Supplier Security Directive

Table of contents

1 Description 2
2 Definitions 2
3 Scope 3
4 The Supplier´s overall responsibility 3
5 Security requirements 3
- 5.1 Risk Management 3
  - 5.1.1 Security risk management 3
  - 5.1.2 Security risk management for Personal Data 3
- 5.2 Information security policies 4
- 5.3 Organization of information security 4
- 5.4 Human resources security 4
- 5.5 Asset management 5
- 5.6 Access control 5
- 5.7 Encryption 5
- 5.8 Physical and environmental security 5
  - 5.8.1 Admission to Buyer's premises and Buyer’s leased premises 5
- 5.9 Operations security 6
- 5.10 Communications security 6
- 5.11 System acquisition, development and maintenance (when software development or system development is provided to the Buyer by Supplier) 6
- 5.12 Personal Data processing 7
- 5.13 Supplier relationship with sub-contractors 7
- 5.14 Security incident management 7
- 5.15 Business continuity management 8
- 5.16 Compliance 8

6 Information security confidentiality classification description and handling requirements 8
- 6.1 Information security confidentiality classification description 8
- 6.2 Information security confidentiality classification handling requirements 9

1 Description

This document “Supplier Security Directive” describes the security requirements applicable to suppliers and other identified business partners to Telia Company. Additional security requirements may apply if agreed by involved parties.

2 Definitions

1. “**Agreement**” shall mean the agreement between Telia Company and Supplier or other identified business partner to the Telia Company group under which the Supplier Security Directive apply, and to which the Supplier Security Directive is part thereof.
2. “**Buyer**” shall mean Telia Company AB or the relevant Telia Company Affiliate.
3. “**Buyer’s Data**” shall mean data or other information that the Buyer, or a person acting on behalf of the Buyer, makes available to the Supplier, including but not limited to Personal Data and the result of Supplier’s processing of such data.
4. “**Information Processing Facilities**” shall mean any information processing system, services or infrastructure, or the physical locations housing them.
5. “**Log**” shall mean to record details of information or events in an organized record-keeping system, usually sequenced in the order in which the information or events occurred.
6. “**Personal Data**” shall mean any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be directly or indirectly identified by reference to an identifier such as a name, address, social security number, subscription number, IP address, location data, an online identifier, traffic data or message content or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
7. “**Applicable Data Protection Laws**” shall mean all information subject to applicable data protection laws, including without limitation to the “Directive on privacy in electronic communications” (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector) and “General Data Protection Regulation” (Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 94/46/RC) and any amendments, replacements or renewals thereof (collectively the “EU Legislation”), all binding national laws implementing the EU Legislation and other binding data protection or data security directives, laws, regulations and rulings valid at the given time.
8. **"Regulatory Requirements”** shall mean all applicable laws, rules, regulations and treaties, in force from time to time, of any international political and economic organization (e.g. the European Union), country, state, administrative agency or governmental body (e.g. the relevant Financial Services Authority, Data Protection Authority, Consumer Protection Agency or Chemicals Agency), as well as any applicable case law, orders, decisions, licences, recommendations, policies, standards and guidelines issued by the said bodies, courts and/or by self-regulatory or advisory organisations and industry sector groups.
9. “**Services**” shall mean the services to be provided by the Supplier to the Buyer, or a person acting on behalf of the Supplier as further defined in the Agreement between the parties.
10. “**Supplier**” shall refer to the counter-party who supplies any kind of deliverables to Buyer identified as “Supplier”, “Vendor, “Partner” or the equivalent in the relevant Agreement.
11. “**Supplier Personnel**” shall mean any person working on behalf of the Supplier such as employees, consultants, contractors and sub-suppliers.
12. “**Security Control**” shall mean any technical countermeasure, organizational setup or process, that helps to maintain IT systems security-quality properties.
13. “**Security Incident**” shall mean a single or a series of unwanted or unexpected security events that have a significant probability of compromising business operations and threatening security.
14. “**Sensitive Products**” and “**Sensitive Services**” shall mean any product or Services defined as sensitive by the Buyer. Sensitive Products or Sensitive Services shall be clearly documented in the applicable Agreement.
15. “**Industry Standard**” shall mean a practice, method, process or criteria, such as well as known security best practices supporting high standards of resilience, and use of unbroken protocols etc, that is formally approved by industry members.

