Informationssicherheit

Übergreifende Richtlinien und Prozesse

Regelung Nr. 03.01.16

Dienstleistung durch Dritte

Klassifikation: Intern – KSU 2.1

Geltungsbereich: Die Regelungen gelten für die AUDI BRUSSELS

Version 1.1

Inhalt

I. Zweck

Bei der AUDI BRUSSELS arbeiten externe Dienstleister im Rahmen von Outtasking- (z.B. externe Beratung) oder Outsourcing-Vorhaben (z.B. externes Hosting). Um Informationen umfassend schützen zu können, müssen externe Dienstleister Sicherheitsregelungen und gesetzliche Anforderungen einhalten. Die vorliegende Regelung legt spezifische Anforderungen an die Informationssicherheit und an Vorgaben für alle Phasen von Outtasking- und Outsourcing-Vorhaben fest.

Im Sinne dieser Regelung bezeichnet der Begriff Informationssicherheit die IT-Sicherheit als Bestandteil der ganzheitlichen Informationssicherheit.

1. Dienstleistung durch Dritte

1.1. Ziel

Die vorliegende Regelung legt Sicherheitsanforderungen fest, die bei der Arbeit mit externen Dienstleistern (Dritten) implementiert werden müssen, um zu gewährleisten, dass das Informationssicherheitsniveau innerhalb der AUDI BRUSSELS und des VW-Konzerns nicht gesenkt wird. Die Anforderungen dieser Regelung gelten für alle Arten der Dienstleistungserbringung und alle Auftragnehmer.

Bevor der Auftrag für Dienstleistungen an einen externen Dienstleister vergeben wird, muss ein Prozess bzw. Maßnahmen ein geeignetes Maß an Sicherheit und die Einhaltung interner Regelungen sicherstellen.

Es muss gewährleistet werden, dass die Interessen der Informationssicherheit, des Datenschutzes und der Unternehmenssicherheit adäquat wahrgenommen werden.

Der verantwortliche Fachbereich muss mit geeigneten Maßnahmen sicherstellen, dass die folgenden Anforderungen (Kapitel 1.2 – Kapitel 1.4) berücksichtigt werden:

1.2. Gemeinsame Anforderungen bei Outtasking und Outsourcing

1.2.1 Allgemeine Anforderungen

- Es muss ein Verfahren zur Beauftragung eines Outtasking- und Outsourcing-Vorhabens (im Folgenden allgemein "Vorhaben" genannt[1]) mit Rollen und Verantwortlichkeiten definiert, dokumentiert und etabliert werden.
- Für sicherheitskritische Vorhaben (Vorhaben mit Zugang zu personenbezogenen, vertraulichen oder geheimen Daten) muss ein Verfahren definiert, dokumentiert und etabliert werden, mit dem die Vertrauenswürdigkeit der Mitarbeiter, die der Dienstleister einsetzen wird, geprüft werden kann (z. B. Zusicherung polizeilicher Führungszeugnisse oder Zusicherung der Vertrauenswürdigkeit durch den Dienstleister im Rahmen des Vertrags).
- Die Eigentümer der Daten müssen in die Entscheidung zu Outtasking-/Outsourcing-Vorhaben involviert werden.

[1]Ein Vorhaben endet, wenn der Vertrag ausläuft, gekündigt wird und alle Migrationsschritte abgeschlossen sind.

