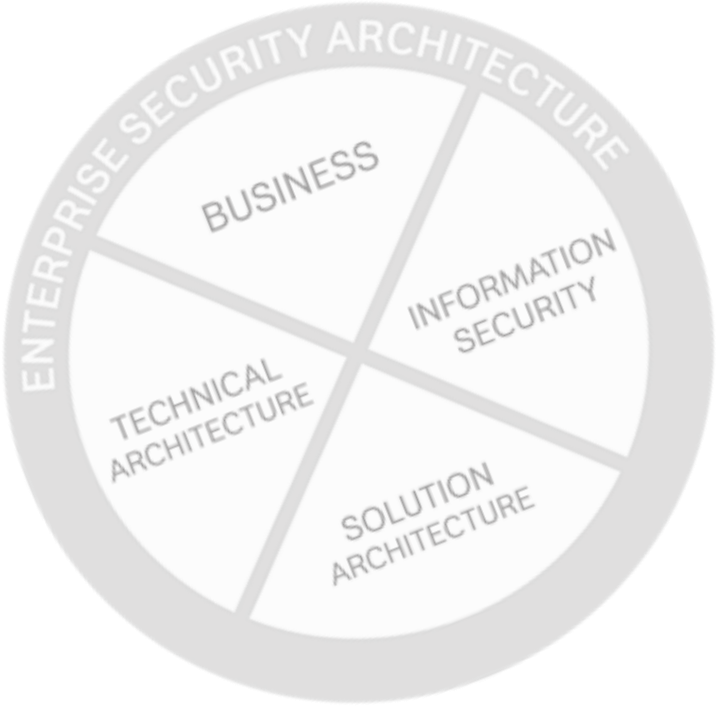
A1 Digital International GmbH & Co KG
Lassallestraße 9, 1020 Wien

A1 Digital Deutschland GmbH
Rosenheimer Strasse 116, 81669 München

A1 Digital Cyber Security Consulting Services

Servicebeschreibung & -bedingung



Version: 3.3

Datum: 01.04.2026

Inhaltsverzeichnis

1 Allgemeines

Diese Servicebeschreibung und -bedingung gilt ab 15.05.2023 Sie erläutert die Leistungen von A1 Digital International GmbH (im Folgenden: A1 Digital), welche Ihnen im Rahmen der Durchführung eines A1 Enterprise Security Architecture Consultings angeboten und bereitgestellt werden.

Diese Servicebeschreibung und -bedingungen beinhalten unser gesamtes Portfolio; die konkret vereinbarten Leistungsteile sind je nach Kunde unterschiedlich und ergeben sich aus dem Angebot für den Kunden. Die Behebung von identifizierten Fehlern/Schwachstellen ist nicht Teil unserer Leistung.

Sofern hier nicht Abweichendes geregelt wird, kommen die Allgemeinen Geschäftsbedingungen für IoT und Security Solutions von A1 Digital zur Anwendung: https://www.a1.digital/de/agb/ .

Kunde von **A1 Digital International GmbH & Co KG** Enterprise Security Architecture Consulting kann nur ein Unternehmer im Sinne des § 1 des Konsumentenschutzgesetzes (KSchG) sein. (AT)

Kunde von **A1 Digital Deutschland GmbH** Enterprise Security Architecture Consulting kann nur ein Unternehmer im Sinne des § 14 des Bürgerlichen Gesetzbuches (BGB) sein. (DE)

