KOEPFER requirements for suppliers to ensure information security

Version January 2024, FO.193

Preamble

As a global, independent supplier, the KOEPFER Group is a strong and reliable partner to the automotive industry. As one of the leading manufacturers of high-precision gears for engine and transmission applications, we combine technological performance with commitment, creativity and motivation. In order to meet our high standards of quality, we employ outstanding specialists in the field of metal processing.

In order to meet the current and future requirements of our customers and legislators as well as to protect the company against cybercrime, aspects of information security must be taken into account more and more. This requirement for suppliers forms the binding framework between KOEPFER and the supplier and serves to meet the requirements for the protection of information with regard to confidentiality, integrity and availability. This document is part of our purchasing conditions and confirmation from the supplier is a prerequisite for delivery to our group of companies.

To ensure that you use the current and valid documents, please visit our KOEPFER homepage:
https://www.koepfer.com/unternehmen/einkauf/

New editions or changes will be communicated to all KOEPFER Group suppliers. The guideline is bilingual German/English. The German edition is binding.

i.V. M. Schweizer

Marcel Schweizer (Jan 16, 2024 15:55 GMT+1)

Marcel Schweizer
Head of Purchasing

i.V. Kammerer

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

Lars Kammerer
Head of IT

1. Information security in supplier relationships

KOEPFER only works with suppliers who are independently committed to fundamentally maintaining the confidentiality of information and business secrets. In individual cases, if the information transferred or shared is subject to an increased need for security, special measures may also be required from suppliers to take the increased need for security into account. This will usually happen within the framework of confidentiality agreements.

2. Requirements for suppliers

2.1 Management system

The supplier is required to expand its management system to include information security principles. The standard of the TISAX assessment / TISAX label should serve as a basis. In individual cases, certificates such as ISO/IEC 27001 or VDA ISA catalog can also become a prerequisite for certain business relationships. If the supplier does not meet any of the above requirements, the supplier will submit an action plan for the introduction of the above-mentioned certificates and a statement in the questionnaire listed below.

2.2 Internal organization

Policies, processes and responsibilities must be defined with which information security can be implemented and controlled.
This includes in particular:

- The creation of an information security policy.
- User guidelines for defining rules for handling applications, systems and IT devices and behavior when using information technology
- The description of processes for managing data carriers, documents and information.
- Defining roles and responsibilities in the area of information security.
- The obligation of employees to maintain confidentiality and data secrecy.
- Regular implementation of training and awareness measures
- The minimum requirements and central content of these regulations above are described in the following chapters.

2.2.1 Mobile devices

The use of mobile devices requires particularly careful handling. Open and unsupervised handling, as well as insight for people distant from the project, must be prevented. Mobile devices with set up company accounts (email, calendar, etc.) may only be used by the supplier themselves. Use by unauthorized third parties is prohibited. If KOEPFER data is stored on mobile systems or IT devices, it must be encrypted using state-of-the-art hardware or software. The disposal of mobile devices is carried out by the supplier's IT department. Independent disposal by the respective employee is prohibited.

2.2.2 Personal logins and passwords

The supplier must ensure that all IT systems are adequately protected and that appropriate regulations are defined for this in the information security policy.
These must include at least the following requirements:

- Sharing login information is not permitted
- Login information is only known to the respective user (initial passwords are changed upon first login)
- Passwords are not recorded unencrypted.
- If there is suspicion of compromise, the password must be changed immediately
- Password length: at least 8 characters; Recommendation regarding password length: 10 characters
- Passwords contain a combination of upper and lower case letters, numbers and special characters (at least 3 out of 4 criteria must be met)
- Passwords must not be easy to guess (date of birth). Trivial passwords (such as 1111, 1234, password, etc.) may not be used.
- Passwords must be changed regularly. Passwords that have already been used may not be used again.
- Smartphones and tablets are equipped with a four-digit code.

2.2.3 Vulnerability and patch management

Exploitation of technical vulnerabilities must be prevented by using up-to-date virus protection software and implementing regulated patch management. If necessary, regular checks to identify weak points in the IT structure must also be carried out by external IT consultants. When downloading and saving programs or similar, make sure that they come from a trustworthy source. Downloading obviously illegal offers or platforms as part of orders from KOEPFER is not permitted. If the suspicion of an IT security incident (virus attack, encryption, unauthorized intrusion from outside, etc.) is confirmed, this must be reported to KOEPFER at security@koepfer.com within 24 hours of becoming aware of it.

2.3 Physical and Environmental Security
The supplier must ensure that unauthorized access to rooms, offices and facilities in which information is processed by KOEPFER is excluded. This also applies to delivery and loading areas through which unauthorized persons could enter the premises. The supplier must create guidelines that regulate tidy work environments and screen locks when not in use. As a general rule, access to and access to information must be limited to a clearly defined group of people and to the extent necessary to fulfill the task. Stored information must be protected against unauthorized access, unauthorized modification and loss.

2.3.1 Handling of operating resources and data carriers
To prevent unauthorized access, confidential documents must never be left unattended. Printed documents containing personal or confidential data must be disposed of appropriately, e.g. with a document shredder with security level P4 or higher. Only company-owned data carriers are used to exchange data. The use of private USB sticks, memory cards, etc. is prohibited. Independent disposal by the respective employee is prohibited. The resources provided may only be used for the intended purpose.

2.3.2 Clean Desk
When leaving the workplace, care must be taken to ensure that unauthorized persons cannot gain access to information from KOEPFER. It must be ensured that information on paper or other media is covered when people from outside the company are in the building. Even after a meeting in a conference room has ended, all information from conference rooms as well as content on flipcharts, whiteboards, etc. must be removed.