- Es muss regelmäßig überprüft werden, ob die für das Vorhaben relevanten Anforderungen an die Informationssicherheit[2] von den beauftragten Dritten eingehalten werden. Hierfür ist ein Verfahren[3] sicherzustellen.
- Organisatorische und technische Änderungen innerhalb der AUDI BRUSSELS und auch des gesamten VW-Konzerns, die für Dritte von Bedeutung sind (z. B. Versionsänderungen von Systemen, Änderungen von Regelungen) sind den davon betroffenen Dritten mitzuteilen.
- Dritte müssen aufgefordert werden, sämtliche Änderungen mit Relevanz für die beauftragte Dienstleistung an den Auftraggeber zu melden.
- Wenn personenbezogene Daten von Dritten verarbeitet werden, hat AUDI BRUSSELS dafür Sorge zu tragen, dass anwendbare geltende gesetzliche und unternehmensspezifische Anforderungen eingehalten werden. Zusätzliche Regelungen bzgl. Cloud Computing in Kapitel 1.4 sind zu beachten.
- Der/Die Dritte muss sicherstellen, dass die erforderlichen Maßnahmen zur technischen und organisatorischen Sicherheit für die Verarbeitung personenbezogener Daten unter Einhaltung der entsprechenden Regelungen implementiert werden[4].
- Zusätzliche Security Anforderungen[5] müssen eingehalten werden.
- Bei der Verarbeitung von Daten auf „Nicht-Audi-Systemen“ durch Dritte welche als „geheim“ oder „vertraulich“ klassifiziert sind oder wenn eine Datenfernübertragung in das Netzwerk von AUDI BRUSSELS oder der VW-Gruppe gibt, ist eine schriftliche Bestätigung der Erfüllung der Anforderungen des VDA-ISA einzuholen Eine detaillierte Übersicht wann eine solche Überprüfung notwendig ist und welcher Prüfumfang erforderlich ist, findet sich in Anhang B.1.6. Der Dritte muss hierfür ein gültiges TISAX Assessment (http://enx.com/tisax/tisax-en.html) vorweisen. Dies muss für alle Standorte und Partnerunternehmen verfügbar sein, an denen Daten der AUDI BRUSSELS verarbeitet und / oder gespeichert werden bzw. entsprechende Dienstleistung erbracht wird. Der auftraggebende Fachbereich ist verantwortlich den entsprechenden Nachweis einzufordern und dass über den kompletten Zeitraum der Beauftragung die Gültigkeit gewährleistet wird. Weitere Informationen finden sich unter Anhang A.1.10.

1.2.2 Management externer Dienstleister im Rahmen des Projektmanagements

- Für jedes Outtasking- und Outsourcing-Vorhaben muss der verantwortliche Fachbereich einen Verantwortlichen[6] bestimmen, die für die Einhaltung der Anforderungen in den Phasen "Planung und Konzeption", "Detailplanung", "Migration", "Betrieb" sowie "Fertigstellung" zuständig sind.
- Jede Anforderung an die Informationssicherheit, die der Dienstleister im Rahmen des Vorhabens zu erfüllen hat, muss definiert und dokumentiert werden (z. B. relevante Sicherheitsregelungen und vorhabenspezifische Auflagen).

---

[2] Siehe Kapitel 1.2.2

[3] z.B. im Rahmen des Projektmanagementprozesses

[4] Siehe Anhang B.1.2

[5] Siehe Anhang A.1.7

[6] Projektmanager oder ähnliches

- Jeder Unterauftragnehmer mit Relevanz für das Vorhaben muss von AUDI BRUSSELS und dem Eigentümer der Daten freigegeben werden.
- Die dokumentierten Anforderungen an die Informationssicherheit gelten auch für Unterauftragnehmer des Dienstleisters.
- Es sollte eine Konzernmethodik gewählt werden, die ein standardisiertes Management von Dienstleistern sicherstellt[7].

1.2.3 Auswahl von Dienstleistern

- Es dürfen nur Dienstleister gewählt werden, die über den gesamten Lebenszyklus des Vertrags die Erfüllung der Anforderungen an die Informationssicherheit gewährleisten können.
- Es muss ein standardisierter Prozess für die Auswahl von Dienstleistern in Übereinstimmung mit den Sicherheitsregelungen implementiert werden[8].
- Wenn personenbezogene Daten verarbeitet werden, dürfen nur Dienstleister ausgewählt werden, die die Anforderungen des Datenschutzes erfüllen. Die Freigabe muss einem definierten Prozess unter Berücksichtigung der Datenklassifizierung und des Orts der Dienstleistung folgen.
- Vor Vertragsabschluss sicherheitskritischer Vorhaben und von Vorhaben im Zusammenhang mit der Verarbeitung personenbezogener Daten muss mittels des definierten Verfahrens[9] die Vertrauenswürdigkeit der Mitarbeiter sichergestellt werden, die der Dienstleister einsetzen wird.
- Für externes Hosting gelten zusätzliche Anforderungen[10].