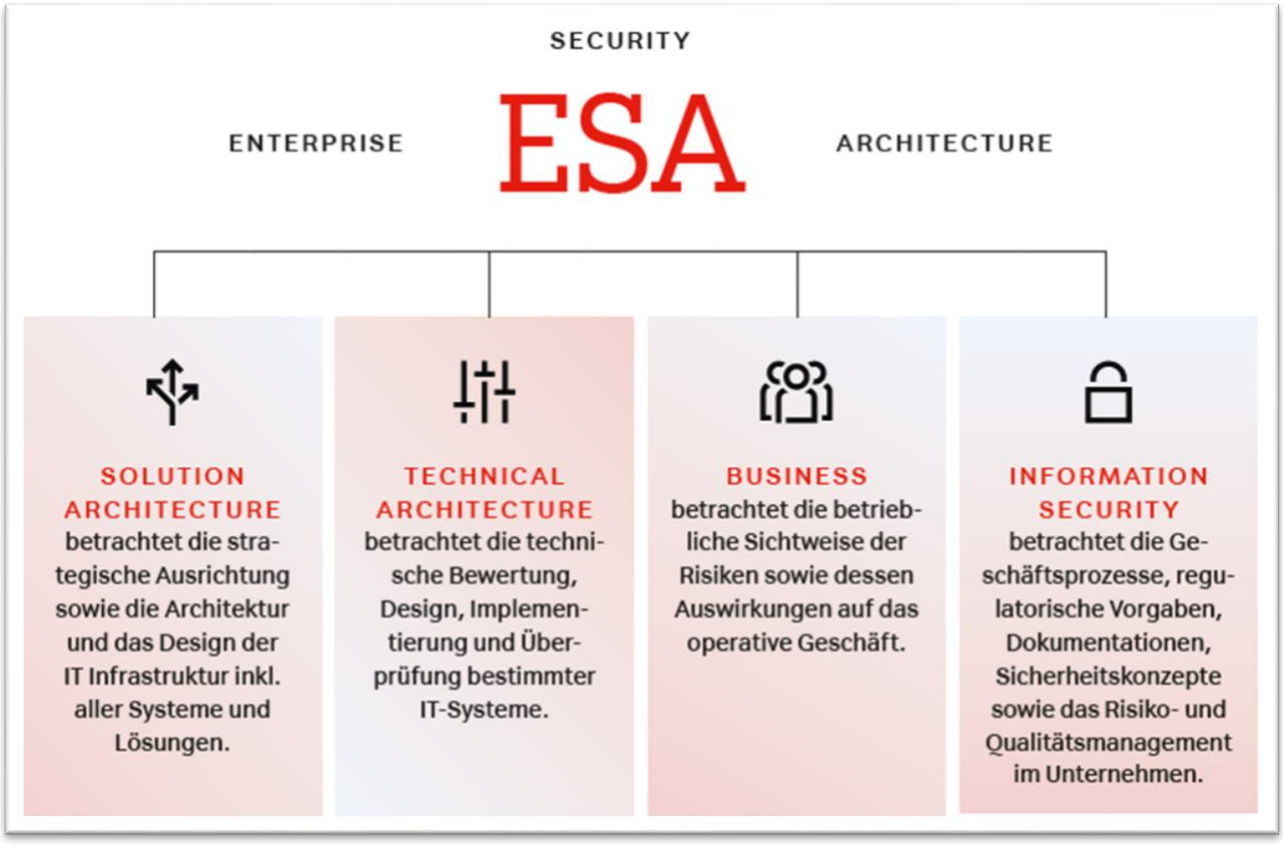
2 Servicebeschreibung

A1 Digital berät Unternehmen in den Bereichen Informationssicherheit und Risikomanagement. Je nach Anforderung können entweder nur bestimmte Teilbereiche des Unternehmens oder auch das gesamte Unternehmen analysiert und bewertet werden, Handlungsempfehlungen und Best Practices abgeleitet sowie bei der Behebung von erkannten Problemen unterstützt werden.

Um jedem Unternehmen basierend auf den unternehmerischen Anforderungen die bestmögliche Beratung bieten zu können, wurde das **A1 Digital Enterprise Security Architecture-Modell** entwickelt.

Die Grundlage dieses Modells bildet eine Kombination aus branchenweiten Standards und Frameworks sowie die jahrelange Erfahrung der A1 Digital Security-Experten im IT Security Consulting-Bereich. Daraus wurde ein standardisiertes Beratungsmodell geformt, welches sowohl allgemein als auch Branchen-spezifisch auf die Gegebenheiten des Unternehmens eingeht.

