SUPPLIER SECURITY DIRECTIVE

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

"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.

"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.

"Buyer" shall mean Telia Company AB or the relevant Telia Company Affiliate.

"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.

"Cloud computing" or **"Cloud"** shall mean a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

"Industry Best Practice" 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 generally accepted and followed by industry members

"Information Processing Facilities" shall mean any information processing system, services or infrastructure, or the physical locations housing them.

"Information Security Management System" or **"ISMS"** shall mean the relevant part of the overall management system, based on a business risk approach, intended to establish, implement, operate, monitor, review, maintain and improve information security. The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources

"Infrastructure as a Service" or **"IaaS"** shall mean a service which its capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

“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.

“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.

“Platform as a Service” or **“PaaS”** shall mean a service which its capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.3 The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

“Private cloud” shall mean a type of cloud computing deployment model on which the cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

“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.

"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.

“Security Control” shall mean any technical countermeasure, organizational setup or process, that helps to maintain IT systems security-quality properties.

“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.

“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.

“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.

“Software as a Service” or **“SaaS”** shall mean a service which its capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.

"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.

"Supplier Personnel" shall mean any person working on behalf of the Supplier such as employees, consultants, contractors and sub-suppliers.

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 "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

Security risk management

1. The Supplier shall periodically identify, analyze, evaluate and treat security risks.

2. The Supplier shall be able to provide evidence of risk assessments upon request related to the services/products that the Buyer has purchased.

5.2 Information security policies

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.

5.3 Organization of information security

The Supplier shall have defined and documented security roles and responsibilities within its organization.

5.4 Human resources security

The Supplier shall ensure that any Supplier Personnel performing assignments under the Agreement is trustworthy and meets any established security criteria for the assignment.

5.5 Asset management

5.5.1 Physical Assets

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. Assets include, but are not limited to, information, IT systems, backup and/or removable media containing information, access rights, software and configuration.

5.5.2 Data

a) 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.

b) The Supplier shall return or destroy (as determined by the Buyer) any of the Buyer's Data and copies thereof. The Supplier shall confirm in writing to the Buyer that the Supplier has met this requirement on termination of the Agreement.

5.6 Access control

1. Have defined and documented access control policy for facilities, sites, network, system, application and information/data access (including physical, logical and remote access controls).

2. Have 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.

3. Assign all access privileges based on the principle of need-to-know and principle of least privilege.

5.7 Encryption

1. When encryption is required according to section 6 "Information security confidentiality classification description and handling requirements" or according to the agreement concluded between the parties, the Supplier shall ensure proper and effective use of encryption according to Industry Best Practices.

2. The Supplier shall use encryption methods which are considered secure according to Industry Best Practices.

5.8 Physical and environmental security

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.

5.9 Operations security

1. Implement malware protection to ensure that any software used for Supplier's provision of the deliverables to the Buyer is protected from malware.

2. Implement operational and technical security controls such as log management, firewalls, antivirus and encryption according to the established security standard.

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.

5.10 Communications security

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 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, at the request of the Buyer, provide the Buyer with evidence regarding sub-contractor's compliance with the Supplier Security Directive.

5.12 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 Best Practice encryption methods such as PGP or equal Industry Best Practice encryption.

5.13 Business continuity management

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. Contribute in mutual Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) upon request by the Buyer.

5.14 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. If an ISAE3000/SSAE18 SOC2 Type I/II and/or SOC3 report is available, it shall be provided to the Buyer.

4. 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.

5. The Supplier shall regularly monitor, review and audit sub-contractor´s compliance with the security requirements.

6. The Supplier shall, at the request of the Buyer, provide the Buyer with evidence regarding sub-contractor's compliance with the security requirements.

7. The Buyer has the right to audit how the Supplier and its sub-contractors fulfil the security requirements or corresponding requirements.

8. 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.

9. 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.

