keine möglicherweise schadenstiftende Software (z.B. Viren, Würmer, Trojaner) mitgeliefert wird.

## 5. Verpflichtungserklärung

### 5.1 Verpflichtung von Mitarbeitern

Mitarbeitende des Lieferanten müssen von ihrer Geschäftsleitung auf die Geheimhaltung im Sinne der bestehenden Vertraulichkeitsvereinbarung zwischen KOEPFER und dem Lieferanten verpflichtet werden. KOEPFER ist jederzeit Einsicht in diese Vereinbarungen zu gewähren. Mitarbeitende des Lieferanten müssen von ihrer Geschäftsleitung auf die Einhaltung der gesetzlichen Datenschutzvorgaben verpflichtet werden. Ein Nachweis der Sicherstellung dieser Verpflichtung ist KOEPFER auf Verlangen vorzulegen.

### 5.2. Verpflichtung und Beauftragung von Dritten

Weitere Lieferant dürfen nur nach vorheriger Absprache und expliziter Freigabe durch KOEPFER beauftragt werden. Lieferant die Zugang/Zugriff zu vertraulichen Informationen haben, sind zur Einhaltung der Anforderungen an die Informations- und IT-Sicherheit gemäß VDA ISA in geeigneter Form in zusätzlichen Vereinbarungen (im Zweifel in gleicher Art und Weise) zu verpflichten. Dies gilt im besonderen Maße für deren projektbeteiligte Abteilungen und Angestellte.

## 6. Auditrecht

KOEPFER ist berechtigt, die Produktionsstätte und sonstige Geschäftsräume von Lieferanten und dessen Vorlieferanten, Unterauftragnehmer und sonstigen Erfüllungs- oder Verrichtungsgehilfen zusammen mit dem Endkunden nach vorheriger Ankündigung während der üblichen Geschäftszeiten zu betreten und die Einhaltung der Anforderungen an die Vertragsprodukte und zugrundeliegende Managementsysteme zu überprüfen. In dringenden Fällen, z.B. akute Reklamation, ist KOEPFER zum Zutritt an dem der Ankündigung nachfolgenden Tag berechtigt.

## 7. Änderungs-/Freiwilligkeitsvorbehalt

Die KOEPFER Zahnrad- und Getriebetechnik GmbH ist jederzeit berechtigt, diese oder einzelne Regelungen hieraus durch anderweitige Regelungen zu ersetzen oder zu ergänzen sowie vollständig aufzuheben. Die Änderungen werden erst durch die Prüfung und Zustimmung des Lieferanten wirksam.