A1 Information Security Supplier / Provider Requirements

Vorgaben an externe Dienstleister & Lieferanten
A1 Informationssicherheitsmanagement

A1 Information Security Supplier / Provider Requirements - Version 1.0
Security Governance & Risk Management
gültig ab 01. November 2017

Klassifizierung: öffentlich

Versionshistorie

Version 1.0		
betrifft:	Erstellung	Freigabe
Erstellung	Maha Sounble	Philipp Röhm
	26. September 2017	03. Oktober 2017
Anmerkung:		
Das Dokument basiert auf die A1 Information Security Guidelines V1.0.		

Inhaltsverzeichnis

Inhaltsverzeichnis

1 Rahmenanforderungen

Projekte, Services und Dienstleistungen müssen vor Implementierung, idealerweise bereits bei der Planung, geprüft und hinsichtlich notwendiger Sicherheitsanforderungen begleitet werden. Bei jeder größeren technischen Anpassung oder Änderung, sowie bei jeder inhaltlichen Vertragsänderung, zumindest aber standardmäßig alle drei Jahre, ist von den involvierten Fachbereichen zu überprüfen, ob sich der für die externe Datenspeicherung maßgebliche Sachverhalt geändert hat und eine Anpassung erforderlich ist.

1.1 Vertragliche Anforderungen an Dienstleister

1.1.1 Non Disclosure Agreements (NDAs)

Externe Dienstleister müssen zur Geheimhaltung verpflichtet werden, bevor vertrauliche Informationen ausgetauscht werden. Hierfür stehen Non Disclosure Agreements[1] (NDAs) zu Verfügung.

1.1.2 Vertragsbestandteile für Informationssicherheit & Datenschutz

In den Verträgen zwischen externen Dienstleistern und A1 sind die etablierten Sicherheitsmaßnahmen zu definieren und die zweckmäßige Verarbeitung der Daten zu vereinbaren. Einseitige Änderungen der Vereinbarung sind nicht zulässig.

1.2 Organisatorische Anforderungen an Dienstleister

1.2.1 Zertifizierungen

Informationstechnologie-Dienstleister, insbesondere jene, die Infrastruktur bzw. Services zur Verfügung stellen, sollten eine Zertifizierung gemäß dem ISO/IEC 27001 Standard vorweisen können. Cloud Service Provider müssen zusätzlich eine ISO/IEC 27018 Zertifizierung halten. Bei externer Datenspeicherung muss eine ISAE 3402-Konformität des Rechenzentrums vorliegen. Die Zertifizierungen sind auf die gesamte Dauer der Partnerschaft aufrecht zu erhalten. Bei der Prüfung des Dienstleisters werden entsprechende Nachweise gefordert. Bei Nichtvorlage von gültigen Zertifikaten können im Zuge der Prüfung andere Zertifizierungen angerechnet werden, wenn sie gleich- oder höherwertig sind.

[1] Hier findest Du Vorlagen für NDAs.

1.2.2 Auditrecht der A1

A1 führt Dienstleister-Audits durch, um die Einhaltung der vereinbarten Security Anforderungen vor Ort zu prüfen. Der Dienstleister muss dafür notwendige Dokumente vorlegen und Einsicht in relevante Einrichtungen und Systeme gewähren. Ein Dienstleister-Audit wird mindestens 4 Wochen im Voraus dem Dienstleister angekündigt.

1.2.3 Einsatz von Subdienstleistern

Der Dienstleister hat dafür Sorge zu tragen, dass alle Anforderungen, die an ihn gestellt werden, auch für alle Subdienstleister, die er für die Erbringung der Dienstleistung für A1 beansprucht, gelten.