1.2.4 Vertragsabschluss

Verträge mit Dienstleistern müssen mindestens Folgendes enthalten:

- Alle für den Dienstleister relevanten Anforderungen an die Informationssicherheit des Vorhabens
- Implementierte Sicherheitsmaßnahmen der Dienstleister mit Relevanz für den Vertrag[11]
- Anforderungen an die Art und Weise des Informationsaustauschs zwischen den Vertragspartnern
- Eigentums- und Nutzungsrechte der Informationen, die im Rahmen des Vorhabens

- dem Dienstleister zur Verfügung gestellt werden
- vom Dienstleister erstellt werden oder
- an den Dienstleister ausgelagert werden

[7] z.B. Leistungsbaukasten

[8] Siehe Anhang B.1.3

[9] Siehe Kapitel 1.2.1

[10] Siehe Kapitel 1.4

[11] Gemäß Anhang A.1.7

- Mitwirkungs- und Sorgfaltspflichten des Dienstleisters, die mindestens folgende Aspekte umfassen müssen:

- Geheimhaltung (NDA[12])
- Einhaltung der für das Vorhaben geltenden Gesetze (z. B. GDPR)
- Einhaltung aller relevanten Anforderungen der Unternehmensregelungen zur Informationssicherheit
- Zusicherung der Vertrauenswürdigkeit der externen Mitarbeiter des Vorhabens
- Zusicherung, dass die externen Mitarbeiter des Vorhabens ausreichende Schulungen zu den für ihre Aufgaben relevanten Informationssicherheitsrisiken erhalten haben

- Anforderung, dass der Dienstleister regelmäßig Berichte über Vorfälle, Änderungen, Risiken und Dienstleistungsunterbrechungen an die genannte verantwortliche Person der Konzerngesellschaft übermitteln muss. Zusätzlich muss der Dienstleister diese Person direkt über größere Vorfälle und Sicherheitsschwachstellen informieren (je nach Kritikalität des Vorfalls/der Schwachstelle).
- Pflichten bei regulärer und außerordentlicher Vertragsbeendigung, die mindestens folgende Aspekte umfassen müssen:

- Vollständige Übergabe aller Ergebnisse, Informationen und Tools, die für die Fortführung des Vorhabens benötigt werden (z. B. Dokumentationen oder Verfahrensbeschreibungen) oder für den Audi Konzern innerhalb einer definierten Periode relevant sind
- Rückgabe von Hard- und Software, die Eigentum der AUDI BRUSSELS sind
- Sichere Löschung von Passwörtern und Benutzerkennungen, die den Zugang zur IT des Audi Konzerns ermöglichen, aus Systemen des externen Dienstleisters
- Rückgabe von Eigentum (insbesondere Token, Zutrittskarten, Schlüssel, …)
- Sicheres Löschen aller Datenbestände des Vorhabens beim Dienstleister[13]

- Pflichten bei der Beauftragung von Unterauftragnehmern, die mindestens folgende Aspekte umfassen müssen:

- Einholen der Zustimmung für den Einsatz genannter Unterauftragnehmer für definierte Aufgaben von der entsprechenden Konzerngesellschaft
- Verpflichtung des Unterauftragnehmers auf die Erfüllung aller Anforderungen, die auch der direkte Auftragnehmer zu erfüllen hat
- Regelungen bezüglich Haftung und Vertragsverletzungen

- Rechte und Erlaubnis zur Durchführung von Audits beim Dienstleister. Der Dienstleister muss auch die Erlaubnis für Audits beim Unterauftragnehmer sicherstellen.

[12] Vertraulichkeitsvereinbarung

[13] Siehe Anhang A.1.2

- Zusätzliche Security Anforderungen müssen eingehalten werden[14].
- Geltende unternehmensspezifische Anforderungen müssen eingehalten werden.
- Für externes Hosting gelten zusätzliche Anforderungen[15].

1.2.5 Betrieb während der Laufzeit des Vertrags

- Während des Betriebs müssen alle vertraglichen Anforderungen[16] eingehalten werden.
- Beide Parteien müssen eine verantwortliche Kontaktperson für das Vorhaben benennen.
- Der Verantwortliche der AUDI BRUSSELS agiert als Kontaktperson zwischen dem Vertragspartner und dem lokal Verantwortlichen für Informationssicherheit.
- Der Verantwortliche der AUDI BRUSSELS muss sicherstellen, dass die Mitarbeiter des Dienstleisters die relevanten Anforderungen an die Informationssicherheit sowie die vertraglichen Anforderungen kennen und einhalten.