Das ESA-Modell ist in vier Teilbereiche (Sichtweisen) untergliedert:



2.1 Consulting Services

Basierend auf dem ESA-Modell werden von A1 Digital verschiedenste Consulting-Leistungen in Form von Paketen angeboten. Obwohl diese Pakete grundsätzlich standardisiert sind, kann es je nach Unternehmensgröße und -anforderung sinnvoll sein, einzelne Pakete zu kombinieren (z.B. im Rahmen unseres CISO-as-a-Service (CISOaaS) in Pkt. 2.1.6) oder Teilbereiche aus den einzelnen Paketen herauszulösen und zu einem neuen Gesamtpaket zusammenzufassen. Daraus ergibt sich eine für jeden Kunden individuell abgestimmte Consulting-Leistung mit eigener Aufwandsabschätzung.

2.1.1 Cyber Risk Evaluation

Mittels des Cyber Risk Evaluation-Pakets wird das gesamte Unternehmen einer detaillierten Analyse unterzogen. Ziel der Analyse ist es, einen ganzheitlichen Überblick über die im Unternehmen verwendeten Technologien, Architekturen und Prozesse zu bekommen, um dessen Bewertung nach einheitlichen Kriterien durchführen zu können und daraus weitere Handlungsschritte ableiten zu können.

Umfang

Basierend auf den vier Sichtweisen des ESA-Modells gliedert sich die Analyse in folgende Teilbereiche:

- Struktur und Organisation
- Compliance, Policies und Frameworks
- Data Security & Confidentiality
- Identity Management
- Infrastructure, Datacenter und Endpoint Security
- Application Security
- Cloud Security
- IoT- und OT-Security
- IT Operations

Ablauf

Die Analyse des Unternehmens wird von erfahrenen Security-Experten der A1 Digital in Form von Analyseworkshops durchgeführt. Jeder Security-Experte ist Spezialist in seinem Gebiet und führt die Analyse anhand einer innerhalb A1 Digital einheitlichen Fragemethodik durch. Durch dieses Vorgehen ist sichergestellt, dass sowohl ein

standardisierter und vergleichbarer Report erstellt wird, als auch die persönliche Erfahrung des Security-Experten in die Bewertung des Unternehmens mit einfließt.

Neben den Security-Experten, welche die Analyseworkshops durchführen, begleitet als interner Projektmanager und Single-Point-of-Contact ein Lead Consultant das Projekt.

Das Cyber Risk Evaluation-Paket gliedert sich in die folgenden Arbeitspakete:

- Im **Kickoff** werden die Rahmenbedingungen für das Projekt abgestimmt, die Zuständigkeiten und Verpflichtungen geklärt, Folgetermine festgelegt sowie im Vorfeld benötigte Dokumente spezifiziert.
- Danach werden die zuvor angeforderten **Dokumente** gesichtet sowie der Analyseworkshop vorbereitet.
- Im Zuge der **Analyseworkshops** werden Experten aus allen Teilbereichen Interviews mit den verantwortlichen Personen führen, um Detailinformationen zum jeweiligen Gebiet zu erhalten. Auch werden erste Bewertungen und Einschätzungen abgegeben.
- Danach werden die Unterlagen und erhaltenen Informationen aufbereitet, die **Risikobewertung** durchgeführt, weitere Maßnahmen zu den einzelnen Teilbereichen definiert und ein detaillierter Bericht erstellt.
- Bei der **Präsentation der Ergebnisse** werden alle Erkenntnisse der Analyse und Risikobewertung sowie mögliche Handlungsempfehlungen präsentiert (z.B. im Rahmen eines Berichts oder einer Abschlusspräsentation).

2.1.2 Incident Response Management

Mittels des Incident Response Management-Pakets werden Unternehmen im Bereich der Analyse und der richtigen Verhaltensweise im Zuge eines Sicherheitsvorfalls beraten. Dies umfasst die Adaptierung von Unternehmensprozessen sowie die Definition von Notfallplänen. Ziel ist es, ein Unternehmen so aufzustellen, dass Sicherheitsvorfälle schnell erkannt, strukturiert bewertet und effizient behoben werden können, um Schäden zu minimieren und die Handlungsfähigkeit sicherzustellen.