2.3.3 Working outside the organization
The supplier must create a policy for its employees that regulates work outside the organization. The focus must be on data confidentiality and preventing unauthorized parties from eavesdropping, viewing, physically stealing or electronically accessing information.

- KOEPFER documents should be stored in a lockable cabinet.
- Personal, confidential paper documents must be disposed of securely (e.g. data protection containers or document shredders). Alternatively, a paperless way of working is recommended.
- When using a smartphone, tablet and laptop, the screen must be protected from viewing as best as possible (e.g. by using a privacy film) (especially when third parties are sitting close, e.g. on an airplane)
- Confidential conversations, telephone calls and video conferences should not be held in public spaces, but only in protected places where no third party can listen.
- Hardware, data storage media and business documents must never be left unattended and should always be carried personally or locked securely.
- Secure access to the company network outside the business premises should, if possible, be established via a VPN connection (Virtual Private Network).

2.4 Protection of information assets
The supplier is required to record his information assets, evaluate their protection needs and implement necessary measures depending on the risk class. KOEPFER uses labeling of its information assets. A guide for classifying information can be provided to the supplier upon request. Documents marked “confidential”, as well as those whose contents are of sensitive value in the normal business world, may only be made accessible to selected employees. Documents marked “internal” are intended for the business relationship between suppliers and KOEPFER and can be freely distributed within the company.
In principle:

- Both data and the carrier of this data must be protected against loss, destruction, manipulation and unauthorized access. Data carriers that are no longer needed must be destroyed using secure procedures (e.g. document shredders from security level P4).
- Data exchange may only be carried out via data exchange channels approved by KOEPFER. The selected secure data exchange paths must meet the minimum requirements of ISO27001 (such as SMIME).
- The supplier must ensure that no unauthorized third parties can overhear or gain access to confidential information. If the supplier intends to consciously forward selected information to third parties, approval must be obtained from KOEPFER. This applies in particular to information about projects that are linked to a non-disclosure agreement. When sending emails, the distribution circle must be limited to the necessary extent.

2.5 Security-related incidents
Consistent and effective measures must be implemented for the management of information security incidents (theft, system failure, data loss, etc.) with a potentially negative impact.
This includes in particular:

- The immediate reporting of information security incidents to the client, especially when so-called cyber attacks become known.

- The logging of security incidents.
- The implementation of processes to initiate measures to prevent / repeat information security incidents
- If events become known that could lead to a violation of information security or data protection, the supplier is obliged to report this to security@koepfer.com within 24 hours.

2.6 Data backups
Measures must be implemented to ensure that sensitive information and data/personal data are protected against accidental destruction or loss.

2.6.2 Cryptography
The use of encryption procedures to ensure the proper and effective protection of the confidentiality, availability or integrity of personal data or information requiring protection. The use of cryptographic communication protection is particularly necessary when data requiring high levels of protection is transmitted over public networks or networks that are not considered sufficiently secure.

2.6.2 Protection of personal data
According to the EU General Data Protection Regulation (EU-GDPR), it is prohibited to process, disclose, make accessible or otherwise use personal data for a purpose other than that assigned to the respective regular fulfillment of tasks. The EU GDPR protects all data of natural persons that is recorded or processed. This also includes recordings on mobile, personal storage and processing media as well as information on forms. This obligation continues even after the activity has ended.

2.7 Emergency management
System availability must be maintained or restored as quickly as possible in difficult situations, such as crises or damage. The supplier must create emergency plans for the critical information assets and IT systems in order to ensure continued business operations. These emergency plans must be regularly tested for effectiveness and optimized if necessary.

3. Special features for organizations with access to the network

3.1 Handling Credentials and Media
Registration data may not be passed on to unauthorized persons. If compromise is suspected, the access data must be changed and the incident reported. As long as there is access to the KOEPFER network, leaving the workplace is prohibited.

3.2 Access rights
Access rights to KOEPFER systems must be requested. Access to KOEPFER data may only be made available to employees on a need-to-know basis.

3.3 Handling information
All information is to be treated under the fundamental assumption that it is strictly confidential. Local storage of information and data is prohibited. Adjustments and updates to software and IT systems must be registered and approved by the KOEPFER contact person.

4. Special features for software suppliers

The software supplied must not contain any functions that jeopardize the protection goals of the data and the software itself, in particular the unwanted introduction and exit of data and functions or the unwanted modification of data or the process logic. The supplier must check according to the state of the art that no potentially damaging software (e.g. viruses, worms, Trojans) is supplied.

5. Declaration of Commitment

5.1 Commitment of employees
The supplier's employees must be obliged by their management to maintain confidentiality in accordance with the existing confidentiality agreement between KOEPFER and the supplier. KOEPFER must be granted access to these agreements at any time. The supplier's employees must be obliged by their management to comply with legal data protection requirements. Evidence of compliance with this obligation must be presented to KOEPFER upon request.

5.2 Obligation and commissioning of third parties
Additional suppliers may only be commissioned after prior agreement and explicit approval by KOEPFER. Suppliers who have access to confidential information must be obliged to comply with the information and IT security requirements according to VDA ISA in an appropriate form in additional agreements (if in doubt, in the same way). This particularly applies to the departments and employees involved in the project.

6. Audit law

KOEPFER is entitled to enter the production facility and other business premises of suppliers and their pre-suppliers, subcontractors and other vicarious agents together with the end customer after prior notice during normal business hours and to check compliance with the requirements for the contractual products and underlying management systems. In urgent cases, e.g. acute complaints, KOEPFER is entitled to access on the day following the announcement.

7. Subject to change/voluntariness

KOEPFER Holding is entitled to change these or individual regulations hereat at any time to be replaced or supplemented by other regulations and to be repealed completely. The changes only become effective once the supplier has checked and approved them.