1.3 Technische Anforderungen an Dienstleister

1.3.1 Datenspeicherung & Datentransfer

Interne Datenspeicherung ist zu präferieren. Sollte aus technischen oder wirtschaftlichen Gründen externe Datenspeicherung erfolgen, hat der Dienstleister für eine physische Trennung bzw. Mandantentrennung der Daten von anderen Kundinnen und Kunden zu sorgen. Die Vorgaben aus dem Kapitel 4 – „Datenspeicherung & Datentransfer“ sind zu erfüllen.

1.3.2 Datenübergabe & -löschung

Eine regelmäßige Löschung von Kunden-, Verkehrs- oder anderen schützenswerten Daten muss nach Vorgaben der A1 erfolgen, nähere Informationen befinden sich im Kapitel 2.2.9 – „Datenlöschung“. Zu Vertragsende muss die Möglichkeit geboten werden, dass der A1 sämtliche bestehende Daten übergeben werden. Jeder Lieferant hat die Daten zu löschen, wenn sie nicht mehr zur Erfüllung der vertraglichen Pflichten benötigt werden.

2 Anforderungen an Systeme & Applikationen

Systeme und Applikationen, die bei oder für A1 eingesetzt werden, müssen Mindestanforderungen erfüllen, um sie vor Bedrohungen, wie vor Datendiebstahl, Datenmanipulation, Sabotage, Blockierung (Denial of Service Attacken) und vielen weiteren zu schützen. Die vorliegenden Bestimmungen enthalten relevante Erfordernisse an Systeme und Applikationen für den internen Gebrauch, unabhängig davon, ob sie ausgelagert wurden, oder nicht. Systeme oder Applikationen für Kundinnen und Kunden unterliegen denselben Vorgaben, sofern sie anwendbar sind. Bei nicht anwendbaren Bestimmungen sind kompensierende Maßnahmen zu setzen, die ein gleiches oder höheres Schutzniveau sicherstellen.

2.1 Organisatorische Anforderungen an Systeme

2.1.1 Anforderungsmanagement

Die strukturierte und nachvollziehbare Abhandlung von technischen Demands (Anforderungen) für eine neue Geschäftsanforderung oder eine Änderung einer bestehenden technischen Lösung ist über ein geeignetes Ticketing-System abzuwickeln. Schnittstellen sind innerhalb des Underpinning Contracts (UC) zu definieren.

2.1.2 Change Management

Alle Änderungen und Implementierungen von Systemen oder Applikationen müssen gemäß einem dokumentierten Change Prozesses durchgeführt werden.

2.1.3 Prüfungen vor Inbetriebnahmen

Vor Inbetriebnahmen erfolgen mehrere Prüfungen, die im Zuge des Change Management Prozesses der A1 durchgeführt werden, unter anderem muss eine umfassende Security Prüfung durchzogen werden.

2.1.4 Berechtigungsmanagement

Berechtigungen müssen prinzipiell rollenbasiert vergeben werden. Für die Autorisierung ist der Standard-Genehmigungsprozess der Benutzerverwaltung der A1 anzuwenden. Der Dienstleister muss der A1 ermöglichen, Berechtigungen nach A1 internen Anforderungen flexibel vergeben bzw. entziehen zu können. Eine zentrale Auflistung bzw. Die Einsicht und eine automatische Auswertung aller Berechtigungen müssen ermöglicht werden.

2.1.5 Internes Kontrollsystem (ICS)

Wenn ein neues System installiert wird, wird A1 intern eine Relevanzanalyse mit dem Internen Kontrollsystem durchgeführt. Wenn eine ICS-Relevanz besteht, müssen alle Kontrollen des internen Kontrollsystems auf dem System durchgeführt werden. Die Minimalanforderung sind die „IT General Controls" von A1.