Umfang

Basierend auf den vier Sichtweisen des ESA-Modells gliedert sich die Beratungs-dienstleistung in folgende Teilbereiche:

- Durchführung eines Analyse-Workshops
- Erhebung und Bewertung der Unternehmensanforderungen
- Bewertung der Risiken und Definition der kritischen Geschäftsabläufe und Prozesse
- Entwicklung von Notfallplänen
- Erstellung und Adaptierung von Incident Response Management-Prozessen
- Mitarbeiter-Schulungen zur Vorbereitung auf Sicherheitsvorfälle

Ablauf

Die Beratungsdienstleistung wird von erfahrenen Security-Experten der A1 Digital durchgeführt. Neben den Security-Experten begleitet als interner Projektmanager und Single-Point-of-Contact ein Lead Consultant das Projekt.

Das Incident Response Management-Paket gliedert sich in die folgenden Arbeitspakete:

- Im **Kickoff** werden die Rahmenbedingungen für das Projekt abgestimmt, die Zuständigkeiten und Verpflichtungen geklärt, Folgetermine festgelegt sowie im Vorfeld benötigte Dokumente spezifiziert.
- Danach werden die zuvor angeforderten **Dokumente** gesichtet sowie der Analyseworkshop vorbereitet.
- Im Zuge des **Analyseworkshops** werden Interviews mit dem Operations Team, dem internen CERT (sofern vorhanden) sowie den zuständigen Prozesseigentümern geführt, um Detailinformationen zum IT Service Management im Allgemeinen sowie

den praktischen Abläufen und Vorgangsweisen im Unternehmen im Speziellen zu erhalten. Auch werden erste Bewertungen und Einschätzungen abgegeben.

- Nach dem Analyseworkshop werden die vorhandenen Incident Response Management-Prozesse und Geschäftsabläufe bewertet sowie Notfallpläne zu kritischen Prozessen erstellt bzw. sofern vorhanden bewertet und adaptiert.
- Von den Ergebnissen des Analyseworkshops werden **Mitarbeiterschulungen** geplant, in welchen neben der Vermittlung von theoretischem Wissen auch Sicherheitsvorfälle analysiert werden, z.B. in Form eines Planspiels (siehe **Error! Reference source not found.** Übung von Notfällen und Krisensituationen).

2.1.3 Übung von Notfällen und Krisensituationen

Im Rahmen von Planspielen (in Form von Tabletop Exercises) werden die Vorbereitung, Durchführung und Bewertung von Notfall- und Krisenplänen beübt. Ziel ist es, die Wirksamkeit der bestehenden Betriebskontinuitäts- und Incident Response-Maßnahmen zu überprüfen sowie organisatorische, prozessuale und kommunikative Abläufe praktisch zu testen.

Umfang

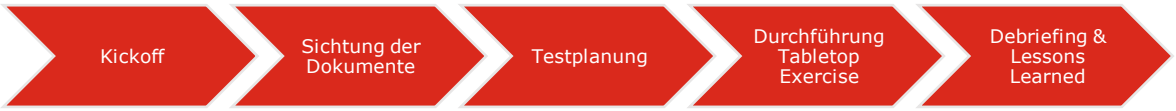
Basierend auf den vier Sichtweisen des ESA-Modells gliedert sich die Beratungsdienstleistung in folgende Teilbereiche:

- Review der vorhandenen Business Continuity- und Incident Response-Dokumentation des Kunden
- Unterstützung bei der Definition des Testszenarios sowie der Testziele und Nicht-Ziele
- Durchführung von einem szenariobasierten Tabletopop Exercise
- Moderation der Übungen sowie Dokumentation der Lessons Learned

Ablauf

Unsere Tabletop Exercises werden von erfahrenen Security-Experten durchgeführt. Ein Lead Consultant übernimmt die Rolle des internen Projektmanagers und fungiert als zentraler Single-Point-of-Contact über den gesamten Projektverlauf.

Das Tabletop Exercise gliedert sich in die folgenden Arbeitspakete:



- **Kickoff**: Abstimmung der Rahmenbedingungen, Rollen, Zuständigkeiten und Kommunikationswege. Klärung der benötigten Dokumente sowie Festlegung der Projektmeilensteine.
- **Sichtung der Dokumente**: Sichtung der bereitgestellten Business Continuity- und Incident Response-Dokumentation zur Vorbereitung der Planspiele.
- **Testplanung**: Gemeinsame Definition der konkreten Testszenarien, Testziele und Nicht-Ziele.