16. “**Pseudonymization**” shall mean the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person

3 Scope

The Supplier Security Directive applies when:

1. The Supplier will process Buyer’s Data, excluding the contact information required to establish or maintain a business relationship.
2. The Supplier will have unescorted access to Buyer’s premises, excluding external areas.
3. The Supplier will access Buyer’s network or IT systems, including remote access.
4. The Supplier will handle Buyer’s information processing equipment.
5. The Buyer has deemed the Supplier as a provider of Sensitive Products and/or Sensitive Services and identified Supplier as such under the relevant Agreement.

4 The Supplier´s overall responsibility

1. The Supplier is fully responsible for the Supplier Personnel’s compliance with the Supplier Security Directive.
2. The Supplier shall implement the measures required to ensure compliance to the Supplier Security Directive prior to commencing any assignment for the Buyer.
3. The Supplier shall, at the request of the Buyer, inform the Buyer how the Supplier complies with the Supplier Security Directive and what measures the Supplier has taken to comply with the Supplier Security Directive.
4. The Supplier shall inform the Buyer at cert@teliacompany.com about any Security Incident (including but not limited to incidents in relation to the processing of Personal Data) as soon as possible but no later than 24 hours after the Security Incident has been identified. See Section 5.14 “Security incident management” below.
5. The Supplier shall assure that any processing of Buyer’s Data will be compliant with the Supplier Security Directive.
6. The Supplier shall not allow any access to Buyer’s Data (it may also concern new, extended, updated, prolonged or in any other way changed real-time network access) in breach of the Agreement to any party without prior written approval by the Buyer.

5 Security requirements

5.1 Risk Management

5.1.1 Security risk management

1. The Supplier shall identify and evaluate security risks related to confidentiality, integrity and availability; and based on such evaluation to implement appropriate technical and organizational measures to ensure a level of security which is appropriate to the risk.
2. The Supplier shall have documented processes and routines for handling risks within its operations.
3. The Supplier shall periodically assess the risks related to information systems and processing, storing and transmitting information. The Supplier shall ensure that residual risks identified during assessment of information systems are periodically reviewed, updated and actively mitigated.

5.1.2 Security risk management for Personal Data

1. The Supplier shall identify and evaluate security risks related to confidentiality, integrity and availability; and based on such evaluation to implement appropriate technical and organizational measures to ensure a level of security which is appropriate to the risk of the specific Personal data types and purposes being processed by the Supplier, including inter alia as appropriate:
    a) The pseudonymization and encryption of personal data
    b) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services

c) The ability to restore the availability and access to Buyer's Data in a timely manner in the event of a physical or technical incident
d) A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

2. The Supplier shall have documented processes and routines for handling risks when processing Personal Data on behalf of Buyer.
3. The Supplier shall periodically assess the risks related to information systems and processing, storing and transmitting Personal Data.

5.2 Information security policies

1. The Supplier shall have a defined and documented information security management system (ISMS) including an information security policy and procedures in place, which shall be approved by the Supplier's management, published within Supplier´s organization and communicated to relevant Supplier Personnel.
2. The Supplier shall periodically review the Supplier's security policies and procedures and update them if required to ensure their compliance with the Supplier Security Directive.

5.3 Organization of information security

1. The Supplier shall have defined and documented security roles and responsibilities within its organization.
2. The Supplier shall appoint at least one person having appropriate security competence, bearing ultimate responsibility for implementing the security measures under the Supplier Security Directive and who shall be the single point of contact for Buyer's security staff.