2.2 Technische Anforderungen an Systeme

2.2.1 Authentifizierung

Daten und sonstige in Systemen / Applikationen enthaltene Inhalte dürfen erst nach erfolgreicher Authentifizierung der User bzw. Zielsysteme ausgegeben werden. Die Authentifizierung eines Users soll mit einem „Verzeichnisdienst", wie beispielsweise Active Directory (AD), erfolgen. Das AD ist die „Zentrale Benutzerdatenbank" bei A1. Durch die Kerberos Authentifizierung wird auch Single-Sign-On (SSO) realisiert. Sollte die Nutzung von Kerberos / SSO nicht möglich sein, ist eine Authentifizierung von Benutzerinnen und Benutzern auch mit alternativen Systemen zulässig, sofern sie den Anforderungen an Passwörter gemäß den A1 internen Vorgaben (A1 Information Security Guidelines, Kapitel 3 – „Passwörter") entsprechen. Jedenfalls muss jede angelegte Benutzerin und jeder angelegte Benutzer auch im Corporate Directory (CD) geführt werden.

Passwörter müssen verschlüsselt im Filesystem bzw. in der Datenbank gespeichert und im Netz übertragen werden, um das Risiko des Passwort-Diebstahls zu verringern. Hierzu dürfen nur State-of-the-Art Verfahren verwendet werden. Eine Passwortspeicherung und -übertragung im Klartext ist nicht zulässig.

Erfolgt der Zugang von außerhalb des Unternehmensnetzwerkes, muss die Authentifizierung höheren Schutzanforderungen gerecht werden. Eine Zwei-Faktor-Authentifizierung mit dem A1 Account und zugehörigem Passwort, sowie einem weiteren Faktor, wie beispielsweise einem Zertifikat, einem SMS-Token oder einem RSA-Token, wird gefordert.

2.2.2 Hardening

Nicht benötigte Ports, Schnittstellen und Services sind zu deaktivieren. Eine Beschreibung der benötigten Ports ist zu dokumentieren. Systeme werden frei von bekannten Sicherheitsmängeln an den A1 Betrieb übergeben. Default Passwörter müssen vor der Übergabe an den A1 Betrieb geändert werden. Bei allen Systemen in der A1 muss die Verwendung des Standard Virenschutzes, den A1 einsetzt, möglich sein. Da diese Regelung auch für zugekaufte Systeme gilt, können sich Lieferanten vor einer Implementierung die notwendigen Informationen dazu einholen.

Die gesetzten Hardening-Maßnahmen und der Patch-Stand werden durch Vulnerability Scans von A1 regelmäßig überprüft.

2.2.3 Logging

Die A1 internen Anforderungen an das Logging (A1 Information Security Guidelines, Kapitel 7 – „Logging") müssen eingehalten werden. Im Idealfall werden auch Systeme, deren Betrieb ausgelagert wurde, in die zentrale Angriffserkennung eingebunden. Die Durchführung forensischer Analysen sollte ohne Zutun eines Lieferanten möglich sein.

2.2.4 Datensicherung

Die A1 internen Anforderungen an die Datensicherung (A1 Information Security Guidelines, Kapitel 8 – „Datensicherung") müssen eingehalten werden. Bei ausgelagerten Systemen wird der Lieferant dazu verpflichtet, entsprechende Datensicherungen und Wiederherstellungsmöglichkeiten zu garantieren.

2.2.5 Architekur

Applikationen sind in mehreren Tiers aufzubauen, die sicher voneinander zu trennen sind, beim Zugriff darf kein Tier übersprungen werden. Der Zugriff von einem Tier zum nächsten darf nur über definierte Protokolle (Ports) erfolgen. Es muss eine Trennung in Test-, Integrations- und Produktivsysteme erfolgen. Entwicklerinnen und Entwickler haben – ohne ausdrückliche schriftliche Erlaubnis seitens A1 - keinen Zugriff auf Produktivsysteme. Wird der Einsatz von Simple Network Management Protocol (SNMP) benötigt, so ist vorzugsweise SNMPv3 zu verwenden. Ältere Versionen von SNMP sollten nicht eingesetzt werden.