6. Information security confidentiality classification description and handling requirements

6.1 Information security confidentiality classification description

Class	Description	Examples of information types
Secret	Unauthorized access or **disclosure of information could seriously damage Telia Company**, its organization, critical functions, workforce, business partners and/or customers.	-Annual report or financial results before public release. -Certain information based on legal requirements, specific customer agreements or non-disclosure agreements
Confidential	Unauthorized access or **disclosure of information could damage Telia Company**, its organization, critical functions, workforce, business partners and/or customers.	-Certain information based on legal requirements (i.e., personal data of customers or employees) -Sensitive business plans, strategies, and decisions (i.e., marketing plans)
Internal	Unauthorized access or **disclosure of information could cause minor damage Telia Company**, its organization, critical functions, workforce, business partners and/or customers.	-Information that is meant for TC's internal use -Communication materials targeted to all TC employees (i.e., related to TC organization, strategy, products, employee services)
Public	Unauthorized access or **disclosure of information causes no damage Telia Company**, its organization, critical functions, workforce, business partners and/or customers	-Annual report and result after they have been released -Marketing materials and published press releases. -Information that needs to be published based on legal requirements

6.2 Information security confidentiality classification handling requirements

Class	Who may access	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	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, 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	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	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

SUPPLIER SECURITY DIRECTIVE - SUB-ANNEX HARDWARE

1. Description

This document is a sub-annex to “Supplier Security Directive”, aiming to govern and describe specific terms related to deliveries based on hardware of different types and describes the security requirements applicable to suppliers and other identified business partners to Telia. Additional security requirements may apply if agreed by involved parties.

2. Scope

The Hardware Sub-Annex of Supplier Security Directive applies when:

1. The Supplier will provide ICT hardware as a delivery to Telia.

2. The content of delivery is an “Infrastructure as a Service” or “Platform as a Service” Cloud computing system or platform.

3. The Supplier will provide ICT hardware directly to Buyer’s customers.

3. Common security requirements for all types of Hardware deliveries

3.1 Risk Management

3.1.1 Security risk management

1.The Supplier shall have an established security risk management framework in accordance with Industry Best Practice, such as ISO/IEC 27005 or ISO 31000. The security risk management framework shall:

a) Identify security risks related to Confidentiality, Integrity and Availability.

b) Analyze security risks based on consequences and likelihood.

c) Evaluate security risks against an acceptance criteria.

d) Define security risk treatment measures which is appropriated to the risk.

2.The Supplier shall be able to provide evidence on assessment of security risks and measures taken to mitigate those risks according to acceptance criteria set by Supplier related to the Deliverables.

3.2 Information security policies

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.

3.3 Organization of information security

1. 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.

2. The Supplier shall secure resources and necessary competence to maintain its ISMS.

3.4 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 have a disciplinary process which covers information security related misconduct.

3. 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) Responsibility for information security relating to the Buyer's confidential, secret or Personal Data (such as protecting customer's privacy-related information, GDPR obligations and reporting actual and suspected Security Incidents).

3.5 Asset management

Physical Assets

The Supplier shall label, treat and protect assets according to a Telia pre-defined classification specified in "Supplier Security Directives - Generic Requirements" section 6 following Industry Best Practices (including, but not limited to, information, removable media storage, disposal and physical transfer).

3.6 Access control

1. The Supplier shall have a formal and documented user registration and de-registration process implemented to enable assignment of access rights.

2. The Supplier shall use strong authentication (multi-factor) for remote access users and users connecting from any untrusted network.

3.7 Encryption

The Supplier shall protect and rotate encryption keys in line with the sensitivity of the information they are being used to protect.

3.8 Operations security

1. The Supplier shall have a vulnerability management process in place which includes scanning, penetration testing and patching.

2. The Supplier shall manage vulnerabilities of all relevant technologies such as operating systems, databases, applications proactively and in a timely manner.

3. The Supplier shall establish security baselines (hardening) for all relevant technologies such as operating systems, databases, applications.

4. 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.

5. The Supplier shall ensure that all development, test and production environments are segregated.

3.9 System acquisition, development and maintenance

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 ensure the protection of confidentiality and integrity of information involved in application service transactions.

3.10 Cloud Security

The Supplier shall provide onboarding processes, methodology, and technology, that ensures strict data security for all data transfers and service initialization.

3.11 Security incident management

1. 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) Experience summary including root cause analysis.

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

3.12 Business continuity management

The Supplier shall periodically, at least annually (unless otherwise agreed), assess the efficiency of its business continuity management including disaster recovery, and compliance with availability requirements.