- **Durchführung der Tabletop Exercise**: Moderation und Dokumentation des definierten Szenarios anhand der geplanten Abläufe.
- **Debriefing & Lessons Learned**: Moderierte Nachbesprechung der gewonnenen Erkenntnisse mit allen Beteiligten.

2.1.4 Compliance- und Zertifizierungs-Unterstützung

Unternehmen stehen oft vor der Herausforderung, bestimmte Compliance-Prüfungen (wie z.B. NIS-2 oder DORA) bzw. Zertifizierungen (wie z.B. ISO 27001, 27018, oder BSI IT-Grundschutz) zu bestehen, um sowohl externen als auch internen Vorgaben gerecht zu werden. Ziel ist es, Unternehmen gezielt dabei zu helfen, Sicherheitsanforderungen strukturiert zu erfüllen und eine erfolgreiche Prüfung oder Zertifizierung zu ermöglichen.

Umfang

Basierend auf den vier Sichtweisen des ESA-Modells gliedert sich die Beratungs-dienstleistung in folgende Teilbereiche:

- Erhebung und Bewertung der relevanten Anforderungen
- Durchführung von Gap-Analysen (z.B. im Rahmen von Workshops)
- Erstellung eines Maßnahmenplans unter Betrachtung der Kundenumgebung und -infrastruktur
- Unterstützung in der Durchführung der technischen und organisatorischen Maßnahmen
- Unterstützung vor und während des Audits oder im Rahmen der Prüfung (sofern möglich und erlaubt)
- Gemeinsame Nachbereitung des Audits oder der Prüfung mit dem Kunden, sowie Definition weiterer Schritte

Ablauf

Das „Get your certification!"-Paket gliedert sich in die folgenden Arbeitspakete:

- Im **Kickoff** werden die Rahmenbedingungen für das Projekt abgestimmt, die Zuständigkeiten und Verpflichtungen geklärt sowie Folgetermine festgelegt.
- Im Zuge einer **Gap-Analyse** werden Interviews mit den zuständigen Stellen/Abteilungen und Prozesseigentümern durchgeführt, um Detailinformationen zur Infrastruktur und Kundenumgebung im Allgemeinen sowie den praktischen Abläufen und Vorgangsweisen im Unternehmen im Speziellen zu erhalten. Interne Dokumente und Prozesse werden bewertet und den jeweiligen Anforderungen gegenübergestellt.

- Nach der Gap-Analyse werden **Maßnahmenpläne** erarbeitet und bei der Durchführung dieser Maßnahmen unterstützt. Hier lassen die A1 Digital Experten ihre langjährige Erfahrung als Auditoren diverser Zertifizierungen mit einfließen.
- Sofern es möglich ist, wird sowohl während als auch nach dem **Audit oder der Prüfung** dem Kunden zur Seite gestanden, Schlüsse aus den Ergebnissen gezogen und weitere Maßnahmen definiert.

2.1.5 IT-/ IoT-/ OT-Security Beratung

Neben strategischer und technischer Beratung im Information Technology-Umfeld bietet A1 Digital auch eine strategische und prozessuale Beratung in den Bereichen Internet-of-Things (IoT) und Operational Technology (OT) Security an. Dies umfasst sowohl eine architekturelle Überprüfung der Infrastruktur als auch eine prozesstechnische und strategische Evaluierung des Ist-Standes im Unternehmen.

Umfang

Unsere OT Security Beratung umfasst folgende Maßnahmen:

- Evaluierung der unternehmensspezifischen Anforderungen und Gegebenheiten im Bereich IoT und OT Security
- Bewertung der Infrastruktur in den Bereichen Perimeterschutz, Zugriffswege, Segmentierung, Schnittstellen und Berechtigungen
- Bewertung der bestehenden Sicherheitsmaßnahmen je Zone und Geräteklasse/-funktion nach gängigen Standards wie zB. NIST CSF oder IEC 62443
- Evaluierung der Unternehmensprozesse im OT-Bereich mit Anknüpfungspunkten in die IT-Welt
- Erstellung eines Maßnahmenkatalogs zur Verbesserung der Sicherheitsarchitektur in den Bereichen IoT und OT

Ablauf

Das „OT Security Beratungs"-Paket gliedert sich in die folgenden Arbeitspakete:

- Im **Kickoff** werden die Rahmenbedingungen für das Projekt abgestimmt, die Zuständigkeiten und Verpflichtungen geklärt, Folgetermine festgelegt sowie im Vorfeld benötigte Dokumente spezifiziert.
- Danach werden die zuvor angeforderten **Dokumente** gesichtet sowie der Analyseworkshop vorbereitet.
- Im Zuge der **Analyseworkshops** werden mit Experten aus allen Teilbereichen Interviews mit den verantwortlichen Personen führen, um Detailinformationen zum jeweiligen Gebiet zu erhalten. Auch werden erste Bewertungen und Einschätzungen abgegeben.

