Informationssicherheitsanforderungen für Lieferanten

1. Verantwortung

Der Lieferant muss die folgenden Informationssicherheitsanforderungen und Sicherheitsmaßnahmen zum Schutz von persönlich identifizierbaren Informationen (PII) und vertraulichen Unternehmensdaten (nachfolgend "PII und vertrauliche Daten"), die im Auftrag von A1 Digital verarbeitet werden, sicherstellen, und falls von A1 Digital angefordert einen Nachweis der Wirksamkeit vorlegen.

Systeme und Applikationen, die der Lieferant nutzt, um Personen-/Vertrauliche Daten für A1 Digital zu speichern oder zu verarbeiten, müssen zumindest über dem Stand der Technik entsprechende Sicherheitsmaßnahmen verfügen um sie gegen Gefahren, wie z.B. Datendiebstahl, Datenmanipulation, Sabotage, Denial-of-Service-Angriffe, etc., zu schützen. Im Falle, dass dem Stand der Technik entsprechende Maßnahmen nicht verwendet werden können, muss der Lieferant kompensierende Maßnahmen implementieren, um zumindest dasselbe Schutzniveau zu erreichen. Der Lieferant hat A1 Digital unverzüglich über alle Abweichungen von in diesem Dokument definierten Sicherheitsmaßnahmen in einer schriftliche Konformitätserklärung über Einhaltung der A1 Digital Informationssicherheits-anforderungen zu informieren.

2. Garantie

Der Lieferant garantiert, dass er angemessene technische und organisatorische Maßnahmen unterhält und auch weiterhin unterhalten wird, welche geeignet sind Personen-/Vertrauliche Daten vor unbeabsichtigtem Verlust, nicht autorisierter Zerstörung, nicht autorisierter Änderung, nicht autorisierter Veröffentlichung oder Zugriff – insbesondere bei Übertragungen über öffentliche Netzwerke – und anderen unrechtmäßigen Arten der Verarbeitung zu schützen.

Die notwendigen organisatorischen und technischen Sicherheitsmaßnahmen, die der Lieferant implementieren muss, wenn er Personen-/Vertrauliche Daten von A1 Digital verarbeitet, sind in der Folge beschrieben.

3. Transparenz

Der Lieferant muss A1 Digital auf Nachfrage über alle organisatorischen und technischen Maßnahmen, welche er implementiert hat, um die Anforderungen von A1 Digital zu erfüllen, informieren.

Alternativ kann der Lieferant A1 Digital seine organisatorischen und technischen Maßnahmen über gültige, unabhängig Sicherheitszertifizierungen nachweisen, die er innehat. Relevante Sicherheitszertifizierungen sind z.B. (soweit anwendbar): ISO 27001,

ISO 27018, ISAE 3402, SSAE 16, BSI C5, CSA (Cloud Security Alliance) STAR Certification, CSA STAR Self-Assessment, etc.

Falls der Lieferant seine Maßnahmen über eine Sicherheitszertifizierungen nachweist, muss er A1 Digital detaillierte Information über den Umfang der Zertifizierung, Anwendbarkeit und ggf. Risikoakzeptanz von Abweichungen zukommen lassen.

4. Sicherheitsmaßnahmen

Die Sicherheitsmaßnahmen in diesem Abschnitt sind anwendbar basierend auf der Art der Services welches der Lieferant für A1 Digital erbringt:

Applikation/Plattform: A1 Digital erhält ein IT System, welches vom Lieferanten zur Verfügung gestellt wird, um seine Daten zu verarbeiten.	**Beispiele**: - IT Systeme gehostet oder betrieben durch den Lieferanten - Cloud-Services	**Maßnahmen:** Alle
Software: A1 Digital erhält ein Softwareprodukt von einem Lieferanten und betreibt es auf seinen eigenen Systemen (kein Systembetrieb durch den Lieferanten). Softwareentwicklung im Auftrag von A1 Digital fällt ebenfalls unter diesen Typ.	**Beispiele:** - Softwarelizenz – Lieferant liefert nur Software-Support (z.B. Updates, Problemlösung) - Softwareentwickler, die Code oder gesamte Applikationen für A1 Digital entwickeln	**Maßnahmen:** v) Softwareentwicklung w) Software- oder Systemqualitätskriterien für Sicherheit
Operational Support: A1 Digital erhält Betriebsführungs- oder Wartungsservices, welche Systemzugriff benötigen, von einem Lieferanten	**Beispiele:** Lieferant liefert IT Support Dienstleistungen auf A1 Digital Systemen, z.B. Administration, Konfiguration, Benutzerverwaltung, Verwaltung von Endgeräten (Laptops, Handys, IoT-Geräte, etc.)	**Maßnahmen:** b) Sicherheit in Kommunikation und Netzwerken c) Politik e) Personalprozesse f) Vertragliche Anforderungen und Training h) Lieferantenmanagement i) Management von Sicherheitsvorfällen j) Zugriffskontrolle k) Benutzerverwaltung l) Kryptografie m) Schutz vor