1.2.6 Beendigung des Vorhabens

- Bei Abschluss des Vorhabens müssen die Anforderungen aus dem Vertrag[17] in Bezug auf die Beendigung des Vorhabens erfüllt werden. Des Weiteren müssen alle Zutritts-, Zugangs- und Zugriffsrechte unverzüglich entzogen werden[18], sofern die gesetzlich geforderte Nachvollziehbarkeit dadurch nicht eingeschränkt wird.

1.3. Zusätzliche Anforderungen für das Outsourcing

1.3.1 Planung und Konzeption

- Die für die Informationssicherheit verantwortliche Stelle[19] muss bereits bei der Planung und Konzeption eines Outsourcing-Vorhabens einbezogen werden. Dies gilt auch für weitere relevante Organisationseinheiten/Rollen (z. B. Datenschutzbeauftragte, Unternehmenssicherheit).
- Es muss eine Risikoanalyse[20] für das Outsourcing-Vorhaben durchgeführt werden. In die Risikoanalyse müssen sämtliche Informationen, Services und IT-Komponenten einbezogen werden, die von dem Outsourcing-Vorhaben unmittelbar betroffen sind. Der Outsourcing-Gegenstand muss exakt definiert werden.

1.3.2 Vertragsabschluss

- Die vertraglichen Vereinbarungen müssen Testkriterien enthalten, um die Implementierung der Anforderungen an die Informationssicherheit zu prüfen.

---

[14] Siehe Anhang A.1.7

[15] Siehe Kapitel 1.4

[16] Siehe Kapitel 1.2.4

[17] Siehe Kapitel 1.2.4

[18] Siehe Anhang A.1.3

[19] Siehe Anhang B.1.1

[20] Siehe Anhang A.1.4

- Dem Unternehmen, das für den Outsourcing-Gegenstand verantwortlich ist, muss es erlaubt sein, regelmäßige Prüfungen zur Einhaltung der Regelungen zur Informationssicherheit im Rahmen des Outsourcing-Vorhabens durchzuführen.
- Diese Prüfungen können an einen Drittanbieter ausgelagert werden.

1.3.3 Detailplanung

- Der Dienstleister muss einen Ansprechpartner und Vertreter für alle Aspekte der Informationssicherheit und des Datenschutzes festlegen.
- Sowohl der verantwortliche Fachbereich als auch der Dienstleister müssen auf der Grundlage der ermittelten Sicherheitsanforderungen ein Sicherheitskonzept für das Outsourcing-Vorhaben erstellen. In diesem Sicherheitskonzept müssen mindestens folgende Aspekte berücksichtigt werden:

- Schnittstellen zwischen AUDI BRUSSELS und Dienstleistern
- Maßnahmen für alle folgenden Phasen des Outsourcing-Vorhabens, die zur Erfüllung der Sicherheitsanforderungen notwendig sind
- Tests, mit denen die Umsetzung und Wirksamkeit der definierten Maßnahmen während und nach der Migration überprüft werden kann
- Das Sicherheitskonzept des Dienstleisters muss außerdem eine Schnittstelle zu folgenden Einheiten der AUDI BRUSSELS aufweisen:
  - Incident Management
  - Change Management
  - Informationssicherheits-Risikomanagement bzw. IT-Risikomanagement und
  - IT Service Continuity Management

- Im Rahmen der Detailplanung ist ein Migrationsplan mit Rollen und Verantwortlichkeiten zu definieren und dokumentieren, der die vollständige Implementierung der Sicherheitskonzepte umfasst.

1.3.4 Migration

- Die Umsetzung der Maßnahmen muss gemäß dem definierten Migrationsplan erfolgen.
- Eine Freigabe für die Implementierung darf erst nach erfolgreichem Abschluss der in den Sicherheitskonzepten definierten Tests erfolgen.

1.3.5 Betrieb

- Zwischen dem Verantwortlichen für das Vorhaben und dem Dienstleister muss ein regelmäßiger Informationsaustausch über den Status der Informationssicherheit (z. B. aktualisierte Regelungen, aktualisierte Anforderungen usw.) stattfinden. Der Verantwortliche der AUDI BRUSSELS muss die Anpassung des Vertrags initiieren, sofern Änderungen der Informationssicherheit oder gesetzliche Anforderungen dies erforderlich machen.
- Änderungen am Outsourcing-Gegenstand müssen vor der Umsetzung durch die zuständigen Stellen[21] freigegeben werden.