5.4 Human resources security

1. The Supplier shall ensure that the Supplier Personnel handles information in accordance with the level of confidentiality required under the Agreement.
2. The Supplier shall ensure that relevant Supplier Personnel is aware of the approved use (including use restrictions as the case may be) of information, facilities and systems under the Agreement. Buyer has the right to request a signed receipt from each and every Supplier Personnel stating that he or she has understood and will comply with the Supplier Security Directive and the approved use of information, systems and facilities.
3. The Supplier shall ensure that any Supplier Personnel performing assignments under the Agreement is trustworthy, meets established security criteria and has been, and during the term of the assignment will continue to be, subject to appropriate screening and background verification.
4. Supplier shall not, without informing and getting the Buyer's prior written approval, assign any Supplier Personnel to Buyer's assignment that:
    i. have any conflict of interest in relation to Buyer or the relevant assignment, or
    ii. has been convicted to imprisonment for any criminal offense during the three (3) year period prior to the engagement or the assignment,

   if that Supplier Personnel will in any manner:
    a) process Personal Data relating to Buyer customers or staff, or to Buyer's customers', or
    b) assist with tasks classified as sensitive by Buyer.

   The Buyer shall provide information about what tasks are classified as sensitive at the time of entering into the Agreement or the latest two weeks prior to a Supplier's Personnel engagement or assignment commences.
5. The Supplier shall ensure that Supplier Personnel with security responsibilities is adequately trained to carry out security related duties.
6. The Supplier shall provide or ensure periodical security awareness training to relevant Supplier Personnel. Such Supplier training shall include, without limitation:
    a) How to handle customer information security (i.e. the protection of the confidentiality, integrity and availability of information);
    b) Why information security is needed to protect customers information and systems;
    c) The common types of security threats (such as identity theft, malware, hacking, information leakage and insider threat);
    d) The importance of complying with information security policies and applying associated standards/procedures;
    e) Personal responsibility for information security (such as protecting customer's privacy-related information and reporting actual and suspected Security Incidents).

5.5 Asset management

1. The Supplier shall have a defined and documented asset management system in place and maintain up-to-date records of all relevant assets and their owners. Information assets include, but are not limited to, IT systems, backup and/or removable media containing confidential or secret information, access rights, software and configuration.
2. The Supplier shall label, treat and protect information according to a pre-defined information classification following Industry Standard (including, but not limited to, removable media storage, disposal and physical transfer)
3. The Supplier shall implement measures to ensure protection against accidental, unauthorized or unlawful loss, destruction, alteration or damage to Buyer data transmitted, stored or otherwise processed.
4. The Supplier shall keep an updated list of Buyer's data processed. The list shall contain the following information:
    a) The processed data
    b) Storage details, such as asset name, location etc.
5. The Supplier shall return or destroy (as determined by the Buyer) any of the Buyer's Data and copies thereof. The Supplier shall issue a signed acknowledgement or a deletion certificate upon termination of the Agreement.
6. The Supplier shall not extract information from the Buyers Data or the Buyer's customer Data, it should be described by the Supplier and explicitly approved by the Buyer before executing in operation; including but not limited to;
    a) Information directly or indirectly related to customers of the Buyer, including statistics.
    b) Information relating to the configuration of systems or equipment describing topology or in bulk.
    c) All machine-to-machine communication, such as extracting data for analytics that is not directly connected to the service delivered.

5.6 Access control

1. The Supplier shall have a defined and documented access control policy for facilities, sites, network, system, application and information/data access (including physical, logical and remote access controls), an authorization process for user access and privileges, procedures for revoking access rights and an acceptable use of access privileges for the Supplier Personnel in place.
2. The Supplier shall have a formal and documented user registration and de-registration process implemented to enable assignment of access rights.
3. The Supplier shall assign all access privileges based on "need-to-know" and "least privilege" principles.
4. The Supplier shall use strong authentication (multi-factor) for remote connection access, elevated access and/or any other type of privileged access
5. The Supplier shall ensure that all relevant Supplier Personnel has a personal, unique and non-transferable identifier (user ID), and use an appropriate authentication technique, keeping accountability of user's actions.