		Schadsoftware q) Management von Softwareupdates (Patches) r) Systemhärtung
Consulting: In diesem Typ sind alle Beratungsdienstleistungen zusammengefasst, welche von A1 Digital konsumiert werden. Dies enthält IT und Projektberatung, wo Dritte Zugriff auf Personen-/Vertrauliche Daten von A1 Digital erhalten.	**Beispiele:** Lieferant liefert Beratungsdienstleistungen an A1 Digital und erhält hierbei Zugriff auf Personen-/Vertrauliche Daten von A1 Digital.	**Maßnahmen:** b) Sicherheit in Kommunikation und Netzwerken c) Politik e) Personalprozesse f) Vertragliche Anforderungen und Training h) Lieferantenmanagement i) Management von Sicherheitsvorfällen j) Zugriffskontrolle k) Benutzerverwaltung l) Kryptografie m) Schutz vor Schadsoftware p) Log Management
Hardware: A1 Digital erhält IT-Hardware von der Stange vom Lieferanten.	**Beispiele:** IT-Hardware, auf welcher Daten von A1 Digital oder seinen Kunden verarbeitet wird (z.B. IoT-Geräte, Smart Meter, etc.)	w) Software- oder Systemqualitätskriterien für Sicherheit

a) Multi-Client-Funktionalität, Datentrennung

Der Lieferant muss angemessene technische Maßnahmen implementiert haben, um Personen-/Vertrauliche Daten von A1 Digital logisch von Daten, die er für Dritte verarbeitet, zu trennen.

b) Sicherheit in Kommunikation und Netzwerken

Der Lieferant muss angemessene technische und organisatorische Maßnahmen implementiert haben, um die Sicherheit jedes elektronischen Kommunikationsnetzwerks oder -services, welches A1 Digital zur Verfügung gestellt wird oder zur Übermittlung von Daten von A1 Digital verwendet wird, sicher zu stellen.

Das beinhaltet zumindest Maßnahmen

- zum Schutz der Vertraulichkeit von Nachrichten,

- zur Verhinderung von unberechtigter Überwachung oder Abfangen von Nachrichten und
- zur Verhinderung von unberechtigtem Zugriff auf Computer oder Systeme, welche die Sicherheit der Kommunikation negativ beeinflussen können.

Der Lieferant muss eine umfassende Netzwerksicherheitsstrategie verfolgen, welche angemessene Sicherheitskomponenten vorsieht (z.B. Firewalls, Internetproxys, Intrusion-Prevention-Systeme, Zonen-Segmentierung, etc.). Der Lieferant muss weiters angemessene, operative Prozesse implementiert haben, um die Effektivität seiner Netzwerksicherheitsmaßnahmen sicherstellen zu können.

c) Politik

Der Lieferant muss interne Verhaltensregeln und Prozesse implementiert haben um Sicherheitsmaßnahmen zum Schutz von Personen-/Vertraulichen Daten von A1 Digital zu adressieren. Zu diesem Zweck muss der Lieferant angemessene Politiken, Richtlinien, Servicebeschreibungen oder andere Dokumente, die Informationssicherheit und Datenschutz regeln, seinen internen und externen Mitarbeitern veröffentlicht haben. Alle relevanten Informationssicherheitsvorgaben müssen von der obersten Leitung der Organisation des Lieferanten frei gegeben sein. Versionen der Informationssicherheitsvorgaben müssen für einen spezifizierten, dokumentierten Zeitraum, ab dem Moment wo sie nicht mehr gültig sind, aufbewahrt werden.