4. Security requirements for ICT Hardware deliveries addressed to Telia Company enterprise.

4.1 Access control

Access to the Buyer's Data in the Buyer's system (On-Premises)

1. All remote access to the Buyers systems shall be authorized and approved by the Buyer.

2. The Supplier (or as the case may be: Supplier's Personnel) may only access Buyer's systems upon and in accordance with the Buyer's access authorization. If access is granted to a specific individual, i.e., Supplier's Personnel, it is explicitly prohibited to transfer such access to another individual.

4.2 Physical and environmental security

The Supplier shall protect goods received or sent on behalf of the Buyer from theft, manipulation and destruction.

4.3 Business continuity management

The Supplier shall ensure that information security is embedded into the business continuity plans

5. Security requirements for ICT Hardware deliveries addressed to Telia Company Infrastructure

5.1 Asset management

Data

The Supplier shall guarantee that any processing of the Buyer's Data will be compliant with the Supplier Security Directive.

5.2 Access control

Access to the Buyer's Data in the Buyer's system (On-Premises)

1. All remote access to the Buyers systems shall be authorized and approved by the Buyer.

2. The Supplier (or as the case may be: Supplier's Personnel) may only access Buyer's systems upon and in accordance with the Buyer's access authorization. If access is granted to a specific individual, i.e., Supplier's Personnel, it is explicitly prohibited to transfer such access to another individual.

5.3 Physical and environmental security

The Supplier shall protect goods received or sent on behalf of the Buyer from theft, manipulation and destruction.

5.4 System acquisition, development and maintenance

The Supplier shall ensure that information involved in application services, passing over public networks shall be protected from fraudulent activity, unauthorized disclosure and modification.

5.5 Business continuity management

The Supplier shall ensure that information security is embedded into the business continuity plans.

6. Security requirements for IaaS or PaaS deliveries addressed to Telia Company Infrastructure or enterprise (Non Telia Private Cloud based)

6.1 Asset management

Data

1.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.

2.The Supplier shall guarantee that any processing of the Buyer's Data will be compliant with the Supplier Security Directive.

6.2 Access control

1.The Supplier shall not allow any access to the 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.

2.If the Buyer's Data is processed in a multi-tenant environment operated by the Supplier, the Supplier shall protect the Buyers Data from other tenants and unauthorized persons.

6.2.1 Access to the Buyers Data in the Supplier's or sub-contractor's system (such as server farm or cloud)

1.The Supplier shall have traceability in all Management Operations and be able to provide related Logs and evidence to the Buyer.

2.The Buyer shall authorize and approve all access to the Buyer's and the Buyer's customer Data.

3.The Supplier shall not extract information from the Buyers Data or the Buyer's customer Data unless explicitly approved by the Buyer, before executing the operation, including:

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.

6.2.2 Access to the Buyer's Data in the Buyer's system (On-Premises)

1. All remote access to the Buyers systems shall be authorized and approved by the Buyer.

2. The Supplier (or as the case may be: Supplier's Personnel) may only access Buyer's systems upon and in accordance with the Buyer's access authorization. If access is granted to a specific individual, i.e., Supplier's Personnel, it is explicitly prohibited to transfer such access to another individual.

6.3 Operations security

1. The Supplier shall have defined, documented and monitored procedures for administrative operations of computing environments where the Buyers Data and the Buyer's customer Data is processed.

2. The Supplier shall protect and store (for at least 6 months) relevant Log information, and on request, deliver monitoring data to the Buyer.

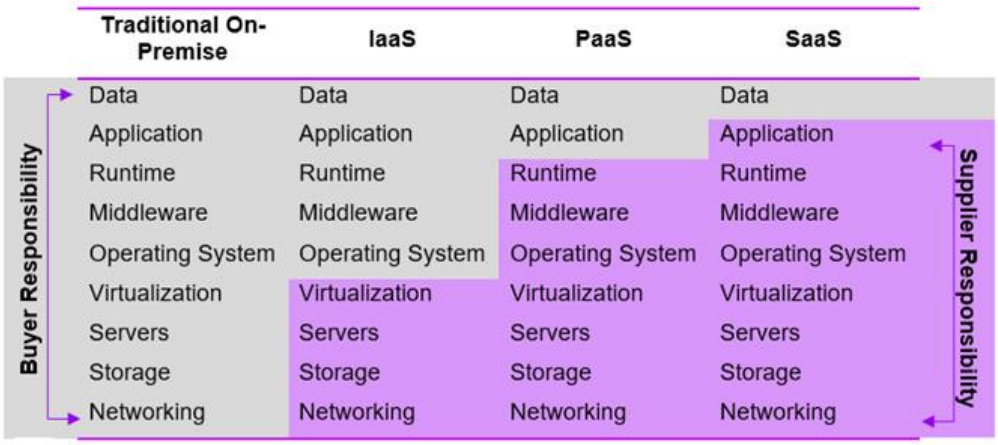
6.4 System acquisition, development and maintenance