5.7 Encryption

1. The Supplier shall ensure proper and effective use of cryptography on information classified as confidential and secret (such as Personal Data) according with Buyer's confidentiality classification scheme, as per Section 6.
2. The Supplier shall protect cryptographic keys.

5.8 Physical and environmental security

1. The Supplier shall protect Information Processing Facilities against external and environmental threats and hazards, including power/cabling failures and other disruptions caused by failures in supporting utilities. This includes physical perimeter and access protection.
2. The Supplier shall protect goods received or sent on behalf of the Buyer from theft, manipulation and destruction.

5.8.1 Admission to Buyer's premises and Buyer's leased premises

The Supplier's admission to Buyer's premises and property (such as datacenter buildings, office buildings, technical sites) is subject to the following:

1. The Supplier shall follow local regulations (such as regulations for "restricted areas") for Buyer's premises when performing the assignments under the Agreement.
2. Supplier Personnel shall carry ID card or a visitor's badge visible at all time when working within the Buyer's premises.

3. After completing the assignment, or when Supplier Personnel is transferred to other tasks, the Supplier shall without delay inform the Buyer of the change and return any keys, key cards, certificates, visitor's badges and similar items.
4. Keys or key cards shall be personally signed for by Supplier Personnel and shall be handled according to the written rules given upon receipt.
5. Loss of the Buyer's key or key card shall be reported without delay to the Buyer.
6. Photograph or video recording within Buyer's premises without permission is strictly prohibited.
7. Buyer's goods shall not be removed from Buyer's premises without permission.
8. Supplier Personnel shall not allow unauthorized persons access to the premises.

5.9 Operations security

1. The Supplier shall have an established change management system in place for making changes to business processes, Information Processing Facilities and systems. The change management system shall include tests and reviews before changes are implemented, such as procedures to handle urgent changes, roll back procedures to recover from failed changes, logs that show, what has been changed, when and by whom.
2. The Supplier shall implement malware protection to ensure that any software used for Supplier's provision of the deliverables to the Buyer is protected from malware.
3. The Supplier shall make backup copies of critical information and test back-up copies to ensure that the information can be restored as agreed with the Buyer.
4. The Supplier shall Log and monitor activities, such as create, reading, copying, amendment and deletion of processed data, as well as exceptions, faults and information security events and regularly review these. Furthermore, the Supplier shall protect and store (for at least 6 months) Log information, and on request, deliver monitoring data to the Buyer. Anomalies, incidents and/or indicators of compromise shall be reported according to the incident management requirements, Section 5.14.
5. The Supplier shall have defined, documented and monitored procedures for administrative operations of computing environments where the Buyer's Data and the Buyer's customer Data is processed.
6. The Supplier shall manage vulnerabilities of all relevant technologies such as operating systems, databases, applications proactively and in a timely manner.
7. The Supplier shall establish security baselines (hardening) for all relevant technologies such as operating systems, databases, applications.
8. The Supplier shall ensure development is segregated from test and production environment.
9. The Supplier shall implement network Security Controls such as service level, firewalling and segregation to protect information systems and, upon request, be able to provide related logs and evidence to the Buyer.
10. In case Buyer's data is processed on a multi-tenant environment operated by the Supplier, the Supplier shall implement security controls to isolate Buyers Data from other tenants and unauthorized users, following Industry Standard

5.10 Communications security

1. The Supplier shall ensure that at least all communication of information classified as internal, confidential or secret is secured according to the Buyer's information classification description in section 6 (Information security confidentiality classification description and handling requirements).

5.11 System acquisition, development and maintenance (when software development or system development is provided to the Buyer by Supplier)

1. The Supplier shall implement rules for the development lifecycle of software and systems including change and review procedures.
2. The Supplier shall establish, document and maintain principles for secure system architecture and those principles shall be applied to the Supplier's information system development and implementation efforts.
3. The Supplier shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.
4. The Supplier shall test security functionality during development in a controlled environment.
5. The Supplier shall not use the Buyers data for testing purposes unless it is required by the Buyer.
6. The Supplier shall ensure that information involved in application services, passing over public networks shall be protected from fraudulent activity, unauthorized disclosure and modification.