- Danach werden die Unterlagen und erhaltenen Informationen aufbereitet, die **Risikobewertung** durchgeführt, weitere Maßnahmen zu den einzelnen Teilbereichen definiert und ein detaillierter Bericht erstellt.
- Bei der **Präsentation der Ergebnisse** werden alle Erkenntnisse und Maßnahmen der Analyse und der Risikobewertung sowie ein Fahrplan für die Zukunft präsentiert.

2.1.6 CISO-as-a-Service (CISOaaS)

Mit dem CISO-as-a-Service-Paket erhalten Unternehmen eine kontinuierliche, strategische und taktisch-operative Unterstützung beim Aufbau und der Weiterentwicklung ihres Informationssicherheitsmanagementsystems. Dies umfasst fachliche Beratung, operative Mitarbeit, Management-Begleitung sowie die Weiterentwicklung sicherheitsrelevanter Prozesse, Richtlinien und Maßnahmen. Ziel ist es, gemeinsam mit dem Kunden sicherzustellen, dass Informationssicherheit dauerhaft im Unternehmen verankert, gesteuert und überwacht wird.

Umfang

Basierend auf unseren oben beschriebenen Consulting Services kann unser CISOaaS folgende Aktivitäten zur Unterstützung der Geschäftsführung beim Aufbau und Pflege eines Informationssicherheitsmanagementsystems (ISMS) umfassen:

- Definition einer Informationssicherheitsstrategie
- Entwicklung von Sicherheitsrichtlinien, -prozessen und -verfahren
- Identifikation von Security-Bedrohungen für die Organisation
- Analyse der Security-Risiken und bestehender Sicherheitsmaßnahmen, um Gefahrenpotentiale festzustellen
- Prüfung sicherheitsrelevanter Risiken und Ableitung geeigneter Maßnahmen im Umgang mit neuen Technologien (z.B. Künstliche Intelligenz, KI)
- Unterstützung bei der Formulierung geeigneter Sicherheitsmaßnahmen (organisatorisch, prozessual, technisch), um den Schutzbedarf der Organisation angemessen abzudecken
- Unterstützung bei Aufbau und Überprüfung einer angemessenen technischen Sicherheitsarchitektur, inklusive technischer Sicherheitsmaßnahmen
- Durchführung von Security-Trainings und Awareness-Maßnahmen
- Durchführung von internen Audits zur Überprüfung der Effektivität der Security-Maßnahmen
- Definition relevanter Kennzahlen und Reporting an die Geschäftsführung

Ablauf

Das „CISO-as-a-Service"-Paket gliedert sich in die folgenden Schritte:

- Im **Kickoff** analysiert A1 Digital mit Ihnen den Stand des Informationssicherheitsmanagements – von der strategischen bis zur taktisch-operativen Umsetzungsebene.
- Basierend darauf werden **Handlungsfelder** identifiziert, priorisiert und als detaillierte Arbeitspakete strukturiert.
- Die Umsetzung dieser **Arbeitspakete** erfolgt in einem vereinbarten Rahmen. Die hohe und breit abgestützte Qualifikation der Mitarbeitenden von A1 Digital stellt dabei sicher, dass Ihnen jederzeit das richtige Fachwissen zur Verfügung steht.

3 Servicebedingung

3.1 Nutzungsvoraussetzungen

- Vor Beginn des Projekts stellt der Kunde A1 Digital einen Ansprechpartner zur Verfügung.
- Hardware, Zugangsdaten und sonstige Informationen, die für die Erbringung der Leistungen notwendig sind, stehen A1 Digital spätestens am Tag vor Beginn der Dienstleistung zur Verfügung.
- Die Ergebnisse werden in Form eines Berichts als PDF-Format oder PowerPoint an den Kunden übermittelt.