2.2.6 Softwareentwicklung

Bei der Entwicklung von Software soll nach entsprechenden Normen (z.B. ÖNORM A7700 in der aktuellen Version) oder dem OWASP Guide[2] vorgegangen werden. Jedenfalls sind die OWASP Top 10 Application Security Risks zu berücksichtigen.

2.2.7 Administration

Eine direkte Verbindung auf ein System zum Zwecke der Administration ist nur innerhalb des A1 Netzwerkes erlaubt. Soll die Administration von außerhalb (des A1 Netzwerkes) erfolgen, darf nur eine Verbindung über festgelegte Ports der Firewall zu einem Zugangspunkt in der Demilitarized Zone (DMZ) möglich sein, von dem aus man sich dann auf das jeweilige Ziel-System weiter verbinden kann (Remote-Zugriffe von Servicepartnerinnen und Servicepartnern terminieren in einer gesonderten Zone.) Eine solche Verbindung muss verschlüsselt erfolgen und eine vorhergehende Authentifizierung ist erforderlich. Servicepartnerinnen und Servicepartner sind nicht berechtigt,

[2] Hier geht es zum OWASP Guide.

Wartungsarbeiten und damit den Zugang zum A1 Netz ohne ausdrückliche Zustimmung des Auftraggebers an Dritte zu übertragen.

2.2.8 Datenlöschung

Kunden-, Verkehrs- oder andere schützenswerte Daten sind nach gesetzlichen und internen Vorgaben der A1 zeitgerecht und regelmäßig zu löschen. In der Design Phase werden auf das jeweilige System angepasste Anforderungen zur Löschung von A1 spezifiziert. Jedenfalls hat jeder Lieferant die Daten zu löschen, wenn diese nicht mehr zur Erfüllung der vertraglichen Pflichten benötigt werden.

2.2.9 Penetration Testing

In der Testphase, spätestens vor der Abnahme, werden Systeme mit einem Tool auf Sicherheitsmängel untersucht. Werden dabei Mängel festgestellt, sind sie unverzüglich zu beheben. Lieferanten dürfen für die Behebung keine zusätzlichen Kosten in Rechnung stellen.

2.2.10 Vulnerability Management

Die Produkte bzw. Systeme oder Applikationen müssen in einem gehärteten und aktuell gepatchten Zustand geliefert bzw. implementiert werden. Vor Inbetriebnahme wird ihr Zustand mittels Vulnerability Scans sichergestellt. Für Sicherheits-Schwachstellen, die nach Inbetriebnahme entdeckt werden, muss der Lieferant notwendige Updates kostenfrei zur Verfügung stellen.

Prinzipiell gilt, dass Hersteller und Lieferanten spätestens eine Woche nach öffentlicher Bekanntgabe auf Security Plattformen (z.B.: CERT, SecurityTracker, Heise, ...) oder in einem Zeitraum, der im Underpinning Contract (UC) definiert ist, Security-Patches bereitstellen müssen.

Werden von A1 Schwachstellen identifiziert, sind sie innerhalb von zwei Wochen zur Verfügung zu stellen. Es muss die automatisierte Möglichkeit geben, heruntergeladene Patches bzw. Software Updates auf ihre Integrität zu prüfen.

Services, die in ihrer Kritikalität hoch bewertet werden (Serviceklasse 4), werden zusätzlich einer Source-Code Analyse unterzogen.

2.2.11 Incident Management

Sicherheitsvorfälle beim Auftragnehmer müssen, im Rahmen der Vertragserfüllung, unverzüglich an A1 gemeldet werden.

2.3 Anforderungen an Internet of Things (IoT) Services

Die IoT-Sensoren (z.B.: Kameras, Smart Meter, Steckdosen, ...) dürfen nicht direkt aus dem Internet erreichbar sein.

Für die IoT Sensoren sind über die gesamte Lebenszeit des Produktes Security Updates automatisiert und ohne manuellen Eingriff durchzuführen.

