Content

1 Introduction

The Company often uses services or products from external service providers, which may sometimes contain sensitive or proprietary information or system components. When developing external service agreements, it should be taken into account that the products and services supplied by suppliers may provide the Company with information about the Company's internal operations, systems, tools or equipment and/or employees that is confidential or proprietary to the Company and therefore constitutes trade secrets.

This confidential or trade secret information may come into the possession of the supplier (external service provider) in various ways. Either by the Company providing such data or access to such data in order to cooperate with the supplier in the performance of a product or service, or by the supplier itself providing such data to the Company, which then becomes confidential or proprietary information internal to the Company.

This is important for all information, but for personal data, data relating to the Company's customers and data relating to the Company's IT systems, this is given special importance and legal effect by specific legislation.

The classification of this data according to data sensitivity and the corresponding protection is of paramount importance to the Company. The protection must be consistent throughout the lifecycle of the data (from its creation, use, storage, processing, return and destruction), including all organisations and individuals involved in this process. In this way, in order to guarantee the security of the data, this should also include the suppliers and external service providers concerned.

In connection with this, the Company is required to establish, operate and document information security (and cybersecurity) measures, assessment and evaluation processes that reduce the risk of malicious and accidental damage to the Company's data and systems mediated by contractors, suppliers, service providers and subcontractors.

This document sets out the necessary principles and implementation guidelines for the implementation of these requirements for typical, different types of suppliers and external service providers.

The general requirements for cooperation with subcontractors and external service providers for various subjects necessary for operations and other operational support are set out in Chapter 2, while the specific requirements for subcontractors providing infocommunications services are set out in detail in Chapter 3, as a special case.

2 Basic principles of information security requirements in procurement

The information security risks of the Company's subcontractors and external service providers determine the strict confidentiality and information security requirements - and their content - that need to be imposed and monitored in the course of each contract.

To achieve this, the following steps need to be implemented in a regulated manner within the framework of the Company's procurement and subcontractor management procedures, embedded in the individual stages of the procurement process:

a) Preparation, analysis, identification of risks at project level: identification of risks, design of measures, analysis of the criticality of residual risk (if necessary).
b) Requirements definition: based on the measures and the criticality analysis, information security requirements for the subcontractor's information security management system and the product or service it supplies can be defined.
c) Subcontractor selection phase: tender based on the basic requirements, obtaining certifications (e.g. ISO 27001 or other certifications, compliance with own supplier's information security/cybersecurity requirements list, which can be verified by subcontractor's checklist or by conducting a preliminary supplier audit) to help assess the suitability of the subcontractor.
d) In subcontracting: prescribing and enforcing confidentiality and information security requirements, and ensuring compliance with them.
e) Subcontractor monitoring: audit of the subcontractor, project close-out report; monitoring of assessed and significant subcontractor information security risks.

These steps are:

2.1 Preparation, analysis, identification of project-level risks

The information security risk of each subcontractor or external service provider collaboration is determined by the potential direct or indirect risk to the Company of inadequate security of the data managed, stored or accessed by that subcontractor or external service provider.

This information security risk assessment can already be done by the organisation requesting the procurement during the pre-requirement phase of the procurement process. The following should be identified:

- the subject, theme and timeframe of subcontracting and external service provider cooperation;
- which data owned by or important to the Company will be managed, accessed or available to the subcontractor, external service provider;
- what is the content and nature of this data;
- whether such data include personal data, data relating to a customer or a customer's product, and/or data relating to information technology systems or their operation;
- what is the data sensitivity classification of these data;
- by whom, where and how this data is held by the subcontractor;
- where and in what form this data is held by the subcontractor (electronically and on paper);
- where and how the subcontractor will have access to the storage of this data in the Company's system;
- how and in what way the subcontractor or external service provider uses this data in the course of providing its services;

- what security measures the subcontractor or external service provider takes to ensure the security of this data (if known in advance);
- whether there is already a confidentiality agreement with the subcontractor or external service provider and what it obliges them to do (if known in advance);

On the basis of this information, it is possible/necessary to determine the information security risks related to the given subcontractor or external service provider cooperation. To assess the risks, the following aspects should be considered:

- What damage event(s) could occur to the Company if the confidentiality/availability/integrity of this data is compromised?
- What kind of damage event(s) could occur to the Company if the security of the Company's data sharing is compromised (e.g. unauthorized access to data) during the cooperation with subcontractors or external service providers?
- In what ways could the security of this data be compromised in the subcontractor's or external service provider's own operations?

The identification of information security risks of subcontractors and external service providers should be assessed, taking into account the above aspects, together with the other subcontracting risks of the given cooperation project, and, if necessary, the appropriate measures should be identified. Therefore, the way to carry out this risk assessment is essentially to apply the existing subcontractor risk assessment in the preparation of the procurement, by adding to its scope/content the risks identified by the above criteria.