3.2 Verantwortlichkeit und Haftung (AT)

A1 Digital haftet nur bei Vorsatz oder grober Fahrlässigkeit. Die Haftung für entgangenen Gewinn, ausgebliebene Einsparungen, Zinsverluste, mittelbare und Folgeschäden, ideelle Schäden, sowie Schäden aus Ansprüchen Dritter, sowie für verlorengegangene oder veränderte Daten, ist ausgeschlossen. Der Kunde hält A1 Digital hinsichtlich sämtlicher von Dritter Seite erhobener Ansprüche in vollem Umfang schad- und klaglos.

3.3 Verantwortlichkeit und Haftung (DE)

A1 Digital leistet gegenüber dem Kunden Schadenersatz oder Ersatz vergeblicher Aufwendungen, gleich aus welchem Rechtsgrund (z. B. aus rechtsgeschäftlichen und rechtsgeschäftsähnlichen Schuldverhältnissen, Pflichtverletzung und unerlaubter Handlung), nur in folgendem Umfang:

a) Die Haftung bei grober Fahrlässigkeit, Vorsatz, Arglist und aus Garantie wird hierdurch nicht vertraglich eingeschränkt.

Auch für Schäden aus der schuldhaften Verletzung des Lebens, des Körpers oder der Gesundheit und bei Ansprüchen nach dem Produkthaftungsgesetz gelten die gesetzlichen Regelungen uneingeschränkt.

b) Bei Verletzung einer vertragswesentlichen Pflicht, deren Erfüllung also die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung der Vertragspartner regelmäßig vertrauen darf (sog. Kardinalpflicht), haftet A1 Digital nur in Höhe des bei Vertragsabschluss typischerweise vorhersehbaren Schadens.

Die Haftung für einfache Fahrlässigkeit ist gegenüber dem Kunden (und auch Körperschaften des öffentlichen Rechts) bei Verletzung einer nicht vertragswesentlichen Pflicht ausgeschlossen.

c) Soweit die Haftung von A1 Digital nach dem Vorstehenden ausgeschlossen oder beschränkt ist, gilt dies auch für die persönliche Haftung der Mitarbeiter, Vertreter und Erfüllungsgehilfen von A1 Digital.

d) Für Schäden, die aus einer vertragswidrigen Verwendung der Leistungen von A1 Digital resultieren, haftet A1 Digital nicht.

3.4 Leistungsabgrenzung

Die Beratung durch A1 Digital Enterprise Security Architecture Consulting kann keine absolute Sicherheit für Systeme, Daten oder Prozesse sicherstellen. A1 Digital übernimmt keinerlei Verantwortung dafür, dass vorhandene Schwachstellen erkannt werden.

Die Behebung von entdeckten Fehlern/Schwachstellen oder technische Unterstützungsleistungen ist nicht Teil der Leistungen.

3.5 Aufwände

In der Regel werden die Aufwände (Personentage) individuell in einem gemeinsamen Scoping Termin/Gespräch mit dem Ansprechpartner anhand von gezielten Fragen ermittelt. Die gesammelten Ergebnisse werden anschließend in Personentagen kalkuliert und im Angebot angeführt.

3.6 Reisezeiten

Sollten Termine vor Ort notwendig sein, behält sich A1 Digital die Verrechnung von Reisekosten, Hotelkosten und Spesen vor. Mitarbeiter des Auftragnehmers reisen zur Leistungserbringung abhängig von der jeweiligen vertragsgegenständlichen Gesellschaft entweder von Wien oder von München an.

Für Vertragsverhältnisse mit der **A1 Digital International GmbH & Co KG** ist für die Berechnung der Reisezeit vorbehaltlich einer abweichenden Vereinbarung der Ausgangsort **Wien** maßgeblich.

Für Vertragsverhältnisse mit der **A1 Digital Deutschland GmbH** ist für die Berechnung der Reisezeit vorbehaltlich einer abweichenden Vereinbarung der Ausgangsort **München** maßgeblich.