[21] Siehe Anhang B.1.1

- Der Dienstleister muss zum Implementierungsstatus regelmäßig Bericht erstatten.
- Der Dienstleister wirkt aktiv bei der Untersuchung von Sicherheitsvorfällen mit und stellt relevante Informationen zur Verfügung.
- Sämtliche durch den Dienstleister durchgeführte Tätigkeiten (z. B. Systemwartungen) sind durch diesen zu dokumentieren.
- Das Sicherheitskonzept und definierte, vertraglich vereinbarte Dienste in Zusammenhang mit der Informationssicherheit müssen mindestens einmal jährlich auf Vollständigkeit und Aktualität hin überprüft werden. Der Verantwortliche des Vorhabens und der Dienstleister sind für die Ausführung entsprechender Maßnahmen verantwortlich.
- Der Dienstleister überwacht die Wirksamkeit der implementierten Sicherheitsmaßnahmen und schlägt Maßnahmen für die Einhaltung bzw. – falls erforderlich – zur Verbesserung des Sicherheitsniveaus vor.

1.3.6 Beendigung des Outsourcing-Vorhabens

- Die Übergabe des Outsourcing-Gegenstands an einen anderen Dienstleister muss wie ein neues Outsourcing-Vorhaben behandelt werden.
- Kommt es zu einer Beendigung des Outsourcing-Vorhabens (Insourcing), müssen die Anforderungen aus den Phasen "Detailplanung" und "Migration" erfüllt werden.
- Bei der Erneuerung des Vertrags muss geprüft werden, ob die Regelungen für die Informationssicherheit und gesetzliche Regelungen weiterhin gültig sind. Ist dies nicht der Fall, müssen der Vertrag und die technischen sowie organisatorischen Sicherheitsmaßnahmen entsprechend angepasst werden.

1.4. Zusätzliche Anforderungen bei externem Hosting

Folgende Auflagen existieren zum externen Hosting von Daten:

- Informationssicherheitsregelungen der AUDI BRUSSELS müssen beachtet werden, insbesondere bezüglich Zugriffsschutz, starker Authentifikation und der Ausgestaltung von IT-Räumen. Bei einem externen Hosting vertraulicher Daten ist über die Informationssicherheitsregelungen der AUDI BRUSSELS hinaus eine Verschlüsselung des Speichermediums einzusetzen[22].
- Für das Cloud Computing müssen entsprechend der Beschreibung in der Definition von Cloud Computing[23] Anwendungen und Infrastrukturkomponenten bereitgestellt werden. Gesellschaftsspezifische Regelungen zum Einsatz von Cloud Computing in Verbindung mit personenbezogenen Daten sind zu beachten[24].
- Der AUDI BRUSSELS muss die Möglichkeit für ein Vor-Ort-Audit der Umgebung eingeräumt werden. Dies gilt auch für Unterauftragnehmer.

[22] Siehe Anhang A.1.5

[23] Siehe Anhang A.1.6

[24] Siehe Anhang B.1.5

- Der für die IT-Sicherheit verantwortlichen Stelle[25] ist eine mit der IT-Architektur abgestimmte Dokumentation der geplanten Infrastruktur vorzulegen.
- Das Vorhaben eines externen Hostings ist mit dem Eigentümer der Daten, der für die Informationssicherheit verantwortlichen Einheit, dem Datenschutz, dem Betriebsrat (falls notwendig) und der Rechtsabteilung der betroffenen Gesellschaften abzustimmen.
- Für Netzwerkverbindungen sind die Anforderungen der Regelung „Netzwerkzugänge[26] einzuhalten.
- Im Rahmen der Beauftragung muss eine Applikationssicherheitsüberprüfung durch einen unabhängigen Dritten zufriedenstellend durchgeführt werden.
- Bei einem externen Hosting von Daten ist die Zustimmung des Daten-Eigentümers einzuholen.
- Ein externes Hosting geheimer Daten ist nicht zulässig.
- Die Vorgaben aus A1.9 (IS-Requirements_Cloud) sind einzuhalten.

[25] Siehe Anhang B.1.4

[26] Siehe Anhang A.1.8

II. Verantwortlichkeiten

II.I Kapitel 1: Dienstleistung durch Dritte

Diese Regelung ist von allen Bereichen die mit externen Dienstleistern zusammenarbeiten anzuwenden und einzuhalten.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig. Bei Bedarf ist der Entscheider Kreis für Informationssicherheit mit einzubinden.