1. The Supplier shall not use the Buyers data for testing purposes unless it is required by the Buyer.

2. The Supplier shall ensure that information involved in application services, passing over public networks shall be protected from fraudulent activity, unauthorized disclosure and modification.

6.5 Cloud Computing

1. Parties shall agree in Agreement upon shared responsibility model that clearly defines all elements of the technology stack under the Suppliers control, and what is Telia responsibility.



2. The Supplier shall ensure that all aspects of the shared responsibility model which the Supplier is responsible for, are regularly security tested using both automated and human in the loop testing methodologies. Relevant issues impacting the service provided and/or Buyer's data shall be communicated to Telia along with a relevant impact summary and mitigation plan.

3. The Supplier shall provide documentation that clearly demonstrates all cloud security capabilities in the Deliverables, including highlighting of all configurable options and their impacts for everything that is the responsibility of Telia to manage.

4. The Supplier shall ensure that user and super-user access control systems for the service seamlessly integrate with Telia's Identity and Access Management technologies using Single Sign On capabilities.

5. The Supplier shall ensure that any super-user or administrative user accounts given to the service will enforce strict Multifactor Authentication.

6. The Supplier shall ensure that all super-user or administrative user accounts are separated from standard user accounts within the service.

7. The service must support role-based access control for both user functions and operational functions, that is able to integrate with Telia's Identity & Access Management technologies.

8. The Supplier shall not permit access to any of Telia's data stored, processed, or otherwise within, the cloud service, by the Suppliers employees or third parties working on behalf of the Supplier.

9. The Supplier shall ensure, upon contract termination, that all Telia data is securely wiped and destroyed. The Supplier shall provide comprehensive process details on how this will occur prior deployment of Buyer's Data on the Cloud solution.

6.6 Business continuity management

The Supplier shall ensure that information security is embedded into the business continuity plans.

6.7 Compliance

1. The Supplier shall ensure that Telia data is restricted to the relevant geographical area and will not under any circumstances transferred outside that geographic area permitted under the Agreement.

2. 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.

7. Security requirements for ICT Hardware deliveries addressed to Telia Company customers

7.1 Risk Management

7.1.1 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.

7.2 Access control

1. The Supplier shall not allow any access to the 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.

2. If the Buyer's Data is processed in a multi-tenant environment operated by the Supplier, the Supplier shall protect the Buyers Data from other tenants and unauthorized persons.

7.3 Physical and environmental security

The Supplier shall protect goods received or sent on behalf of the Buyer from theft, manipulation and destruction.

7.4 System acquisition, development and maintenance

The Supplier shall ensure that information involved in application services, passing over public networks shall be protected from fraudulent activity, unauthorized disclosure and modification.

7.5 Personal Data processing

This section 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 are attached to the Agreement.

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. The Supplier shall appoint at least one person having appropriate Data Protection & Privacy competence, bearing ultimate responsibility for implementing the Data Protection measures under the Supplier Security Directive and who shall be the single point of contact for Buyer's data protection staff.

5. The Supplier shall never allow access to Buyer's data to any entity based in a third country if the processing includes Personal Data, unless expressly agreed in writing.

6. 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.

7. 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 Best Practices.

8. 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.

7.6 Compliance

1. The Supplier shall ensure that Telia data is restricted to the relevant geographical area and will not under any circumstances transferred outside that geographic area permitted under the Agreement.

2. 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.

SUPPLIER SECURITY DIRECTIVE - SUB-ANNEX SERVICES

1. Description

This document is a sub-annex to “Supplier Security Directive”, aiming to govern and describe specific terms related to deliveries based on professional services of different types; being those related or not to Information and Communication Technology (ICT) and Information Security (IS), whether the Supplier personnel will have or not access to Telia premises or leased premises; and describes the security requirements applicable to suppliers and other identified business partners to Telia. Additional security requirements may apply if agreed by involved parties.