d) Security-Organisation und Verantwortlichkeiten

Der Lieferant muss alle notwendigen Verantwortlichkeiten (z.B. CISO, operationale Security, Audit, etc.) und Aufgaben, um Informationssicherheit in seiner Organisation sicherzustellen, zugewiesen haben. Jede definierte Security-Aufgabe muss einer Rolle oder Organisationseinheit zugeordnet sein, welche für die Durchführung verantwortlich ist.

e) Personalprozesse

Der Lieferant muss Sicherheitsüberprüfungen von Mitarbeiten, die neu in die Organisation kommen, implementiert haben. Eine Sicherheitsüberprüfung muss zumindest eine Prüfung der Identität der Person sowie eine Prüfung auf Vorstrafen beinhalten.

f) Vertragliche Anforderungen und Training

Der Lieferant muss gültige Vertraulichkeitsvereinbarungen und Datenverarbeitungsvereinbarungen mit allen Parteien, welche Zugriff auf Personen-/Vertrauliche Daten von A1 Digital haben, vereinbart haben.

Der Lieferant muss regelmäßig Trainings oder Anweisungen zur korrekten und verantwortungsbewussten Handhabung von Informationen und Daten der Parteien durchführen, insbesondere mit Bezug auf Personen-/Vertrauliche Daten.

Administratoren mit privilegierten Zugriffsrechten und Personen, deren Hauptaufgabe es ist mit Personen-/Vertraulichen Daten zu arbeiten, müssen regelmäßig spezialisierte Trainings erhalten.

g) Inventarisierung von Informationen (Information Asset Management)

Der Lieferant muss ein Inventar über alle relevanten Informationen und IT-Assets führen, dieses sollte insbesondere alle IT-Assets welche Personen-/Vertrauliche Daten verarbeiten beinhalten.

Temporäre Dateien und Dokumente, welche Personen-/Vertrauliche Daten beinhalten, müssen innerhalb einer spezifizierten, dokumentierten Zeitspanne gelöscht oder zerstört werden.

Das Erstellen von Ausdrucken von Personen-/Vertraulichen Daten muss eingeschränkt sein und Ausdrucke müssen nach Verwendung sicher zerstört werden.

Der Lieferant muss die Verarbeitung von Personen-/Vertraulichen Daten auf tragbaren Speichermedien/-geräten ohne angemessene Verschlüsselung unterbinden, außer dies kann nicht mit angemessenem Aufwand implementiert werden und jede Verwendung ist dokumentiert. Jedes Speichermedium mit Personen-/Vertraulichen Daten von A1 Digital, welches die Räumlichkeiten des Lieferanten verlässt, muss einen entsprechenden Freigabe-Prozess durchlaufen haben und Maßnahmen zum Zugriffsschutz müssen implementiert sein (z.B. Verschlüsselung).

h) Lieferantenmanagement (Sicherheit und Datenschutz in Verträgen)

Wenn der Lieferant Sub-Lieferanten nutzt um Personen-/Vertrauliche Daten von A1 Digital zu speichern oder verarbeiten, muss er eine schriftliche Zustimmung von A1 Digital einholen bevor er den Sub-Lieferant beauftragt.

Der Lieferant muss alle Datenschutz- und Sicherheitsvorgaben von A1 Digital vertraglich an seine Sub-Lieferanten weiterreichen.

Der Lieferant muss regelmäßig sicherstellen, dass seine Sub-Lieferanten die Datenschutz- und Sicherheitsvorgaben von A1 Digital einhalten. Der Lieferant muss A1 Digital auf Nachfrage Nachweise über diese Überprüfungen aushändigen können.

i) Management von Sicherheitsvorfällen

Der Lieferant muss einen Prozess zur Behandlung von Sicherheitsvorfällen definiert und implementiert haben. Dieser Prozess muss zumindest die folgenden Aspekte abdecken: Meldesystem für Vorfälle (z.B. Mailadresse, Telefonnr., Website, etc.), definierte Vorgänge und Verantwortlichkeiten für die Reaktion auf und Behandlung von Sicherheitsvorfällen.

Der Lieferant muss A1 Digital unverzüglich über jeden Sicherheitsvorfall in Kenntnis setzen, welcher Auswirkungen auf die Personen-/Vertraulichen Daten, die der Lieferant für A1 Digital verarbeitet, haben könnte.