Anhang

A. Allgemeines

A.1 Mitgeltende Dokumente

A.1.1 Informationssicherheit Regelung Nr. 03.01.09 Ausnahmeprozess

A.1.2 Informationssicherheitshandlungsleitlinien für Mitarbeiterinnen und Mitarbeiter

A.1.3 Informationssicherheit Regelung Nr. 03.01.05 Authentifizierung und IAM

A.1.4 Informationssicherheit Regelung Nr. 03.01.15 Risikomanagement in der Informationssicherheit

A.1.5 Informationssicherheit Regelung Nr. 03.01.02 Kryptographie

A.1.6 Definition Cloud Computing: siehe Regelung Nr. 03.01.16 Dienstleistung durch Dritte - Anhang Cloud Computing A1 zur Regelung Nr. 03.01.16

A.1.7 siehe A.1.2 und URLB_007 Werksicherheit

A.1.8 Informationssicherheit Regelung Nr. 03.02.04 Netzwerkzugänge

A.1.9 IS-Requirements_Cloud

A.1.10 Information-Security-Wiki

A.2 Referenzen zu Standards

Die folgende Tabelle zeigt die Referenzen zu den Standards ISO/IEC 27001:2013, ISO/IEC 27001:2005 und VDA.

Thema	Kapitel	ISO 27001:2013	ISO 27001:2005	VDA(2014)
Monitoring and review of supplier services	1.2, 1.3	A.15.2.1	A.10.2.2	15.2
Managing changes to supplier services	1.2, 1.3	A.15.2.2	A.10.2.3	-

A.3 Anlagen

A.3.1 Anlage 1 Feedbackformular

Das Feedbackformular für Änderungsvorschläge zu Regelungen kann von der MyNet-Webseite Gesellschaften → Audi Brussels → Organisation → Finanz (B/F) → IT (B/FP) → IT-Sicherheit → Regelwerk heruntergeladen werden.

Das Feedback-Formular ist folgendermaßen auszufüllen:

Die Spalten 2 bis 6 müssen für jede vorgeschlagene Änderung ausgefüllt werden. Änderungen, für die nicht alle Spalten 2 bis 6 ausgefüllt sind, werden automatisch ohne weitere Prüfung abgelehnt.

Spalte 3: Folgende Kommentararten sind möglich: a=allgemein, f=fachlich, r=redaktionell

Spalte 4: Bitte bisherigen Text, Tabelle oder Bild einfügen

Spalte 5: Bitte vollständig umformulierten Text, geänderte Tabelle oder geändertes Bild einfügen

Spalte 6: Bitte begründen Sie die gewünschte Änderung möglichst ausführlich.

Bitte senden Sie das ausgefüllte Formular an: it-security.audibx@audi.de

A.4 Abkürzungen und Definitionen

In diesem Abschnitt werden ausschließlich Begriffe und Abkürzungen aus dem Informationssicherheitsbereich definiert. Begriffe und Abkürzungen aus anderen Bereichen werden durch die dafür verantwortlichen Stellen definiert.

Term	Definition
Audit	Systematische Untersuchung und Bewertung von Prozessen in Bezug auf das Erfüllen von Anforderungen und Richtlinien durch Experten hinsichtlich spezifizierter Prüflisten. Der Audit ist ein systematischer, unabhängiger und dokumentierter Prozess zum Erreichen von Nachweisen und ihrer objektiven Evaluierung in welchem Maße die Kriterien erfüllt sind.
CISO	Chief Information Security Officer
IT Service Continuity Management	Management Methode, die anhand eines Lebenszyklus-Modells die Fortführung der IT Services unter Krisenbedingungen oder zumindest unvorhersehbar erschwerten Bedingungen absichert. Es beinhaltet unter anderem die Entwicklung von Strategien, Plänen und Handlungen, um Tätigkeiten oder Prozesse – deren Unterbrechung der Organisation ernsthaften Schaden oder vernichtende Verluste zufügen würden – zu schützen bzw. alternative Abläufe zu ermöglichen.