2. Scope

The Services Sub-Annex of Supplier Security Directive applies when:

1.The Supplier will have unescorted access to Buyer’s premises, excluding external areas.

2.The Supplier will handle Buyer’s information processing equipment .

3.The Supplier will be involved or collaborate during any stage of the software development lifecycle of any Telia system or platform.

4.The Supplier will provide managed services supporting any Telia system or platform.

5.The Supplier will provide information security or physical security related services.

3. Common security requirements for all types of professional services deliveries

3.1 Access control

Access to the Buyer’s Data in the Buyer’s system (On-Premises)

The Supplier (or as the case may be: Supplier’s Personnel) may only access Buyer’s systems upon and in accordance with the Buyer’s access authorization. If access is granted to a specific individual, i.e., Supplier’s Personnel, it is explicitly prohibited to transfer such access to another individual.

4. Specific security requirements for ICT and/or security related services requiring physical access to Telia premises or leased premises

4.1 Risk Management

4.1.1 Security risk management

1. The Supplier shall have an established security risk management framework in accordance with Industry Best Practice, such as ISO/IEC 27005 or ISO 31000. The security risk management framework shall:

a) Identify security risks related to Confidentiality, Integrity and Availability.

b) Analyze security risks based on consequences and likelihood.

c) Evaluate security risks against acceptance criteria.

d) Define security risk treatment measures which is appropriated to the risk.

2. The Supplier shall be able to provide evidence on assessment of security risks and measures taken to mitigate those risks according to acceptance criteria set by Supplier related to the Deliverables.

4.1.2 Security risk management for Personal Data

1. The Supplier shall have documented processes and routines for handling risks when processing Personal Data on behalf of Buyer.

2. The Supplier shall periodically assess the risks related to information systems and processing, storing and transmitting Personal Data.

4.2 Information security policies

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.

4.3 Organization of information security

1.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.

2. The Supplier shall secure resources and necessary competence to maintain its ISMS.

4.4 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 have a disciplinary process which covers information security related misconduct.

3. 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) Responsibility for information security relating to the Buyer's confidential, secret or Personal Data (such as protecting customer's privacy-related information, GDPR obligations and reporting actual and suspected Security Incidents).

4. The Supplier is responsible for Supplier's Personnel having access to Buyer's information, data, systems and/or premises. In order to secure traceability of Suppliers personnel, Supplier shall, at the request of the Buyer, provide, first name, last name (surname), date of birth, Social Security number, Passport or national ID number of Supplier's Personnel.

4.5 Asset management

4.5.1 Physical Assets

The Supplier shall label, treat and protect assets according to a Telia pre-defined classification specified in the "Supplier Security Directives - Generic Requirements" section 6, following Industry Best Practices (including, but not limited to, information, removable media storage, disposal and physical transfer).

4.5.2 Data

1. 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.

2. The Supplier shall guarantee that any processing of the Buyer's Data will be compliant with the Supplier Security Directive.

4.6 **Access control**

The Supplier shall have a formal and documented user registration and de-registration process implemented to enable assignment of access rights.

4.6.1 Access to the Buyers Data in the Supplier's or sub-contractor's system (such as server farm or cloud)

1. The Supplier shall have traceability in all Management Operations and be able to provide related Logs and evidence to the Buyer.

2. The Buyer shall authorize and approve all access to the Buyer's and the Buyer's customer Data.

3. The Supplier shall not extract information from the Buyers Data or the Buyer's customer Data unless explicitly approved by the Buyer, before executing the operation, including:

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.

4.6.2 Access to the Buyer's Data in the Buyer's system (On-Premises)

All remote access to the Buyers systems shall be authorized and approved by the Buyer.

4.7 **Physical and environmental security**

The Supplier shall protect goods received or sent on behalf of the Buyer from theft, manipulation and destruction.

4.7.1 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 times 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.

4.8 Operations security

1. The Supplier shall manage vulnerabilities of all relevant technologies such as operating systems, databases, applications proactively and in a timely manner.

2. The Supplier shall establish security baselines (hardening) for all relevant technologies such as operating systems, databases, applications.

3. 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.

4.9 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 test security functionality during development in a controlled environment.