Der Lieferant muss A1 Digital unverzüglich über rechtlich bindende Anforderungen zur Offenlegung von Daten durch Strafverfolgungsbehörden informieren, außer eine Kommunikation ist explizit von der Behörde untersagt worden. Im Falle einer Offenlegung

muss der Lieferant A1 Digital informieren, welche Daten an wen zu welcher Zeit weitergegeben wurden.

j) Zugriffskontrolle

Der Lieferant muss angemessene Methoden zur Benutzer-Authentifikation (Passwort, Biometrie, 2-Faktor-Authentifikation) und Verwaltung von Benutzerrechten definieren und implementieren.

Die Authentifikationsmethode muss auf jedem System, welches verwendet wird, um Personen-/Vertrauliche Daten von A1 Digital zu speichern oder zu verarbeiten, implementiert sein. Fernzugang über das Internet oder andere geteilte Netzwerke müssen mit 2-Faktor-Authentifikation geschützt werden.

Die Granularität von Zugriffsrechten muss angemessenen Schutz von Personen-/Vertraulichen Daten gegen nicht autorisierten Zugriff, Änderung oder Offenlegung bieten. Passwörter müssen mit Verschlüsselungstechnologien, welche dem Stand der Technik entsprechen, zu jeder Zeit während Speicherung und Transport geschützt werden.

k) Benutzerverwaltung

Der Lieferant muss die folgenden Benutzerverwaltungsprozess für jede Applikation, welche Personen-/Vertrauliche Daten von A1 Digital speichert oder verarbeitet, implementiert haben: Benutzer erstellen, Ändern von Benutzerrechten, Löschen eines Benutzers, Überprüfung von Benutzern auf geschäftliche Notwendigkeit, Zurücksetzen von Passwörtern.

Die Vergabe von Zugriffsrechten muss auf geschäftlicher Notwendigkeit basieren und sicherstellen, dass Personen-/Vertrauliche Daten angemessen gegen unerlaubten Zugriff, Änderung oder Veröffentlichung geschützt sind. Benutzerkonten, die von mehreren Personen geteilt werden, dürfen keinen Zugriff auf Personen-/Vertrauliche Daten von A1 Digital erhalten.

Alle Benutzerkonten (Mitarbeiter, Administratoren, Externe) müssen zumindest einmal im Quartal auf geschäftliche Notwendigkeit überprüft werden. Deaktivierte oder abgelaufene Benutzerkonten dürfen nicht anderen Personen erneut vergeben.

l) Kryptografie

Der Lieferant muss Regeln für die Verwendung von Kryptografie bei Speicherung und Übertragung von Personen-/Vertraulichen Daten definiert haben. Der Lieferant muss sicherstellen, dass Personen-/Vertrauliche Daten von A1 Digital immer verschlüsselt über unsichere Netzwerke (z.B. Internet) übertragen werden.

m) Schutz vor Malware

Der Lieferant muss Endgeräte (PCs, Notebooks, Mobiltelefone, etc.), Server, E-Mailverkehr und Webverkehr gegen Malware schützen. Der Lieferant muss angemessene Anti-Malware-

Software einsetzen und sicherstellen, dass die Software aktuell gehalten wird und immer die aktuellsten Malware-Signaturen installiert hat.

n) Änderungsmanagement

Der Lieferant muss einen formalen Prozess zur Handhabung von Änderungen in allen produktiven Umgebungen, welche Personen-/Vertrauliche Daten von A1 Digital speichern oder verarbeiten, implementiert haben. Alle Änderungen an und Produktivnahmen von Systemen oder Applikationen müssen nach dem Prozess durchgeführt und dokumentiert werden. Der Prozess muss sicherstellen, dass angemessene Sicherheitstests vor Änderungen in Produktivumgebungen durchgeführt werden.

Der Lieferant muss die Effektivität seines Änderungsmanagement-Prozesses regelmäßig überwachen und A1 Digital Nachweise über die Überwachung auf Nachfrage zukommen lassen.

o) Datensicherung und -wiederherstellung

Der Lieferant muss eine Datensicherungs- und -wiederherstellungstrategie, sowie einen Prozess zur Durchführung und Überwachung von Sicherungen und Wiederherstellungen implementiert haben. Diese Strategie muss definieren welche Daten gesichert werden müssen, wie lange die Sicherungen aufbewahrt werden müssen und auf welchen Systemen/Standorten die Backups aufbewahrt werden.