2.2 Definition of requirements

The main objective is to ensure that the information security risks posed by the subcontractor or external service provider are adequately managed by the subcontractor or external service provider. To do this, it is necessary to ensure that subcontracting contracts provide acceptable answers to the following questions by prescribing and enforcing subcontracting requirements.

- How does the subcontractor or external service provider ensure the security of this data within its own system?
- What guarantees do you give us to make sure and check this?
- What guarantee do you offer for damages suffered in the event of a breach of information security?

The information security risks of each subcontractor or external service provider cooperation determine the confidentiality and other information security measures required in the course of the cooperation. These measures should be defined as requirements for the preparation of the relevant cooperation agreements and then enforced in the subcontracting and external service provider agreements.

This can be done by the requesting organisation itself at the pre-procurement stage of the procurement process, immediately after the information security risk assessment, together with the specification of the product/service to be procured.

The scope, detail and security level of the requirements should be adapted as appropriate to the content of the cooperation, the volume of data handled or accessed by the subcontractor or external service provider, the sensitivity of the data and the information security risks identified. The requirements should cover at least the following topics, taking into account these aspects:

- the subject of the agreement;
- the period of validity of the agreement (temporary or permanent);

- a procedure to monitor the validity of provisional confidentiality agreements and to seek their timely renewal;
- the persons/organisations concerned (explicit list of supplier personnel authorised to access or receive information from the subcontractor, external service provider);
- the (content) nature of the information subject to the agreement and the data sensitivity category;
- rules on acceptable use of information, including, where appropriate, unacceptable use;
- the responsibilities of the parties to the agreement (i.e. the obligations of both parties);
- a statement of the obligation of confidentiality (including the definition and interpretation of a trade secret, the nature, rules and expectations of confidentiality, ...);
- provisions on the treatment of confidential, secret or other confidential information outside the contractual relationship;
- depending on the access to data or IT infrastructure, including data communication - the necessary information security requirements;
- rules on the maintenance, configuration, updating and testing of IT systems, including rules on mobile data media, portable computers, diagnostic and test equipment;
- the subcontractor's, external service provider's information security management system requirements, and the ability and evidence of compliance;
- security awareness and security awareness training of the subcontractor's or external service provider's staff involved in the given agreement;
- incident management requirements and procedures (in particular, notification and cooperation during incident recovery);
- the means of demonstrating compliance (e.g. independent third-party review or the Company's right to audit);
- extending confidentiality to subcontractors - where relevant;
- sanctions for non-compliance with the established safety requirements;

2.3 Subcontractor selection

Subcontractors are selected as part of the procurement process, typically through a tendering procedure. The suitability of the subcontractor to meet the above (defined) information security requirements should form the basis of the selection criteria.

This requires that, taking into account the results of the previous points, the tender dossier contains (at least) the following elements:

- subcontractor's declaration of confidentiality and acceptance of information security requirements;
- (if required) subcontractor certifications (e.g. ISO/IEC 27001, PCI DSS, SOC3, TISAX, ...);
- subcontractor's declaration of acceptance of the preliminary information security supplier audit (if applicable);

During the evaluation of the proposals, the technical evaluation of the proposals and the security clearance of the bidders is a process step that includes the evaluation of the suitability and compliance with the information security requirements. In different cases this can be done in the following ways:

- If the award is made on the basis of the lowest price principle, tenders will not be evaluated technically and professionally, but will be assessed for technical adequacy in terms of their compliance with the specifications set out in the call for tenders (compliant/not compliant). In this case, the information security requirements and expectations shall be specified in the tender dossier in such a way that compliance can be clearly determined by a yes/no answer based on the answers and declarations given.

- If the evaluation is based on the principle of the overall most advantageous tender, the technical and professional evaluation consists of two steps. First, the evaluators check that the tenders comply with the minimum technical and technical requirements and parameters set out in the call for tenders, including the information security requirements laid down therein. In the case of compliant and valid tenders, they are evaluated on the basis of technical, professional and other criteria (including information security), according to the specific rules for the evaluation criteria. The evaluation criteria will be approved in an internal document defined in accordance with the Company's procurement procedures. In this case, the evaluation criteria shall be complemented by information security criteria, where the degree of weighting shall be proportionate to the information security risks initially identified.

If necessary, e.g. to select a suitable subcontractor from among those in competition, the subcontractor's ability to comply with information security requirements can be verified, for example by requesting external (3rd party) certifications, or by checking the subcontractor's completion of a checklist of its own requirements, or by conducting an information security supplier audit of the subcontractor. The possibility to do so should be included in the Procurement Procedure.