IT-Risikomanagement	Dem Risikomanagement des Unternehmens untergeordnet.
ITSG	IT Security Governance
Sicherheitsvorfall	Ein Sicherheitsvorfall ist jedes Ereignis bezogen auf Informationssicherheit, das an eine zentrale CERT-Hotline oder an ein CERT gemeldet wurde und dort weiter verfolgt/protokolliert wird.
Risikoanalyse	Prozessschritt des Risikomanagements, zur Identifikation und Bewertung der identifizierten Gefahren hinsichtlich ihrer Eintrittswahrscheinlichkeiten und möglichen Auswirkungen betrachtet. (ISO 31000:2009)
Schwachstelle / Vulnerability	Eine Schwachstelle ist die ausnutzbare Bedrohung eines oder mehrerer Assets. Eine fehlende Maßnahme ist ebenfalls eine Schwachstelle.
Token	Ein Token ist eine Hardwarekomponente mit deren Hilfe Personen Identifiziert und Authentifiziert werden können. Mit Hilfe von Tokens kann die Anforderung Wissen und Besitz für die Umsetzung einer starken Authentifizierung realisiert werden.

A.5 Gültigkeit

Diese Regelung ist mit der Veröffentlichung sofort gültig.

Bereits bestehende Ausnahmeregelungen sind spätestens bei der nächsten Änderung (z.B. Verlängerung, Änderung der Auflagen) an diese Regelung anzupassen.

Nächster Überprüfungstermin: 01.10.2023

Für die Meldung von Änderungswünschen verwenden Sie bitte das vorgegebene Formular[27].

[27] Siehe Anhang A.3.1 Anlage 1 Feedbackformular

A.6 Dokumentenhistorie

Version	Name	Org.-Einheit	Datum	Bemerkung
1.0	Andreas Walter	B/FP	07.08.2019	Veröffentlicht
1.1	Andreas Walter	B/FP	01.10.2020	Anapassung Kapitel 1.2.1 und 1.4

B. Spezifische Ausprägungen

B.1 Kapitel 1: Dienstleistung durch Dritte

B.1.1 IT-Sicherheit, (Je nach Bedarf unter Einbindung des Entscheiderkreises für Informationssicherheit)

B.1.2 URLB_016 Datenschutz – Schutz personenbezogener Daten / Einbindung DPO

B.1.3 keine weiteren Details

B.1.4 IT-Sicherheit

B.1.5 Die Speicherung oder Verarbeitung von personenbezogenen Daten durch cloud-basierte Anwendungen oder Infrastrukturkomponenten ist nur unter Einhaltung der EU-Datenschutzverordnung und den Datenschutzbestimmungen der jeweiligen Länder zulässig.

B.1.6 Die folgende Tabelle zeigt wann eine Überprüfung notwendig ist und gibt den erforderlichen Prüfumfang an:

Kategorie/ Klassifizierung	**Prüfumfang und –tiefe, TISAX Label**
Intern	Keine Bewertung erforderlich
Vertraulich / hoher Schutzbedarf bzgl. Integrität und Verfügbarkeit	TISAX Assessment Level 2 (Plausibilitätsprüfung) Basis VDA ISA Modul „Informationssicherheit“, Schutzbedarf „hoch“ TISAX Label „Info High“
Geheim / sehr hoher Schutzbedarf bzgl. Integrität und Verfügbarkeit	TISAX Assessment Level 3 (Vorort-Prüfung) Basis VDA ISA Modul „Informationssicherheit“, Schutzbedarf „sehr hoch“ TISAX Label „Info Very High“
Prototypenfahrzeuge	TISAX Assessment Level 3 (Vorort-Prüfung), Basis VDA ISA Modul „Prototypenschutz“ TISAX Label “Proto Very High”
Prototypenteile, Komponenten und Aggregate	Assessment Level 2 (Plausibilitätsprüfung), Basis VDA ISA Modul „Prototypenschutz“ TISAX Label “Proto High”
Wegfahrsperren-relevante Bauteile	TISAX Assessment Level 3 (Vorort-Prüfung) sowie Anforderungen bezüglich Wegfahrsperren-relevante Bauteile Basis VDA ISA Modul „Informationssicherheit“, Schutzbedarf „sehr hoch“
Anbindung an das Unternehmensnetzwerk	TISAX Assessment Level 2 (Plausibilitätsprüfung) Basis VDA ISA Modul „Informationssicherheit“, Schutzbedarf „hoch“