4. The Supplier shall not use the Buyers data for testing purposes unless it is required by the Buyer.

5. The Supplier shall ensure that information involved in application services, passing over public networks shall be protected from fraudulent activity, unauthorized disclosure and modification.

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

4.10 Security Incident management

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

4.11 Business continuity management

1. The Supplier shall ensure that information security is embedded into the business continuity plans.

2. The Supplier shall periodically, at least annually (unless otherwise agreed), assess the efficiency of its business continuity management including disaster recovery, and compliance with availability requirements.

5. Specific security requirements for ICT and/or security related services not requiring physical access to Telia premises or leased premises

5.1 Risk Management

5.1.1 Security risk management

1.The Supplier shall have an established security risk management framework in accordance with Industry Best Practice, such as ISO/IEC 27005 or ISO 31000. The security risk management framework shall:

a) Identify security risks related to Confidentiality, Integrity and Availability.

b) Analyze security risks based on consequences and likelihood.

c) Evaluate security risks against acceptance criteria.

d) Define security risk treatment measures which is appropriated to the risk.

2.The Supplier shall be able to provide evidence on assessment of security risks and measures taken to mitigate those risks according to acceptance criteria set by Supplier related to the Deliverables.

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

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 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.

2. The Supplier shall secure resources and necessary competence to maintain its ISMS.

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 have a disciplinary process which covers information security related misconduct.

3. 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) Responsibility for information security relating to the Buyer's confidential, secret or Personal Data (such as protecting customer's privacy-related information, GDPR obligations and reporting actual and suspected Security Incidents).

4. The Supplier is responsible for Supplier's Personnel having access to Buyer's information, data, systems and/or premises. In order to secure traceability of Suppliers personnel, Supplier shall, at the request of the Buyer, provide, first name, last name (surname), date of birth, Social Security number, Passport or national ID number of Supplier's Personnel.

5.5 Asset management

Data

1.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.

2.The Supplier shall guarantee that any processing of the Buyer's Data will be compliant with the Supplier Security Directive.

5.6 Access control

1. The Supplier shall have a formal and documented user registration and de-registration process implemented to enable assignment of access rights.

2. The Supplier shall not allow any access to the 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.

3. The Supplier shall use strong authentication (multi-factor) for remote access users and users connecting from any untrusted network.

4. If the Buyer's Data is processed in a multi-tenant environment operated by the Supplier, the Supplier shall protect the Buyers Data from other tenants and unauthorized persons.

5.6.1 Access to the Buyers Data in the Supplier's or sub-contractor's system (such as server farm or cloud)

1.The Supplier shall have traceability in all Management Operations and be able to provide related Logs and evidence to the Buyer.

2.The Buyer shall authorize and approve all access to the Buyer's and the Buyer's customer Data.

3.The Supplier shall not extract information from the Buyers Data or the Buyer's customer Data unless explicitly approved by the Buyer, before executing the operation, including:

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.

5.6.2 Access to the Buyer's Data in the Buyer's system (On-Premises)

All remote access to the Buyers systems shall be authorized and approved by the Buyer.

5.7 Encryption

The Supplier shall protect and rotate encryption keys in line with the sensitivity of the information they are being used to protect.

5.8 Operations security

1. The Supplier shall have a vulnerability management process in place which includes scanning, penetration testing and patching.

2. The Supplier shall manage vulnerabilities of all relevant technologies such as operating systems, databases, applications proactively and in a timely manner.

3. The Supplier shall establish security baselines (hardening) for all relevant technologies such as operating systems, databases, applications.

4. 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.

5. The Supplier shall ensure that all development, test and production environments are segregated.

6. The Supplier shall have defined, documented and monitored procedures for administrative operations of computing environments where the Buyers Data and the Buyer's customer Data is processed.

7. The Supplier shall protect and store (for at least 6 months) relevant Log information, and on request, deliver monitoring data to the Buyer.

5.9 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.

