A1 Digital Information Security Requirements for Suppliers

1. Responsibility

The Contractor shall establish and – if requested by A1 Digital – provide evidence of effectiveness of the following information security requirements defining security measures for protecting personally identifiable information (PII) and confidential company data (hereinafter "PII and Confidential Data") processed on behalf of A1 Digital.

Systems and applications used by the Contractor for storing and processing of PII and Confidential data on behalf of A1 Digital must meet minimum state-of-the-art requirements to protect them against threats such as data theft, data manipulation, sabotage, denial of service attacks, and many more. In case that state-of-the-art methods cannot be used, the Contractor shall apply alternative measures to ensure the same or a higher level of protection. The Contractor shall immediately inform A1 Digital of any deviations from the security measures defined in this document by means of a written declaration of compliance with A1 Digital Information Security Requirements.

2. Warranty

The Contractor warrants that it maintains and shall continue to maintain appropriate and sufficient technical and organizational security measures to protect PII and Confidential Data against accidental, unlawful destruction or accidental loss, damage, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing. The necessary technical and organizational measures, which the Contractor must establish when processing PII and Confidential data on behalf of A1 Digital, are described below.

3. Transparency

If requested by A1 Digital, the Contractor must inform A1 Digital about all organizational and technical measures which it is using to fulfil the requirements of A1 Digital. Alternatively, the Contractor may provide information about valid security certifications it is holding, such as (to the extent applicable) ISO 27001, ISO 27018, ISAE 3402, SSAE 16, BSI C5, CSA (Cloud Security Alliance) STAR Certification, CSA (Cloud Security Alliance) STAR Self-Assessment. In this case, the Contractor must provide A1 Digital with detailed information about scope, applicability and risk acceptance of these certifications.

4. Security measures

The security measures defined in this section are applicable based on the service type that the Contractor provides to A1 Digital:

Application/Platform: A1 Digital acquires an IT system provided by the Contractor to process data.	**Examples**: - IT systems hosted/operated by the Contractor - Cloud services	**Measures:** All
Software: A1 Digital acquires a software product from a Contractor to run it on A1 Digital systems (no system operation by the Contractor). Contracted software development also falls under this type.	**Examples:** - Software license, Contractor only provides software support (e.g. updates, troubleshooting) - Software developers who create code or whole applications for A1 Digital.	**Measures:** v) Software development w) Software or systems quality criteria for security
Operational Support: A1 Digital acquires operational or maintenance services requiring system access by the Contractor.	**Examples:** Contractor provides IT support services on A1 Digital systems, e.g. administration of configuration, user management, maintenance of clients (laptops, mobile phones, IoT devices, etc.), etc.	**Measures:** b) Security of Communications and Networks c) Policy e) HR Processes f) Awareness and Training h) Supplier Management i) Security Incident Management j) Access Control k) User Management l) Cryptography m) Malware Protection q) Patching r) Hardening
Consulting: This service type bundles all consulting services acquired by A1 Digital, including IT and project consulting, where externals have access to PII and Confidential Data of A1 Digital.	**Examples:** Contractor provides consulting services to A1 Digital and has access to or is provided PII and Confidential Data of A1 Digital	**Measures:** b) Security of Communications and Networks c) Policy e) HR Processes f) Awareness and Training h) Supplier Management i) Security Incident Management j) Access Control k) User Management l) Cryptography

		m) Malware Protection p) Logging
Hardware: A1 Digital acquires an off-the-shelf IT hardware product from the Contractor.	**Examples:** IT hardware processing data of A1 Digital or its customers (e.g. IoT devices, smart meters, etc.).	w) Software or systems quality criteria for security

a) Multi-client capability, Separation of Data

The Contractor shall have appropriate measures to keep PII and Confidential Data of A1 Digital logically separated from data processed on behalf of any other third party in place.

b) Security of Communications and Networks

The Contractor shall have appropriate technical and organizational measures to safeguard the security of any electronic communication networks or services provided to A1 Digital or utilized to transfer or transmit A1 Digital data in place.

This includes, but is not limited to, measures designed

- to ensure the secrecy of communications,
- to prevent unlawful surveillance or interception of communications and
- to prevent unauthorized access to any computer or system, thus guaranteeing the security of the communications.