Die Integrität von Backups muss regelmäßig getestet werden, indem eine komplette Datenbank aus einem Backup auf ein Testsystem eingespielt wird und die Daten verifiziert werden. Alle Wiederstellungsvorgänge müssen angemessen aufgezeichnet werden (Verantwortliche Person, Beschreibung der wiederherstellten Daten, Liste der Datensätze/Dateien, die wieder hergestellt wurden).

Alle Daten, die auf Band gesichert werden, müssen verschlüsselt werden. Bänder müssen sicher zerstört werden, wenn sie außer Betrieb genommen werden.

p) Log Management

Der Lieferant muss ein Log Management Konzept implementiert haben, welches definiert welche Transaktionen und Aktivitäten geloggt werden müssen (zumindest: Zugriff und Änderung von Personen-/Vertraulichen Daten von A1 Digital), wie lange die Logs aufbewahrt werden, wie die Logs regelmäßig/automatisiert auf Unregelmäßigkeiten überwacht werden und wer Zugriff auf die Logdateien hat.

q) Management von Softwareupdates (Patches)

Der Lieferant muss einen Prozess zur Handhabung von Softwareupdates implementiert haben, welcher sicherstellt, dass alle Systeme alle Sicherheits-relevanten Softwareupdates innerhalb definierter Zeiträume erhalten.

r) Systemhärtung

Der Lieferant muss einen Prozess implementiert haben, um sicherzustellen, dass alle Systeme und Applikationen, welche Personen-/Vertrauliche Daten von A1 Digital speichern oder verarbeiten, sicher konfiguriert sind. Der Prozess muss sicherstellen, dass zumindest alle nicht benötigten Ports, Interfaces und Services auf allen Systemen deaktiviert sind und Standard-/Hersteller-Passwörter geändert wurden.

Der Lieferant muss A1 Digital auf Nachfrage Nachweise seiner Härtungsmaßnahmen zur Verfügung stellen können.

s) Schwachstellen- und Webanwendungsscans

Der Lieferant muss einen Prozess implementiert haben, um regelmäßig (zumindest monatlich) alle seine Systeme auf Schwachstellen zu überprüfen. Schwachstellen sind z.B. fehlende Softwareupdates, unsichere Konfiguration oder schwache Verschlüsselungstechnologien. Der Prozess muss weiters sicherstellen, dass in einer angemessenen Zeit nach Identifikation einer Schwachstelle entsprechende Gegenmaßnahmen getroffen werden, um die Schwachstelle zu schließen.

t) Penetrationstest

Der Lieferant muss regelmäßig angemessene Security Tests/Audits von Systemen, die Personen-/Vertrauliche Daten von A1 Digital speichern oder verarbeiten, durchführen. Penetrationstest gelten als angemessene Tests. Der Lieferant muss A1 Digital auf Nachfrage Einsicht in die Testergebnisse und abgeleitete Maßnahmen gewähren.

u) Trennung von Produktion, Test und Entwicklung

Der Lieferant muss Produktions-, Test- und Entwicklungsumgebung mit angemessenen technischen Maßnahmen (z.B. Firewalls) voneinander trennen. Der Lieferant muss sicherstellen, dass keine produktiven Daten von A1 Digital in Test- oder Entwicklungssystemen verwendet werden. Testbenutzer des Lieferanten dürfen keinen Zugriff auf produktive Systeme haben, welche Daten von A1 Digital speichern oder verarbeiten.

v) Softwareentwicklung

(1) Der Lieferant muss Politiken, Richtlinien und Anweisungen von technischen und organisatorischen Sicherheitsmaßnahmen, die eine angemessen sichere Software- und Systementwicklung gewährleisten, implementiert haben. Dies beinhaltet auch Entwicklungen für Middleware, Datenbanken, Betriebssysteme, Netzwerkkomponenten und alle anderen Komponenten der IT-Umgebungen. Die Sicherheitsmaßnahmen müssen zumindest die folgenden Aspekte abdecken:

- Sicherheit ist Teil der Softwareentwicklungsmethodik und richtet sich nach verbreiteten Standards (z.B. OWASP für Webanwendung, OWASP Secure Coding Practices Checklist, etc.). Zumindest die folgenden Aspekte müssen in der Methodik adressiert werden: Sichere (verschlüsselte) Maschinenkommunikation, sichere Kommunikation mit Endbenutzern, Zugriffskontrollen und Benutzerverwaltung nach Stand der Technik, sichere Interaktion mit Web-Browsern.