7. The Supplier shall ensure the protection of confidentiality and integrity of information involved in application service transactions.

5.12 Personal Data processing

This section (5.12) shall apply whenever the Supplier is considered as Data Processor of Personal Data where the Buyer is the Data Controller. The following terms constitutes the controller´s instructions on the **security requirements** of personal data. The terms specify the minimum-security requirements regarding Personal Data. The general legal terms of the DPA is attached to the Master Agreement.
Sections (4.2.3 – 4.2.5.) regarding Access Control and Operational Security are applicable for Data at rest and Data in use.

1. The Supplier shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk related to the processing. In assessing the appropriate level of security account shall be taken of the risks from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data processed. Based on the results of the privacy risk assessment the Supplier shall plan, implement and control the processes needed to meet data protection and privacy requirements.
2. The Supplier shall promote Privacy by Design and put into place accountability and governance measures.
3. The Supplier shall inform the Buyer at controlcenterem-security@teliacompany.com about any incidents in relation to Personal Data without undue delay after the Personal Data Incident has been identified.
4. **Data at rest:** The Supplier shall ensure the confidentiality, integrity, availability and resilience of processing systems and services. The Supplier shall ensure that Personal Data storage is logically and physically protected and controlled, has restricted access control and is protected according to section 6 (Information security confidentiality classification description and handling requirements). Personal Data shall be classified and handled at least as Confidential.
5. **Data in transit:** The Supplier shall implement robust security controls to ensure that Personal Data is transferred through
protected communication channels in a controlled and trusted network, or in a secure portable storage to ensure the confidentiality and integrity of Personal Data. Security controls such as TLS, SFTP etc. according to current Industry Standards.
6. **Data in use:** The Supplier shall ensure that Personal Data is only processed by authorized person(s) in a controlled workspace and protected from harmful use. Furthermore, the Supplier shall ensure that privacy policy is in place, that privacy processes are implemented, that awareness programs are deployed, that change management control is in place and that dual-control principles are implemented.

5.13 Supplier relationship with sub-contractors

1. The Supplier shall reflect the content of the Supplier Security Directive in its agreements with sub-contractors that perform tasks assigned under the Agreement.
2. The Supplier shall regularly monitor, review and audit sub-contractor compliance with the Supplier Security Directive.
3. The Supplier shall, at the request of the Buyer, provide the Buyer with evidence regarding sub-contractor's compliance with the Supplier Security Directive.

5.14 Security incident management

1. The Supplier shall have established procedures for Security Incident management.
2. The Supplier shall inform the Buyer at cert@teliacompany.com about any Security Incident without undue delay after the Security Incident has been identified.
3. All reporting of security related incidents shall be treated as confidential information and be encrypted, using Industry Standard encryption methods such as PGP or equal Industry Standard encryption.
4. The security incident report shall contain at least the following information:
    a) Notwithstanding the requirement for immediate notification, the Supplier shall, comprise a written preliminary report to the Buyer of any security incident that could possibly affect the Buyer or the Buyer's assets in any imaginable way
    b) Sequence of events, including actions taken during the incident handling
    c) Affected portions of the infrastructure, systems and information

d) Estimated (or, upon a high level of uncertainty, worst-case) consequences/impact
e) Consequence reducing measures already implemented
f) Risk-reducing measures already implemented
g) Consequence reducing measures to be implemented, including implementation plan (date; responsible; dependencies)
h) Risk reducing measures to be implemented, including implementation plan (date; responsible; dependencies)
i) Experiences summary including root cause analysis

5. The Supplier shall provide the Buyer with support in case of forensic investigation.

5.15 Business continuity management

The Supplier shall:

1. Have documented processes and routines for handling business continuity including disaster recovery.
2. Ensure that information security is embedded into the business continuity plans
3. Periodically identify, analyze and evaluate business continuity risks and take necessary actions to control and mitigate such risks.
4. Periodically, at least annually (unless otherwise agreed), assess the efficiency of its business continuity management including disaster recovery, and compliance with availability requirements.