The Contractor must have an overall network protection strategy with appropriate security components (e.g. firewalls, internet proxy, intrusion prevention systems, zone segmentation, etc.) defined. The Contractor must have operating procedures to ensure effectiveness of the implemented network security measures established.

c) Policy

The Contractor must have internal behavioral rules and procedures to address and ensure its security measures for protecting PII and Confidential Data of A1 Digital defined. For this purpose, the Contractor must have appropriate policies, guidelines or service instructions on information security and data protection published/made available to its internal and external employees. All relevant information security policies should be approved by the management of the Contractor. Copies of security policies and operating procedures must be retained for a specified, documented period on replacement (including updating).

d) Security Organization and Responsibilities

The Contractor must have all necessary responsibilities (e.g. CISO, operational security, audit, etc.) and tasks to ensure information security in its organization defined. Each defined security task must be assigned to an organizational unit responsible for it.

e) HR Processes

The Contractor must have processes for security background checks of employees at onboarding and exit established. The minimum requirements are an identity check and obtaining a current police clearance certificate.

f) Contractual requirements and Training

The Contractor must have valid confidentiality and data processing agreements with all parties having access to PII and Confidential Data of A1 Digital signed and must provide regular training or instructions in the correct and responsible handling of information and data, especially PII and Confidential Data.

Administrators with privileged access rights and persons whose main task is processing PII and Confidential Data must regularly receive specialized training.

g) Information Asset Management

The Contractor must have an inventory of all information assets and IT assets, especially containing all IT assets where PII and Confidential Data is stored or processed, established.

Temporary files and documents containing PII and Confidential Data must be erased or destroyed within a specified, documented period.

The creation of hardcopy material displaying PII and Confidential Data must be restricted and securely destroyed after use.

The Contractor must not use portable physical media and portable devices that do not permit encryption to process PII and Confidential Data, except where it is unavoidable, and any use of such portable media and devices should be documented. Any storage media containing PII and Confidential Data of A1 Digital leaving the Contractor’s premises must be subject to an authorization procedure and must have access control measures in place (e.g. encryption).

h) Supplier Management (security and privacy in contracts)

If the Contractor is using subcontractors for storing or processing PII and Confidential Data on behalf of A1 Digital, it must obtain a written approval for this from A1 Digital prior to engaging the subcontractor.

The Contractor must contractually delegate all privacy and security requirements of A1 Digital to its subcontractors.

The Contractor must regularly ensure that its subcontractors fulfil the privacy and security requirements of A1 Digital. The Contractor must provide A1 Digital with evidence of its supplier security evaluations upon request.

i) Security Incident Management

The Contractor must have a process for dealing with security incidents defined and implemented. This process must describe at least the following aspects: Reporting system for incidents (e.g. e-mail address, telephone number, website, etc.), defined procedures and responsibilities for the whole incident management and response process.

The Contractor must inform A1 Digital immediately about any security incident concerning PII and Confidential Data, which it stores or processes on behalf of A1 Digital.

The Contractor must inform A1 Digital immediately about legally binding disclosure requests by law enforcement authorities, unless such communication is explicitly prohibited by the authority. In case of a disclosure, the Contractor must provide A1 Digital with records of which data was disclosed to whom at what time.

j) Access Control

The Contractor must define and implement appropriate methods for user authentication (password, biometry, two-factor authentication) und user rights management.

The authentication method must be implemented on each system, which is involved in storing and processing PII and Confidential Data on behalf of A1 Digital. Remote access via the internet or other unsecured networks must be secured by two-factor authentication.

The granularity of access rights must allow sufficient protection of PII and Confidential Data against unauthorized access, alternation or disclosure of such data. Passwords must be encrypted with state-of-the-art technology in all stages of storage and transport.

k) User Management

The Contractor must have the main user management processes for each application in place: add user, change rights, delete user, check business need, reset password.

Granting of access rights must be based on "business need" principle and should assure that PII and Confidential Data is correctly protected against unauthorized access, alteration or disclosure. Shared user accounts must not be allowed access to PII and Confidential Data of A1 Digital.

All accounts (for employees, administrator and external workforce) must be audited and revalidated at least quarterly. De-activated or expired user IDs must not be granted to other individuals.

l) Cryptography

The Contractor must have rules for encryption of storage and transfer of PII and Confidential Data in place. The Contractor must ensure that PII and Confidential Data of A1 Digital is encrypted whenever transferred over public networks.

m) Malware protection

The Contractor must protect endpoints (PCs, notebooks, mobile phones, etc.), mail traffic, web traffic and servers against malware. The Contractor must implement appropriate malware-protection software. The Contractor must ensure that the malware-protection software is up-to-date and equipped with the most current malware signatures.

n) Change Management

The Contractor must establish a formal change management process for all changes in the productive environments handling PII and Confidential Data of A1 Digital. All changes and implementations of systems or applications must be carried out according to the documented change process. The process must ensure that adequate security tests are being performed prior to performing a change in the productive environment. The Contractor must monitor the effectiveness of its change management process regularly and provide A1 Digital with evidence of its evaluation upon request.

o) Backup

The Contractor must have a backup strategy and a process to monitor backup operations established. The backup strategy must define which data must be backed up, how long the backups must be retained and on which systems/sites the backups must be kept. The integrity of backups must be tested regularly by restoring a complete database from a selected backup onto a test system and verifying the data. All data restoration efforts must be adequately logged (responsible person, description of the data, list of data sets/files that were restored).