- Sicherheit der Entwicklungsumgebung (z.B. getrennte Entwicklungs-/Test-/Produktionsumgebungen).
- Richtlinien für sichere Programmierung für alle verwendeten Programmiersprachen (z.B. hinsichtlich Buffer Overflows, verbergen von internen Object References vor Benutzern, etc.).
- Sicherheit in der Versionierung und Speicherung von Quellcode.

(2) Wenn die Entwicklung der Software oder des Systems (oder Teile der Software/Systeme), insbesondere Design, Entwicklung, Tests und/oder Ausrollen von Quellcode, an Dritte ausgelagert ist, müssen die folgenden Aspekte zwischen dem Lieferanten und seinem Sub-Lieferanten vereinbart werden:

- Anforderungen an einen sicheren Softwareentwicklungsprozess, insb. in Design, Entwicklung und Tests.
- Abnahmetests und die Qualität der zu liefernden Leistungen auf Basis der vereinbarten funktionalen und nicht-funktionalen Anforderungen
- Nachweise, dass angemessene Security-Tests durch die Sub-Lieferanten durchgeführt wurden.

w) Software- oder Systemqualitätskriterien für Sicherheit

Die folgenden Anforderungen müssen für jedes Release oder jede neue Softwareversion, die an A1 Digital ausgeliefert wird, sichergestellt werden:

- Jedes Release oder neue Version von Software oder Systemen muss vor der Auslieferung auf Qualitäts- und Sicherheitskriterien hin getestet werden. Die gewählte Testmethode muss sicherstellen, dass ausgelieferte Software oder Systeme keine Schadsoftware und keine veröffentlichten Schwachstellen enthalten. Testprotokolle müssen A1 Digital auf Nachfrage vorgelegt werden können.
- Im Fall, dass eine neue Schwachstelle in der Software, dem System oder darunter liegenden Softwareteilen oder Komponenten, die an A1 Digital ausgeliefert wurden, identifiziert werden, ist der der Lieferant verpflichtet A1 Digital unmittelbar darüber zu informieren und notwendige Sicherheitsupdates in angemessener Zeit zur Verfügung zu stellen.
- Jede unspezifizierte Zugriffsmethode (Backdoor) zur Software oder zu dem System für den Lieferanten oder Dritte ist strengstens verboten.

x) Physikalische Sicherheit, Zutrittskontrolle

Der Lieferant muss sicherstellen, dass alle Systeme und Applikationen, welche für Speicherung und Verarbeitung von Personen-/Vertraulichen Daten von A1 Digital verwendet werden, in angemessen ausgestatteten Rechenzentren betrieben werden. Die Rechenzentren müssen angemessene Kontrollen gegen Umwelteinflüsse (z.B. Klimaanlage, unterbrechungsfreie Stromversorgung, Feuerbekämpfungssysteme, etc.),

eine angemessene physikalische Konstruktion und angemessene Zutrittsschutzmaßnahmen implementiert haben.

Die Rechenzentren müssen kontrollierten Zutritt zu den Gebäuden, sowie gesicherten Zutritt zu den verschiedenen Bereichen der Mieter implementiert haben. Der Zutritt muss mittels Zutrittskarte, Pin-Codes, biometrischen Sensoren oder anderen angemessenen Methoden gesichert sein. Weiters muss ein formaler Prozess implementiert sein, welcher das Hinzufügen, Löschen, Ändern sowie regelmäßige Überprüfen von Zutrittsrechten sicherstellt.

y) Business Continuity Management

Der Lieferant muss zumindest die folgenden Aspekte von Business Continuity Management definiert und implementiert haben: Angemessene Redundanzen von IT-Systemen, um die Anforderungen an die Verfügbarkeit der Services von A1 Digital sicherstellen zu können, Verantwortlichkeiten für Krisenmanagement, Prozesse und Prozeduren zum Verhalten in einem Krisenfall.