In den IoT-Sensoren sind keine hardcoded Passwörter erlaubt. Default Passwörter der IoT-Sensoren müssen bei Inbetriebnahme geändert werden. Wo technisch möglich und praktikabel, muss für Kundenschnittstellen eine 2-Faktor-Authentifizierung angeboten werden.

Im gesamten Produktlebenszyklus der Gesamtlösung gelten die Grundsätze von Security by Default und Security by Design.

2.4 Anforderungen an Cloud Service Provider

Von Cloud Service Providern wird ein Cloud Computing verlangt, welches EU General Data Protection Regulation (GDPR) konform ist. Zudem werden folgende Zertifizierungen eingefordert, die auf die gesamte Dauer der Partnerschaft bzw. der Nutzung des Services aufrecht zu erhalten sind:

- ISO/IEC 27001 (Informationssicherheit) und ISO/IEC 27018 (PII-Daten in der Cloud) des Service Providers
- ISAE 3402-Konformität des Rechenzentrums bei externer Datenspeicherung

Der Service Provider hat entsprechende Nachweise zu erbringen, um die Zertifizierungen zu belegen. Bei Nichtvorlage von gültigen Zertifikaten für ISO/IEC 27001, ISO/IEC 27018 und ISAE 3402 können andere Zertifizierungen angerechnet werden, wenn sie gleich- oder höherwertig sind. Beispielsweise wird ein 5-Sterne-StarAudit-Zertifikat von EuroCloud[3] angerechnet, welches ebenfalls die Einhaltung genereller Vorgaben an Cloud Provider garantiert.

Cloud Services werden geprüft. Bei Einhaltung der Mindestanforderungen und entsprechenden vertraglichen Vereinbarungen zur Wahrung der Sicherheit der Informationen und Daten werden sie für die Nutzung freigegeben. Ungeprüfte Cloud Services dürfen nicht genutzt werden.

[3] Hier sind nähere Informationen zu dem 5-Sterne-StarAudit-Zertifikat von EuroCloud zu finden.

3 Anforderungen bei Auslagerung von Systemen

3.1 Vertragliche Anforderungen an Dienstleister bei Auslagerung

3.1.1 Underpinning Contract (UC)

Bei Auslagerung von Systemen müssen Underpinning Contracts (UCs) vertraglich vereinbart werden. Eine Zuständigkeitsmatrix der jeweiligen Leistungen muss vertraglich vereinbart werden.

3.2 Organisatorische Anforderungen an Dienstleister bei Auslagerung

3.2.1 Security Konzept

Wenn ein System oder Systemteile an einen Lieferanten ausgelagert werden, hat der Dienstleister ein Sicherheitskonzept über die Sicherheit der Daten vorzulegen, welches von A1 im Rahmen der Angebotsverhandlungen bewertet wird.

3.2.2 Personalmanagement

Der Dienstleister muss bei seinen Mitarbeiterinnen und Mitarbeitern eine Sicherheitsüberprüfung bei Einstellung durchführen, wenn sie für Zwecke des Vertrags mit A1 eingesetzt werden. Als Mindestanforderung sind die Identitätsprüfung und die Einholung eines aktuellen polizeilichen Führungszeugnisses verpflichtend. Der Dienstleister muss gültige Vertraulichkeitsvereinbarungen mit ihnen abschließen und sie im korrekten und verantwortungsbewussten Umgang mit Informationen und Daten der A1 schulen bzw. instruieren. Verantwortlichkeiten hinsichtlich der Informationssicherheit und des Datenschutzes müssen definiert sein. Der Dienstleister muss für diese Zwecke entsprechende Richtlinien oder Dienstanweisungen zu Informationssicherheit und zu Datenschutz veröffentlicht und seinen internen und externen Mitarbeiterinnen und Mitarbeitern zugänglich gemacht haben. Sie müssen ausreichend ausgebildet und geschult sein, um die Tätigkeiten für die Partnerschaft mit A1 entsprechend verrichten zu können. Engpässe hinsichtlich personeller Ressourcen sind beispielsweise durch personelle Redundanzen und Stellvertretungsregelungen zu vermeiden, sodass die Erbringung der Dienstleistung an A1 nicht darunter leiden kann.