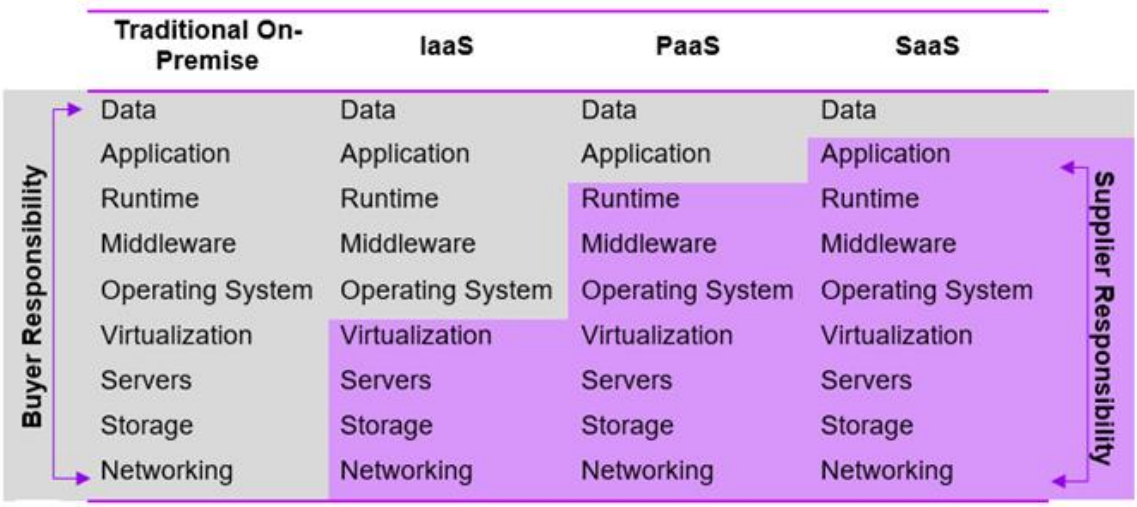
5. The Supplier shall not use the Buyers data for testing purposes unless it is required by the Buyer.

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.

5.10 Cloud Computing Security

1. Parties shall agree in Agreement upon shared responsibility model that clearly defines all elements of the technology stack under the Suppliers control, and what is Telia responsibility.



2. The Supplier shall ensure that all aspects of the shared responsibility model which the Supplier is responsible for, are regularly security tested using both automated and human in the loop testing methodologies. Relevant issues impacting the service provided and/or Buyer's data shall be communicated to Telia along with a relevant impact summary and mitigation plan.

3. The Supplier shall provide documentation that clearly demonstrates all cloud security capabilities in the Deliverables, including highlighting of all configurable options and their impacts for everything that is the responsibility of Telia to manage.

4. The Supplier shall ensure that user and super-user access control systems for the service seamlessly integrate with Telia's Identity and Access Management technologies using Single Sign On capabilities.

5. The Supplier shall ensure that any super-user or administrative user accounts given to the service will enforce strict Multifactor Authentication.

6. The Supplier shall ensure that all super-user or administrative user accounts are separated from standard user accounts within the service.

7. The service must support role-based access control for both user functions and operational functions, that is able to integrate with Telia's Identity & Access Management technologies.

8. The Supplier shall not permit access to any of Telia's data stored, processed, or otherwise within, the cloud service, by the Suppliers employees or third parties working on behalf of the Supplier.

9. The Supplier shall provide onboarding processes, methodology, and technology, that ensures strict data security for all data transfers and service initialization.

10. The Supplier shall ensure, upon contract termination, that all Telia data is securely wiped and destroyed. The Supplier shall provide comprehensive process details on how this will occur prior deployment of Buyer's Data on the Cloud solution.

5.11 Personal Data processing

This section 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 are attached to the Agreement.

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. The Supplier shall appoint at least one person having appropriate Data Protection & Privacy competence, bearing ultimate responsibility for implementing the Data Protection measures under the Supplier Security Directive and who shall be the single point of contact for Buyer's data protection staff.

5. The Supplier shall never allow access to Buyer's data to any entity based in a third country if the processing includes Personal Data, unless expressly agreed in writing.

6. 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.

7. 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 Best Practices.

8. 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.

5.12 Security Incident management

1. 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) Experience summary including root cause analysis.

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

5.13 Business continuity management

1. The Supplier shall ensure that information security is embedded into the business continuity plans.

2. The Supplier shall periodically, at least annually (unless otherwise agreed), assess the efficiency of its business continuity management including disaster recovery, and compliance with availability requirements.

5.14 Compliance

1. The Supplier shall ensure that Telia data is restricted to the relevant geographical area and will not under any circumstances transferred outside that geographic area permitted under the Agreement.