2.4 Subcontracting

Compliance with confidentiality and information security requirements should be part of the subcontracting, external service provider agreement. It should therefore be documented as part of the subcontracting or external service provider agreement to ensure that there are no misunderstandings between the Company and the supplier or external service provider regarding the obligations of both parties to comply with the relevant information security requirements.

Depending on the type of cooperation and the type of contract, these confidentiality and information security requirements may form the core text of the contract itself, or they may be separate and valid annexes. Either way, they must in any case include a contractual specification and acceptance by both parties of the requirements set out in point 2.2 for the cooperation in question.

2.5 Subcontractor monitoring

When working with subcontractors and external service providers, it is important to ensure that the confidentiality and other information security requirements set out and contractually required are complied with at all times.

The monitoring and continuous observation of these, as part of the cooperation, is the responsibility of the cooperating company organisation.

If the procurement process includes a subcontractor performance evaluation procedure, which evaluates suppliers (subcontractors, external service providers) in terms of their contractual obligations and customer satisfaction, it is recommended to complement this evaluation criteria with an evaluation of compliance with information security requirements.

If there is no such procedure, it is necessary to establish one to monitor compliance with information security requirements and to monitor identified information security risks of subcontractors.

3 Information security requirements for information communication service providers

In the case of ICT service providers, the information security requirements aim to protect the Company's data in the IT and communication system provided and to ensure the secure and continuous operation of the ICT service.

In the case of the Company's IT services operated by external companies, the operating company itself regulates the operation and operational security on the basis of its own internal procedures.

It is the responsibility of the Company, as the IT service user, to enforce the appropriate information security and operational requirements that are important and required by the Company through the service contract, and to hold the service accountable and monitor them, also in accordance with the terms of the contract.

Through information and communications technology (ICT) services provided by external service providers, service providers (suppliers) access (or manage) the service user's data, information, infrastructure and (to the extent appropriate to the level of service) influence the performance and efficiency of the service user's business processes. These and the associated information security risks should be the basis for establishing the conditions for the operation of IT services by an external party to protect against intentional or accidental data leakage, unauthorised access to data, lack of availability of IT services, etc.

3.1 Requirements for service (supplier) contracts

Agreements with suppliers (directly or indirectly) should include requirements that address and guarantee the resolution of information security risks associated with the information and communication technology service and product supply chains.

Considerations on the content of contracts:

- Confidentiality statement (on the part of the subcontracting organisation, and individually on the part of the subcontractor's personnel who have access to the Company's data);
- Information concerned (transferred or accessed) and the method of controlling and implementing access to it;
- The classification of the information in the Company's security class and the expectations of the security class with the service provider;
- To set requirements in line with the relevant legal requirements;
- The level of security control or control required for access to data, - on both sides;
- Permitted rules for processing or handling information or a list of the supplier's personnel who have access to the information;
- The information security rules applicable to the specific contract (paper and electronic data processing and, where applicable, physical security);
- Establish procedures for information, contact and cooperation in the event of incidents;
- Set expectations for security awareness training for those involved in providing the service;
- Impose requirements (including controls) on the supplier's subcontractors;
- Names of contact persons responsible for information security;
- The names of the employees of the subcontractor who have access to the Company's data;
- Information security supplier audit and other process audits and/or security or security awareness audits (if required), including the rights, requirements and conditions and framework;

- Troubleshooting (problem-solving) expectations;
- Penalties for breaching the information security requirements of the contract;
- Requirements for the return of information and media on termination or expiry of the contract, and for the destruction of information on the contractor's media;
- Validation and quality assurance requirements for the ICT services provided;

3.2 Oversight of outsourced ICT services

The Company's outsourced IT services department (or the department appointed to be responsible for the outsourced IT services department) shall regularly monitor, evaluate and review the performance of the vendor services, in the following respects:

- Monitoring the quality of service delivery (e.g. SLA), checking compliance with agreements;
- Review service reports prepared by the service provider and, if necessary, organise system meetings as required by the service contract;
- Enable supplier audits or other process audits and/or safety or security awareness audits;
- Requesting and reviewing information on information security incidents in accordance with service provider contracts;
- Obtaining and reviewing the service provider's audit trail documents related to the provision of the service, as well as safety events, operational problems, failures, faults and records of interruptions related to the provision of the service, in accordance with the service provider's contracts;
- Address and solve the problems identified;
- Reviewing suppliers' own supplier-related information security aspects;
- Verifying and monitoring that the supplier has sufficient and appropriate capacity (and capability) and suitable plans to ensure the agreed service continuity without service failures and disasters.

Date: .....

Commissioned by: ..... Commissioned by: .....