4 Datenspeicherung & Datentransfer

4.1 Datenspeicherung innerhalb der A1

Prinzipiell ist eine lokale Datenspeicherung bei A1 in inländischen Rechenzentren, soweit wirtschaftlich vertretbar, zu bevorzugen.

4.2 Datenspeicherung außerhalb der A1

Jede Datenspeicherung außerhalb von A1 bedeutet, dass sich die Daten nicht mehr in der Einflusssphäre von A1 befinden und damit der unmittelbaren Kontrolle von A1 entzogen sind. Das setzt voraus, dass erhöhte Sicherheitsanforderungen zu beachten sind. Werden Mindeststandards nicht erfüllt, ist die Datenspeicherung außerhalb von A1 unzulässig. Zudem muss in jedem Fall eine A1 interne Risikobewertung (rechtlich, datenschutzrechtlich, technisch und wirtschaftlich) erfolgen. Sind Daten betroffen, die von A1 im Auftrag unserer Kundinnen und Kunden als Dienstleister außerhalb unserer Rechenzentren verarbeitet werden, sind die betroffenen Kundinnen und Kunden in jedem Fall aus Transparenzgründen entsprechend zu informieren.

4.2.1 Mindeststandards für externe Datenspeicherung

Jede Datenspeicherung von im Geschäftsbetrieb von A1 anfallenden Daten außerhalb von A1 setzt voraus, dass eine nachweisliche wirtschaftliche, rechtliche, datenschutzrechtliche und technische Beurteilung und Risikoabwägung erfolgt ist. Die Risikobeurteilung erfolgt in Abstimmung der jeweils mit dem Thema befassten Fachbereiche und ist entsprechend den dort etablierten Prozessen zu dokumentieren. Erst dann darf eine Überlassung der Daten an einen Dienstleister erfolgen. Auch die Datenspeicherung bei Konzernunternehmen ist davon betroffen (TAG, AMEX), welche wie jeder andere Dienstleister zu betrachten sind. Werden Mindestanforderungen nicht erfüllt, ist eine externe Datenspeicherung untersagt. Eine Datenspeicherung außerhalb von A1 (z.B.: bei Cloud Services) ist dann erlaubt, wenn damit datenschutzrechtlichen Bestimmungen nicht widersprochen wird und explizit eine Freigabe für die Nutzung ausgesprochen wurde.

Vertrauliche Informationen dürfen nur verschlüsselt übertragen und extern gespeichert werden.

Unternehmenskritische und geheime Informationen dürfen prinzipiell nicht extern gehostet werden. Nur in Sonderfällen dürfen sie, bei einer entsprechenden Freigabe, in verschlüsselter Form außerhalb der A1 gespeichert werden, wobei sich der Schlüssel ausschließlich bei A1 befinden muss. Insbesondere bei Daten mit Bezug auf Kundinnen und Kunden ist Vorsicht geboten, da gegebenenfalls zusätzlich datenschutzrechtliche und vertragliche Verpflichtungen zu berücksichtigen sind.

Datenspeicherung & Datentransfer

Die nachfolgende Matrix stellt dar, welche Daten extern gespeichert werden dürfen, vorausgesetzt, die Mindeststandards werden eingehalten:

EXTERNE DATENSPEICHERUNG GEM. A1 INFORMATIONSKLASSEN

	INFORMATIONSKLASSE	A1	extern (AUT, EU & sichere Drittstaaten oder genehmigungspflichtige Drittstaaten)
	öffentlich	✓	✓
	intern	✓	✓
	vertraulich	✓	✓ (mit Verschlüsselung)
A/B/C	unternehmenskritisch	✓	✗ (nur in Ausnahmefällen)
A/B/C	→ davon: sensible Daten	✓	✗
A/B/C	→ davon: Inhaltsdaten (Inhalte übertragener Nachrichten)	✗	✗
	geheim	✓	✗ (nur in Ausnahmefällen)

Der Anbieter des Rechenzentrums, bei dem die externe Speicherung erfolgt, muss eine ISAE 3402 Konformität bestätigen oder eine gleich- bzw. höherwertige Zertifizierung vorweisen.