5.16 Compliance

1. The Supplier shall comply with all Regulatory Requirements and contractual requirements including but not limited to Personal Data protection.
2. The Supplier shall, on request, provide the Buyer with a compliance status report with regards to the security requirements without any unjustified delay.
3. The Supplier shall, at the request of the Buyer, inform the Buyer how the Supplier complies with the security requirements and what measures the Supplier has taken to comply with the security requirements.
4. The Supplier shall regularly monitor, review and audit sub-contractor´s compliance with the security requirements.
5. The Supplier shall, at the request of the Buyer, provide the Buyer with evidence regarding sub-contractor's compliance with the security requirements
6. The Buyer has the right to audit how the Supplier and its sub-contractors fulfil the security requirements or corresponding requirements.
7. If an incident falls under legal requirements to be reported to the authorities, the Buyer shall be entitled to perform incident audit within three (3) hours' notice.
8. If an incident does not fall under legal requirements to be reported to the authorities, the Buyer shall be entitled to perform incident audit with five (5) days' notice.
9. As to surveillance requests about Buyer's customers and users received outside of Buyer's normal routines (e.g. if received directly by the Supplier), such must be referred to Buyer.

6 Information security confidentiality classification description and handling requirements

6.1 Information security confidentiality classification description

Class	Description	Examples of information types
Secret	The unauthorized access or **disclosure of information could seriously damage Telia Company**, its organization, critical functions, workforce, business partners and/or its customers.	- annual report and result before they have been released - certain information based on legal requirements or specific customer agreements or non-disclosure agreements
Confidential	The unauthorized access or **disclosure of information could damage Telia Company**, its organization, critical functions, workforce, business partners and/or its customers.	- certain information based on legal requirements e.g. personal data of customers or employees - sensitive business plans, strategies and decisions (e.g. marketing plans)

Internal	The unauthorized access or **disclosure of information could cause minor damage Telia Company**, its organization, critical functions, workforce, business partners and/or its customers.	- information that is meant for TC's internal use - communication materials targeted to all TC employees e.g. related to TC organization, strategy, products, employee services
Public	The unauthorized access or **disclosure of information causes no damage Telia Company**, its organization, critical functions, workforce, business partners and/or its customers.	- annual report and result after they have been released - marketing materials and press releases that are published - information that needs to be published based on legal requirements

6.2 Information security confidentiality classification handling requirements

Class	Who may access the information	How to store	How to transfer	How *to* use	How to assess need for protection (risk-based approach)
Secret	Appointed persons only	Logically and physically secure storage i.e. encrypted or locked	Through secure communication channels or in a secure portable storage (locked)	To be used within secure areas that are protected from insight and eavesdropping (by unauthorized persons)	It shall be very hard to break the protection. Only highly motivated and/or resourceful attackers could dismantle the protection.
Confidential	A limited *and controlled* group of persons only	Logically and physically controlled and trusted storage with strict access control	Through secure communication channels or within a controlled and trusted network, or in a secure portable storage	To be used by authorized persons for business purposes only within a controlled workspace or place protected from insight and eavesdropping (by unauthorized persons)	It shall be hard for unauthorized persons to get access to the information. Only well motivated attackers could dismantle the protection.
Internal	Those who perform work for Telia Company	Under logical and physical access control	Through protected communication channels or within a trusted network	To be used by authorized persons for business purposes only within a controlled workspace or place protected from insight and eavesdropping (by unauthorized persons)	It shall be unlikely for unauthorized persons to get access to the information. Only motivated attackers could dismantle the protection.
Public	No restrictions	No restrictions	No restrictions	No restrictions	No restrictions