2. 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. Specific security requirements for non-ICT and/or security related services requiring physical access to Telia premises or leased premises

6.1 Physical and environmental security

The Supplier shall protect goods received or sent on behalf of the Buyer from theft, manipulation and destruction.

6.1.1 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:

a) The Supplier shall follow local regulations (such as regulations for "restricted areas") for Buyer's premises when performing the assignments under the Agreement.

b) Supplier Personnel shall carry ID card or a visitor's badge visible at all times when working within the Buyer's premises.

c) 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.

d) Keys or key cards shall be personally signed for by Supplier Personnel and shall be handled according to the written rules given upon receipt.

e) Loss of the Buyer's key or key card shall be reported without delay to the Buyer.

f) Photograph or video recording within Buyer's premises without permission is strictly prohibited.

g) Buyer's goods shall not be removed from Buyer's premises without permission.

h) Supplier Personnel shall not allow unauthorized persons access to the premises.

7. Specific security requirements for non-ICT and/or security related services not requiring physical access to Telia premises or leased premises

7.1 Risk Management

7.1.1 Security risk management

The Supplier shall be able to provide evidence on assessment of security risks and measures taken to mitigate those risks according to acceptance criteria set by Supplier related to the Deliverables.

7.1.2 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.

7.2 Organization of information security

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.

7.3 **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 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) Responsibility for information security relating to the Buyer's confidential, secret or Personal Data (such as protecting customer's privacy-related information, GDPR obligations and reporting actual and suspected Security Incidents).

7.4 **Asset management**

7.4.1 Physical Assets

The Supplier shall label, treat and protect assets according to a Telia pre-defined classification specified in "Supplier Security Directives - Generic Requirements" section 6 following Industry Best Practices (including, but not limited to, information, removable media storage, disposal and physical transfer).

7.4.2 Data

1.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.

2.The Supplier shall guarantee that any processing of the Buyer's Data will be compliant with the Supplier Security Directive.

7.5 Access control

1.The Supplier shall not allow any access to the 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.

2.The Supplier shall use strong authentication (multi-factor) for remote access users and users connecting from any untrusted network.

3.If the Buyer's Data is processed in a multi-tenant environment operated by the Supplier, the Supplier shall protect the Buyers Data from other tenants and unauthorized persons.

7.5.1 Access to the Buyers Data in the Supplier's or sub-contractor's system (such as server farm or cloud)

1.The Buyer shall authorize and approve all access to the Buyer's and the Buyer's customer Data.

2.The Supplier shall not extract information from the Buyers Data or the Buyer's customer Data unless explicitly approved by the Buyer, before executing the operation, including:

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.

7.5.2 Access to the Buyer's Data in the Buyer's system (On-Premises)

All remote access to the Buyers systems shall be authorized and approved by the Buyer.

7.6 Physical and environmental security

The Supplier shall protect goods received or sent on behalf of the Buyer from theft, manipulation and destruction.

7.7 Operations security

1. The Supplier shall have an established change management process in place.

2. The Supplier shall manage vulnerabilities of all relevant technologies such as operating systems, databases, applications proactively and in a timely manner.

3. The Supplier shall establish security baselines (hardening) for all relevant technologies such as operating systems, databases, applications.

4. The Supplier shall have defined, documented and monitored procedures for administrative operations of computing environments where the Buyers Data and the Buyer's customer Data is processed.

5. The Supplier shall protect and store (for at least 6 months) relevant Log information, and on request, deliver monitoring data to the Buyer.

7.8 Personal Data processing

This section 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 are attached to the Agreement.

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. The Supplier shall appoint at least one person having appropriate Data Protection & Privacy competence, bearing ultimate responsibility for implementing the Data Protection measures under the Supplier Security Directive and who shall be the single point of contact for Buyer's data protection staff.

5. The Supplier shall never allow access to Buyer's data to any entity based in a third country if the processing includes Personal Data, unless expressly agreed in writing.

6. 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.

7. 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 Best Practices.

8. 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.

7.9 Security Incident management

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) Experience summary including root cause analysis.

7.10 Compliance

1. The Supplier shall ensure that Telia data is restricted to the relevant geographical area and will not under any circumstances transferred outside that geographic area permitted under the Agreement.

2. 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.