4.2.2 Laufende Überprüfung

Bei jeder größeren technischen Anpassung oder Änderung, sowie bei jeder inhaltlichen Vertragsänderung, zumindest aber standardmäßig alle drei Jahre, ist von den involvierten Fachbereichen zu überprüfen, ob sich der für die externe Datenspeicherung maßgebliche Sachverhalt geändert hat und eine Anpassung erforderlich ist. Soweit noch nicht vorhanden, sind von den betroffenen Fachbereichen entsprechende Prozesse zu implementieren.

4.2.3 Extern gespeicherte Kundinnen- & Kundendaten und Daten mit Personenbezug

Werden im Auftrag der Kundin oder des Kunden Daten durch A1 verarbeitet oder gespeichert (z.B.: bei Hosting oder bei Housing), und sollte die Verarbeitung bzw. Speicherung außerhalb der Rechenzentren von A1 (z.B. bei Cloud Service Providern als Subdienstleistern) erfolgen, ist die nachweisliche Zustimmung der Kundin bzw. des Kunden einzuholen. Die Zustimmung kann in Form einer individuellen Vertragsgestaltung, einer Klausel in der Leistungsbeschreibung, oder auf elektronischem Wege (z.B. im Online-Shop) geschehen. Auf diese Weise ist die Transparenz der Datenspeicherung (auch außerhalb von A1) für die Kundin bzw. für den Kunden gewährleistet, sodass sie bzw. er ihren bzw. seinen datenschutzrechtlichen Melde- und Genehmigungspflichten nachkommen kann.

Datenspeicherung & Datentransfer

Sollen Kundinnen- und Kundendaten im Sinne des TKG oder personenbezogene Daten, die im Geschäftsbetrieb von A1 anfallen, außerhalb von A1 gespeichert und /oder verarbeitet werden, so ist vorab festzulegen, in welchem Land die Speicherung der Daten erfolgen wird. Befinden sich die Daten in weiterer Folge im Europäischen Wirtschaftsraum oder in sicheren Drittstaaten, ist der Datentransfer ohne Genehmigung durch die Datenschutzbehörde erlaubt (gegebenenfalls gelten zusätzliche Sicherheitserfordernisse). In allen anderen Fällen ist, sofern die Daten für die Empfängerin bzw. für den Empfänger nicht nur indirekt personenbezogen sind, eine Genehmigung der Datenschutzbehörde einzuholen. Das Verfahren vor der Datenschutzbehörde wird von der Abteilung National Data Privacy durchgeführt. Ein Zugriff auf Daten aus dem Ausland (außerhalb des Europäischen Wirtschaftsraumes oder sicheren Drittstaates) ist hinsichtlich der Genehmigungspflicht einer Speicherung der Daten im Ausland gleichzusetzen.

Zu sicheren Drittstaaten zählen:

- Schweiz
- Argentinien
- Guernsey
- Isle of Man
- Jersey
- Färöer Inseln
- Andorra
- Uruguay
- Neuseeland
- Kanada
- Israel

5 Publikation & inhaltliche Verantwortung

Die A1 Information Security Guidelines können nach Freigabe und Verabschiedung im Intranet[4] von A1 eingesehen werden.

Der Inhalt wurde erstellt von:
Security Governance & Risk Management
security@a1telekom.at

[4] Die bestehenden Sicherheitsrichtlinien sind unter A1 Inside/Wissen/Sichere Daten abrufbar.