Any data going into tape backups must be encrypted. Tapes must be securely destroyed when retired.

p) Logging

The Contractor must have a log management concept established, defining which transactions and activities are being logged (e.g. accessing and changing PII and Confidential Data), how long these logs must be retained, how the logs will be regularly monitored and who has access to the log files.

q) Patching

The Contractor must have a patch management process established, ensuring that all systems are being patched (all necessary security update are installed) within defined timeframes.

r) Hardening

The Contractor must have a process in place to securely configure all its systems and applications used for storing or processing PII and Confidential Data on behalf of A1 Digital. The process must ensure that all not-needed ports, interfaces and services in all systems involved in storing and processing of PII and Confidential Data on behalf of A1 Digital are being disabled. The process must also ensure that all default passwords are being changed. The Contractor must provide A1 Digital with a documentation of its hardening measures on its systems upon request.

s) Vulnerability and Web application scans

The Contractor must have a process in place to regularly (at least monthly) check if all its systems are free of vulnerabilities (such as missing patches, insecure configuration or weak cryptography). The process must further ensure that in case that vulnerable systems are identified all necessary measures to close the vulnerabilities are taken within a reasonable time.

t) Pentest

The Contractor must organize regular, adequate security tests/audits of systems storing or processing PII and Confidential Data on behalf of A1 Digital. Penetration tests are considered adequate security tests. The Contractor must provide A1 Digital with test results, if requested.

u) Separation production/development

The Contractor must separate production and test system with adequate technical measures (e.g. firewalls). The Contractor must ensure that no production data of A1 Digital is used in test systems. Test users of the Contractor must not have any access to production systems storing or transferring data of A1 Digital.

v) Software development

(1) The Contractor shall have policies, guidelines and instructions of technical and organizational safeguards for the proper development of software or systems, including middleware, databases, operating systems, network components and all other parts, in place. The policies and instructions must describe at least the following aspects:

- Security in software development methods in compliance with well-known security standards (e.g. OWASP for web applications and OWASP Secure Coding Practices Checklist). At least the following aspects must be addressed: secure (encrypted) device communication, secure end-user communication, state-of-the-art access control and user management, secure Web-Browser.
- Security of the development environment (e.g. separate development/test/production environments).
- Programming policies for each programming language used (e.g. regarding buffer overflows, hiding internal object references towards users, etc.).
- Security in version control.

(2) If the development of the software or system (or parts thereof) is outsourced regarding the design, development, test and/or provision of source code of software or systems, the following aspects must be contractually agreed between the Contractor and its sub-suppliers:

- Requirements for a secure software development process (especially design, development and testing).
- Acceptance testing of the quality of the services rendered, according to the agreed-upon functional and non-functional requirements.
- Provision of evidence demonstrating that adequate testing was carried out by the sub-suppliers.

w) Software or systems quality criteria for security

The following features must be implemented in each release or new version of software delivered to A1 Digital:

- Each release or new version of software or systems must be tested for quality and security before delivery. The chosen test method must guarantee that delivered software or systems are malware-free and have no known vulnerabilities. Test protocols must be provided to A1 Digital upon request.
- In case of new vulnerabilities being found in software, systems or underlying software parts or components, which are delivered to A1 Digital by the Contractor, the Contractor is obliged to inform A1 Digital immediately about it and provide necessary security updates within a reasonable time.
- Any unspecified access method (back door) to access software or systems, independent for whichever reason, is absolutely forbidden.

x) Physical security, Admission control

The Contractor must ensure that all systems and applications used for storing and processing PII and Confidential Data of A1 Digital are located in an appropriately equipped data center. The data center must provide appropriate environmental controls (e.g. climate control, uninterrupted power supply, fire suppression systems, etc.), an appropriate physical construction and appropriate access controls to ensure availability and restricted access to systems and applications.

The data center must provide controlled building access and secure access to specific areas through the administration of access cards, Pin codes, biometric sensors or other adequate methods. There must be a formal procedure in place to add, delete and modify access rights and to review access attempts/successful access.

y) Business Continuity Management

The Contractor must have at least the following aspects of business continuity management defined and implemented: Appropriate redundancy of IT systems to fulfil A1 Digital

availability requirements, defined responsibilities for crisis management, process and procedures for dealing with a crisis.