Etwaige darüber hinaus anfallende Reise- und Nebenkosten werden, sofern vertraglich vereinbart, gesondert in Rechnung gestellt.

4 Datenschutz und Datensicherheit

Das Service wird innerhalb Europas betrieben.

Weitere Informationen können unserer Website entnommen werden: https://www.a1.digital/de/agb/

Es gelten die Allgemeinen Geschäftsbedingungen der A1 Digital für Auftragsverarbeitung (AGB AVV). Diese finden Sie auf https://www.a1.digital/de/agb/

5 Datenschutzanhang zur Leistungsbeschreibung

In Rahmen den von uns bereitgestellten Leistungen werden wir Ihre personenbezogenen Daten im Sinne der Art. 28 DSGVO als Auftragsverarbeiter (AV) verarbeiten.

1. Gegenstand des Auftrags

1.1 Der Auftrag des für die Verarbeitung Verantwortlichen an den Auftragsverarbeiter umfasst folgende Produkte oder Leistungen: **„A1 Digital Enterprise Security Architecture"**

1.2 Folgende Datenarten können regelmäßig Gegenstand der Verarbeitung sein:

- ☒ Personen-Stammdaten
- ☐ Personen-Kennungen
- ☐ Besondere personenbezogene Daten
- ☐ Marketing/Sales-Daten mit Personenbezug
- ☒ Personen-Rollen/-Assoziationen
- ☐ Kundeninventar
- ☐ Kundeninteraktionen
- ☐ Verkehrsdaten
- ☐ Bewegungsdaten | Geolocation Data
- ☐ Inhaltsdaten
- ☐ Finanzdaten
- ☐ Login, Passwörter

1.3 Kreis der von der Datenverarbeitung Betroffenen:

- ☐ Kunde des Auftraggebers - natürliche Person

☐ Kunde des Auftraggebers - juristische Person

☐ User des Enterprise Kunden

☒ Mitarbeiter des Auftraggebers

☒ Vertragspartner des Auftraggebers

☐ Kinder oder Schutzbedürftige Personen

2. Liste der beauftragten Subunternehmer

Name	Firmenadresse	Art der Verarbeitung	Ort der Verarbeitung
Tresorit	Tresorit AG Franklinstrasse 27, 8050 Zürich Schweiz	Übermittlung der Reports und Archivierung	Österreich, Schweiz

3. Technisch-organisatorische Maßnahmen

Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen zur Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen. Sofern in der Leistungsvereinbarung nicht genauer geregelt, obliegt es dem Auftragsverarbeiter, das der jeweiligen Verarbeitung angemessene Schutzniveau insbesondere durch eine Kombination der nachstehend genannten technisch-organisatorischen Maßnahmen sicherzustellen. Es ist dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

A. VERTRAULICHKEIT (ART. 32 ABS. 1 LIT. B DS-GVO)

- **Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B. durch Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen.
- **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung durch z.B.(sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern.
- **Zugriffskontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch, z.B. Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.
- **Trennungskontrolle:** Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. durch Standard-Berechtigungsprofile auf „need to know-Basis".
- **Pseudonymisierung**: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenverarbeitung entfernt, und gesondert aufbewahrt.
- **Klassifikationsschema für Daten:** Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

B. DATENINTEGRITÄT[1] (ART. 32 ABS. 1 LIT. B DS-GVO)

- **Weitergabekontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch z.B. Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur.
- **Eingabekontrolle**: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch z.B. Dokumentenmanagement.

C. VERFÜGBARKEIT UND BELASTBARKEIT (ART. 32 ABS. 1 LIT. B DS-GVO)

- **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch z.B. Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne.
- **Wiederherstellbarkeit**

[1] Verhinderung von (unbeabsichtigter) Zerstörung/Vernichtung, (unbeabsichtigter) Schädigung, (unbeabsichtigtem) Verlust, (unbeabsichtigter) Veränderung von personenbezogenen Daten.

D. VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG (ART. 32 ABS. 1 LIT. D DS-GVO; ART. 25 ABS. 1 DS-GVO)

- **Datenschutz-Management**, einschließlich regelmäßiger Mitarbeiter-Schulungen
- **Incident-Response-Management**
- **Datenschutzfreundliche Voreinstellungen**:
- **Auftragskontrolle:** Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers