Technische und organisatorische Maßnahmen (TOMs)

ecovium Holding GmbH & ecovium GmbH
Justus-von-Liebig-Straße 3
31535 Neustadt

Stand: August 2024

Inhaltsverzeichnis

A. Dokumenthistorie

Datum	Version	Beschreibung
15.08.2024	2.5	Erweiterung um relevante Änderungen seit letzter Version • Rechenzentrum Microsoft Azure (F.5): Alle Services werden ausschließlich am Rechenzentrumsstandort Europa West (Niederlande) gehostet • Das Produkt Transport Hub (D.26) wurde hinzugefügt • Das Produkt Drivers Workplace (D.4) wurde hinzugefügt • Ergänzung MFA im Kapitel Zugriffskontrolle (C.3) • Für das Produkt eCommerce Suite (D.5) wurde die Referenz auf den Standort ergänzt • Der Abschnitt zum Produkt eCommerce Suite (D.5) gilt zusätzlich für das Produkt Return Handling, das mittlerweile auch getrennt vom Produkt eCommerce Suite vermarktet wird • Produkt S-Check (OnPremise) ist obsolet (Produkt wird nicht mehr verkauft und ist nicht mehr im Einsatz)
05.04.2024	2.4	Erweiterung um relevante Änderungen seit letzter Version • Ersetzen des Rechenzentrums NetCom BW durch MS Azure (alle Services, die zuvor im Rechenzentrum NetCom BW gehostet wurden, werden ab April 2024 bei MS Azure gehostet).
31.01.2024	2.3	Erweiterung um relevante Änderungen seit letzter Version • Gültigkeit der TOMs (Abschnitt C) • Trennungskontrolle (Abschnitt C.4) • Produkt eCommerce Suite (Abschnitt D.4) • Produkt Transroad (Abschnitte D.26 und D.27) • Produkt V-LOG (Abschnitt D.31)

14.07.2023	2.2	Kleinere Anpassungen
16.05.2023	2.1	Erweiterung um kleinere Rechenzentren
17.04.2023	2.0	Komplett überarbeitete Version unter Berücksichtigung aller ecovium-Standorte und ecovium-Produkte
08.11.2022	1.1	Aufgliederung der TOMs in die Bereiche Allgemein, Produkte, Standorte, Rechenzentren und Fernwartung.
30.06.2022	1.0	Erste Version nach Überführung aller Tochtergesellschaften in die ecovium GmbH

B. Einleitung

B.1 Voraussetzung

Die EU-Datenschutzgrundverordnung (DSGVO) schreibt gemäß Art. 32 vor, dass Unternehmen für die Sicherheit von Daten zu sorgen haben. Die hierfür umzusetzenden technischen und organisatorischen Maßnahmen (TOMs) sollen dabei geeignet sein, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung von Daten auf Dauer sicherzustellen. Dabei sind die Art und der Umfang der Datenverarbeitung genauso zu berücksichtigen, wie der Stand der Technik sowie die Implementierungskosten.

Dieses Dokument beschreibt von der ecovium umgesetzten TOMs. Dabei unterliegen die TOMs dem technischen Fortschritt, sodass die beschriebenen Maßnahmen kontinuierlich überprüft und ggf. angepasst werden. Die Änderungen sind in diesem Dokument jeweils zeitnah anzupassen.

B.2 Auftragsverarbeitung

Die ecovium stellt als Logistikdienstleister neben Hardware auch Software zur Verfügung. Die Software wird dabei sowohl vom Kunden selbst als On-Premise-Lösung betrieben oder auch als SaaS-Lösung von der ecovium gehostet. In beiden Installationsarten hat die ecovium bei Support, Wartung und Betrieb Zugriff auf Daten. Dies stellt eine Auftragsverarbeitung nach Art. 28 DSGVO dar.

B.3 Umgang mit diesem Dokument

Die ecovium ist in den vergangenen Jahren aus mehreren Unternehmen durch gesellschaftsrechtliche Verschmelzung entstanden. Hieraus ergeben sich je nach Unternehmensstandort teilweise unterschiedliche TOMs, die in der Zukunft sukzessive vereinheitlicht werden sollen. Aufgrund der Vielzahl der Unternehmensstandorte wird dieser Prozess jedoch einige Zeit in Anspruch nehmen. Dieses Dokument beinhaltet daher sowohl eine Beschreibung der bereits unternehmensweit vereinheitlichten als auch der standortspezifischen TOMs.

Darüber hinaus wird eine Vielzahl von Produkten und Dienstleistungen angeboten, die historisch bedingt von verschiedenen Standorten betreut bzw. in unterschiedlichen Rechenzentren gehostet werden. Daher enthält dieses Dokument jeweils produktspezifische TOMs mit Verweisen auf weiterführende TOMs zu den Standorten, den Rechenzentren sowie der eingesetzten Fernwartungstools.

Daher sollten Kunden bei der Beurteilung der TOMs zunächst die allgemeingültigen sowie die produktspezifischen Angaben bewerten. Ausgehend von den eingesetzten Produkten sind dann jeweils noch die spezifischen TOMs der Standorte, Rechenzentren und eingesetzten Fernwartungstools zu berücksichtigen.

C. Allgemeine TOMs

In diesem Abschnitt werden alle TOMs beschrieben, die unternehmensweit gelten. Darüber hinaus sind spezielle TOMs je nach Standort möglich (siehe Punkt E Standortbezogene TOMs).

Diese TOMs sind gültig für die ecovium GmbH und die ecovium Holding GmbH.

C.1 Zutrittskontrolle

Es haben ausschließlich befugte Personen Zutritt den Geschäftsräumen, dies wird je nach Standort durch Alarmanlagen und manuelle Schließsysteme mit Sicherheitsschlössern bzw. Transponderkarten mit entsprechenden Schlössern sichergestellt. Die Schlüsselausgabe für die Schließsysteme wird protokolliert. Zudem existiert an verschiedenen Standorten noch eine Videoüberwachung der Eingänge.

Besucher können die Räumlichkeiten nur betreten, indem sie durch einen Mitarbeiter eingelassen werden. Besucher werden während ihres Aufenthalts durch einen Mitarbeiter beaufsichtigt.

Die Reinigung der Büroräume erfolgt ausschließlich durch sorgfältig ausgewählte Reinigungskräfte, die jeweils einzeln auf Vertraulichkeit verpflichtet werden.

C.2 Zugangskontrolle

Benutzeranmeldungen werden über ein zentrales Active Directory über alle Standorte gleich gesteuert. Die Anmeldung erfolgt per Benutzername und Passwort. Es gibt dabei Vorgaben für sichere Passworte. Dies gilt sowohl für Arbeitsplatzrechner und Notebooks, sowie andere mobile Endgeräte.

Von außerhalb des Unternehmens kann mittels verschlüsselter VPN-Verbindung auf die Systeme zugegriffen werden.

Mobile Datenträger und Festplatten in Notebooks sowie Smartphone-Inhalte werden verschlüsselt.

C.3 Zugriffskontrolle

Die Verwaltung aller Benutzerrechte erfolgt durch Systemadministratoren und die Anzahl der Administratoren ist dabei auf ein Minimum reduziert. Die Benutzerrechte werden standortübergreifend vergeben.

Zum weiteren Schutz der Systeme werden sowohl eine zentrale Hardware-Firewall als auch Software-Firewalls auf den Systemen selbst eingesetzt. Außerdem ist auf den Systemen ein Virenscanner installiert.

Nicht mehr benutzte Datenträger werden physisch zerstört, sodass sie nicht mehr verwendbar sind. Papier wird in kleinen Mengen hausintern mittels ei-

nes ordnungsgemäßen Schredders (P4) und bei größeren Mengen durch einen zertifizierten Dienstleister vernichtet.

Für alle zentralen Systeme in der Microsoft Office Cloud ist eine Multi-Factor-Authentifizierung aktiviert.

- Detailinformationen sind auch in den folgenden TOMs zu finden:Rechenzentrum Microsoft Azure (F.5)

- Standortbezogene TOMs (E)

C.4 Trennungskontrolle

Kundensysteme werden getrennt von den internen Systemen des Auftragsverarbeiters betrieben. Innerhalb der Systeme erfolgt eine Mandantentrennung softwareseitig.

Produktivsysteme sind getrennt von Testsystemen. In allgemeinen Testsystemen werden keine Testdaten aus Produktivsystemen verwendet, die einen Rückschluss auf Produktivdaten zulassen. Kann eine Fehlersuche nur mit Produktivdaten erfolgen, dann wird in Rücksprache mit dem Kunden eine temporäre kundenspezifische Testumgebung mit Produktivdaten aufgesetzt, die nach der Fehleranalyse und -behebung wieder gelöscht wird.

C.5 Pseudonymisierung

Eine durch Pseudonyme geschützte Datenverarbeitung wird überall dort eingesetzt, wo es sinnvoll ist. Die zugehörigen personenbezogenen Daten zur Identifikation werden in separaten Datenbanktabellen abgelegt.

C.6 Weitergabekontrolle

Der Zugriff von außen auf die Firmeninfrastruktur ist über eine verschlüsselte VPN-Verbindung möglich. Für Zugriffe per Internet werden die Verbindungen per HTTPS verschlüsselt.

Auf Systeme des Verantwortlichen wird über Fernwartungstools ebenfalls nur über verschlüsselte Verbindungen zugegriffen.

C.7 Verfügbarkeit und Belastbarkeit

Um die Verfügbarkeit von Daten zu gewährleisten, werden unterbrechungsfreie Stromversorgungen (USV) und Klimaanlagen in Serverräumen eingesetzt. Weiter existieren Feuer- und Rauchmeldeanlagen.

Datensicherungen erfolgen mehrstufig und werden je nach System täglich oder gar stündlich bzw. laufend erstellt. Die Sicherungsdaten werden dabei getrennt von den Livesystemen extern abgelegt.

C.8 Rasche Wiederherstellbarkeit

Die Sicherungen werden regelmäßig getestet. So ist im Notfall eine schnelle Wiederinbetriebnahme gewährleistet.

C.9 Datenschutzmanagement

Ein externer Datenschutzbeauftragter ist schriftlich benannt. Es existiert eine interne Verarbeitungsübersicht der Verarbeitungsprozesse. Mittels eines Datenschutz-Management-Systems wird eine wiederkehrende Kontrolle alle datenschutzrelevanten Vorgänge gewährleistet.

Die Beschäftigten erhalten jeweils zu Beginn ihrer Tätigkeit und danach regelmäßig Schulungen zum Datenschutz und allgemeine Sensibilisierungen zur IT-Sicherheit. Hierbei kommen sowohl Online-Schulungen als auch Präsenzschulungen zum Einsatz.

Darüber hinaus werden die Beschäftigten auf Vertraulichkeit verpflichtet. Auch diese Verpflichtung wird zu Beginn der Tätigkeit sowie anschließend regelmäßig erneuert.

C.10 Incident-Response-Management

Datenschutzvorfälle werden zentral von einem Datenschutz-Team in Zusammenarbeit mit den internen IT-Administratoren und dem externen Datenschutzbeauftragten bearbeitet. Das Datenschutz-Team ist hierfür speziell geschult.

C.11 Auftragskontrolle

Die Unter-Auftragsverarbeiter werden hinsichtlich Datensicherheit sorgfältig ausgewählt. Darüber hinaus wird, sofern notwendig, eine Vereinbarung zur Auftragsverarbeitung abgeschlossen. Darüber werden sowohl die notwendigen Kontrollrechte definiert als auch und die Datenlöschung bei Auftragsende sichergestellt.

Die Schutzmaßnahmen der Dienstleister werden regelmäßig unter Zuhilfenahme des externen Datenschutzbeauftragten kontrolliert. Diese Kontrolle erfolgt je Einzelfall durch Fragebögen, Überprüfung von Zertifikaten externer Auditoren oder auch Inspektionen vor Ort.

D. Produktspezifische TOMs

In diesem Abschnitt werden alle TOMs beschrieben, die spezifisch für die jeweiligen Produkte gelten.

D.1 Dock & Yard Management

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Die Accounts und Zugriffsrechte werden von der ecovium verwaltet.

Die Benutzeranmeldungen werden protokolliert. Passworte der Benutzer werden nur als Hash in der Datenbank hinterlegt und sind nicht zurückrechenbar.

Die Software ist mandantenfähig. Wenn es die Lizenz es zulässt, können daher mehrere Mandanten angelegt werden. Die Daten der unterschiedlichen Mandanten sind softwareseitig getrennt.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Der Kunde hat selbst die Möglichkeit, diese Konfiguration anzupassen.

ecovium greift zu Wartungszwecken mittels Webbrowser zu. Fernwartungen finden über verschlüsselte Verbindungen statt.

Neben den Datensicherungen, die durch Microsoft im Rechenzentrum durchgeführt werden, gibt es parallele Datensicherungen durch einen weiteren Dienstleister für die Datenbanken.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Rechenzentrum Microsoft Azure (F.5)

D.2 docuware (On-Premise)

Der Kunde erhält Zugriff auf die Software-Installation und einen Lizenzschlüssel. Für die Installation, die weitere Einrichtung und Vergabe von Zugriffsrechten ist der Kunde eigenständig verantwortlich. Dem Kunden obliegt überdies die Umsetzung aller technischen und organisatorischen Schutzmaßnahmen.

ecovium unterstützt bei allen Arbeiten. Hierfür wird bei Bedarf per TeamViewer auf den Kunden-Client zugegriffen. Dies ist nur nach vorheriger Freigabe des Kunden möglich.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standortbezogene TOMs (E)

- Fernwartung TeamViewer (G.1)

D.3 docuware (SaaS)

Die Software wird beim Hersteller selbst gehostet. ecovium übernimmt den Support und unterstützt beim Betrieb. Hierfür legt ecovium eine eigene Instanz für den Kunden an und übergibt die Zugangsdaten zu diesem an den Kunden. Für die weitere Einrichtung und Vergabe von Zugriffsrechten ist der Kunde eigenständig verantwortlich.

ecovium unterstützt bei allen Arbeiten. Hierfür wird bei Bedarf per TeamViewer auf den Kunden-Client zugegriffen. Dies ist nur nach vorheriger Freigabe des Kunden möglich.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standortbezogene TOMs (E)
- Fernwartung TeamViewer (G.1)
- Rechenzentrum docuware (F.3)

D.4 Drivers Workplace

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Die Accounts und Zugriffsrechte werden von der ecovium verwaltet.

Die Benutzeranmeldungen werden protokolliert. Passworte der Benutzer werden nur als Hash in der Datenbank hinterlegt und sind nicht zurückrechenbar.

Die Software ist mandantenfähig. Wenn es die Lizenz es zulässt, können daher mehrere Mandanten angelegt werden. Die Daten der unterschiedlichen Mandanten sind softwareseitig getrennt.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Der Kunde hat selbst die Möglichkeit, diese Konfiguration anzupassen.

ecovium greift zu Wartungszwecken mittels Webbrowser zu. Fernwartungen finden über verschlüsselte Verbindungen statt.

Neben den Datensicherungen, die durch Microsoft im Rechenzentrum durchgeführt werden, gibt es parallele Datensicherungen durch einen weiteren Dienstleister für die Datenbanken.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für den Fall einer fehlenden Internetverbindung existiert ein sogenannter Offline-Modus. Alle Daten und Dokumente, die der Fahrer zur Ausführung der Tour benötigt, werden auf dem mobilen Gerät zwischengespeichert. Dazu

werden die Standardspeichermechanismen des Browsers verwendet. Mit den auf einem Smartphone vorhandenen Tools können diese Daten nicht ausgelesen werden. Die Daten werden nach Abschluss der Tour gelöscht.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Rechenzentrum Microsoft Azure (F.5)
- Standort Böbingen (E.3)

D.5 eCommerce Suite & Return Handling

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Die Accounts und Zugriffsrechte werden von der ecovium verwaltet.

Die Benutzeranmeldungen werden protokolliert. Passworte der Benutzer werden nur als Hash in der Datenbank hinterlegt und sind nicht zurückrechenbar.

Die Software ist mandantenfähig. Wenn es die Lizenz es zulässt, können daher mehrere Mandanten angelegt werden. Die Daten der unterschiedlichen Mandanten sind softwareseitig getrennt.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Der Kunde hat selbst die Möglichkeit, diese Konfiguration anzupassen.

ecovium greift zu Wartungszwecken mittels Webbrowser zu. Fernwartungen finden über verschlüsselte Verbindungen statt.

Neben den Datensicherungen, die durch Microsoft im Rechenzentrum durchführt, gibt es parallele Datensicherungen durch einen weiteren Dienstleister für die Datenbanken.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Neustadt (E.4)
- Rechenzentrum Microsoft Azure (F.5)
- Rechenzentrum AWS (F.1)

D.6 Exportkontrolle4Erp (On-Premise)

Die wesentlichen Maßnahmen werden über das SAP-System des Kunden vorgegeben: Benutzerverwaltung, Mandantenfähigkeit, Protokollierung, Datensicherung.

ecovium hat im Falle einer Wartung nur durch vorherige Freischaltung des Kunden Zugriff auf die Systeme. Fernwartungen finden über verschlüsselte Verbindungen statt. Die Art des VPN-Tunnels und auch die Fernwartungssoftware wird vom Kunden vorgegeben.

Es gibt diverse Dokumentationen zum Produkt. Spezifische Dokumentation der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Pforzheim (E.6)

D.7 F-COST

Das System sieht keine eigene Benutzerverwaltung vor. Es wird auf die Datenbank von V-LOG zugegriffen (siehe D.30 V-LOG (On-Premise)).

Die Software ist analog zu V-LOG mandantenfähig und kann auf die verschiedenen Tennants zugreifen.

Je nach Kundenwunsch kann ecovium im Falle einer Wartung über eine permanente Verbindung oder auch nur durch vorherige Freischaltung des Kunden auf die Systeme zugreifen. Fernwartungen finden über verschlüsselte Verbindungen statt.

Datensicherungen und Rücksicherungen können analog zu V-LOG vom Kunden umgesetzt werden.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Neustadt (E.4)
- Fernwartung TeamViewer (G.1)

D.8 Forwarder Suite

Grundlage des Produkts ist die Installation von WHM (D.35) mit WEB-API.

Zusätzlich sind folgende TOMs zu beachten:

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Die Accounts und Zugriffsrechte werden von der ecovium verwaltet.

Die Benutzeranmeldungen werden protokolliert. Passworte der Benutzer werden nur als Hash in der Datenbank hinterlegt und sind nicht zurückrechenbar.

Die Software ist mandantenfähig. Wenn es die Lizenz es zulässt, können daher mehrere Mandanten angelegt werden. Die Daten der unterschiedlichen Mandanten sind softwareseitig getrennt.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Der Kunde hat selbst die Möglichkeit, diese Konfiguration anzupassen.

ecovium greift zu Wartungszwecken mittels Webbrowser zu. Fernwartungen finden über verschlüsselte Verbindungen statt.

Neben den Datensicherungen, die durch Microsoft im Rechenzentrum durchführt, gibt es parallele Datensicherungen durch einen weiteren Dienstleister für die Datenbanken.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Rechenzentrum Microsoft Azure (F.5)

D.9 Hardware Suite

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Die Accounts und Zugriffsrechte werden von der ecovium verwaltet.

Die Benutzeranmeldungen werden protokolliert. Passworte der Benutzer werden nur als Hash in der Datenbank hinterlegt und sind nicht zurückrechenbar.

Der Zugriff mittels ServiceApp wird über einen individuellen Barcode abgesichert, welcher in der App gescannt werden muss. Erst danach ist eine Datenübermittlung möglich.

Um eine Verbindung zum Drucker-Service herzustellen, muss dieser im gleichen Netzwerk wie die Drucker installiert werden. Darüber hinaus wird auf beiden Seiten eine eindeutige Service-ID eingegeben.

Die Software ist mandantenfähig. Wenn es die Lizenz es zulässt, können daher mehrere Mandanten angelegt werden. Die Daten der unterschiedlichen Mandanten sind softwareseitig getrennt.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Der Kunde hat selbst die Möglichkeit, diese Konfiguration anzupassen.

ecovium greift zu Wartungszwecken mittels Webbrowser zu. Fernwartungen finden über verschlüsselte Verbindungen statt.

Neben den Datensicherungen, die durch Microsoft im Rechenzentrum durchführt, gibt es parallele Datensicherungen durch einen weiteren Dienstleister für die Datenbanken.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Rechenzentrum Microsoft Azure (F.5)

D.10 Interfaces

Auf die Benutzeroberfläche der Interfaces haben nur die Administratoren der ecovium Zugriff. Für den Zugriff auf die Daten der Kundeninstallation stellt der Kunde die notwendigen Anmeldedaten zur Verfügung. Über diese werden dann die Daten zur Konvertierung abgerufen und wieder zurückgespielt.

Standardmäßig wird die REST-API via HTTPS verschlüsselt angesprochen. Optional kann der Kunde auch andere Kommunikationswege für die Datenübermittlung bereitstellen. In diesem Fall ist der Kunde für die Vertraulichkeit und Sicherheit der Kommunikationswege verantwortlich.

Die Zugangsdaten zum Kundensystem werden auf Seiten der ecovium in einer Datenbank verschlüsselt abgelegt. Die Software ist mandantenfähig, sodass die Konfigurationsdaten verschiedener Kunden voneinander getrennt in der Datenbank abgelegt werden.

Transaktionsdaten während des Konvertierungsvorgangs werden nicht gespeichert. Es werden jedoch Protokolle mit Zeitpunkten und technische Meldungen der Verarbeitungsvorgänge geführt. In spezifischen Kundenszenarien und nach Anforderung sind weitere Protokollinhalte möglich.

ecovium greift zu Wartungszwecken per Remote-Desktop über eine verschlüsselte Verbindung auf den Server in der Azure-Cloud zu. Weiterhin kann mittels eines Clients verschlüsselt auf die Software zugegriffen werden.

Neben den Datensicherungen, die durch Microsoft im Rechenzentrum durchgeführt werden, gibt es parallele Datensicherungen durch einen weiteren Dienstleister für die Datenbanken.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Rechenzentrum Microsoft Azure (F.5)
- Fernwartung Remote-Desktop (G.2)

D.11 Komalog

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Vorgaben zur Passwortkomplexität werden nicht gemacht. Der Kunde erhält von der ecovium einen Standard-Admin-Account. Es obliegt dem Kunden, die weiteren Zugangsdaten individuell zu vergeben.

Die Benutzeranmeldungen werden protokolliert. Passworte der Benutzer werden nur als Hash in der Datenbank hinterlegt und sind nicht zurückrechenbar.

Die Software ist mandantenfähig. Wenn es die Lizenz es zulässt, können daher mehrere Mandanten angelegt werden. Die Daten der unterschiedlichen Mandanten sind softwareseitig getrennt.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Die Endkonfiguration liegt jedoch beim Kunden.

ecovium hat im Falle einer Wartung nur durch vorherige Freischaltung des Kunden Zugriff auf die Systeme. Fernwartungen finden über verschlüsselte Verbindungen statt.

Datensicherungen und Rücksicherungen sind mit dem System möglich. Es können Dumps der Datenbanken erzeugt werden. Rücksicherungen sind auch testweise möglich. Bei Updates können beispielsweise Daten zunächst in ein Testsystem rückgesichert werden. Die Umsetzung der Datensicherung obliegt dem Kunden.

Es gibt diverse Online-Dokumentationen zum Produkt. Spezifische Dokumentation der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Bielefeld (E.1)
- Fernwartung TeamViewer (G.1)
- Rechenzentrum Hetzner (F.4)
- Rechenzentrum Myloc BNS Cloud-Dienste (F.6)

D.12 LCF.NET

Grundlage des Produkts ist eine Installation von WHM (D.35), dessen TOMs ebenso relevant sind. Zusätzlich sind folgende TOMs zu beachten:

Über die LCF.NET-API kann auf die Daten des WHM zugegriffen werden. Zur Authentifizierung wird der im WHM hinterlegte Benutzer verwendet. Es obliegt dem Kunden, den für die Schnittstelle notwendigen IP-Port nur intern oder auch extern freizugeben.

Der Zugriff auf die LCF.NET-API kann durch eine HTTPS-Verbindung gesichert.

D.13 LLE Webportal (On-Premise)

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Passwörter müssen mindestens acht Zeichen lang sein und ein Sonderzeichen und einen Großbuchstaben beinhalten. Die Dauer der Passwortgültigkeit ist einstellbar. Für die Admins ist eine 2FA vorgeschrieben. Die Benutzer können eine solche nutzen. Der Kunde erhält von der ecovium einen Standard-Admin-Account. Es obliegt dem Kunden, die weiteren Zugangsdaten individuell zu vergeben.

Die Benutzeranmeldungen werden protokolliert. Passworte der Benutzer werden nur als Hash in der Datenbank hinterlegt und sind nicht zurückrechenbar.

Die Software ist mandantenfähig. Wenn es die Lizenz es zulässt, können daher mehrere Mandanten angelegt werden. Die Daten der unterschiedlichen Mandanten sind softwareseitig getrennt.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Die Endkonfiguration wird durch ecovium nach Vorgaben des Kunden durchgeführt.

ecovium hat im Falle einer Wartung nur durch vorherige Freischaltung des Kunden Zugriff auf die Systeme. Fernwartungen finden über verschlüsselte Verbindungen statt. Der Zugriff erfolgt per SSH.

Eingaben, Änderungen und Löschungen der Daten werden in der Datenbank benutzerbezogen protokolliert.

Datensicherungen und Rücksicherungen sind mit dem System möglich. Zum einen können Exportdateien erstellt und zum anderen auch Dumps der Datenbanken erzeugt werden. Rücksicherungen sind auch testweise möglich. Bei Updates können beispielsweise Daten zunächst in ein Testsystem rückgesichert werden. Die Umsetzung der Datensicherung obliegt dem Kunden.

Es gibt diverse Dokumentationen zum Produkt. Spezifische Dokumentation der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Pforzheim (E.6)

D.14 LLE Webportal (SaaS)

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Passwörter müssen mindestens acht Zeichen lang sein und ein Sonderzeichen und einen Großbuchstaben beinhalten. Die Dauer der Passwortgültigkeit ist einstellbar. Für die Admins ist eine 2FA vorgeschrieben. Die Benutzer können eine solche nutzen. Der Kunde erhält von der ecovium einen Standard-Admin-Account. Es obliegt dem Kunden, die weiteren Zugangsdaten individuell zu vergeben.

Die Benutzeranmeldungen werden protokolliert. Passworte der Benutzer werden nur als Hash in der Datenbank hinterlegt und sind nicht zurückrechenbar.

Die Software ist mandantenfähig. Wenn es die Lizenz es zulässt, können daher mehrere Mandanten angelegt werden. Die Daten der unterschiedlichen Mandanten sind softwareseitig getrennt.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Die Endkonfiguration wird durch ecovium nach Vorgaben des Kunden durchgeführt.

ecovium hat im Falle einer Wartung nur durch vorherige Freischaltung des Kunden Zugriff auf die Systeme. Fernwartungen finden über verschlüsselte Verbindungen statt. Der Zugriff erfolgt per SSH.

Eingaben, Änderungen und Löschungen der Daten werden in der Datenbank benutzerbezogen protokolliert.

Datensicherungen werden täglich und Rücksicherungen gelegentlich getestet.

Es gibt diverse Dokumentationen zum Produkt. Spezifische Dokumentation der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Pforzheim (E.6)
- Rechenzentrum PlusServer (F.7)

D.15 OnFleet

OnFleet ist ein Zusatzmodul zu OnRoad (incl. OnWeb). Zusätzlich sind folgende TOMs zu beachten:

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Dabei werden zum Installationszeitpunkt die Benutzer der zugehörigen OnRoad-

Installation synchronisiert. Als Startpasswort wird ein einheitliches Standardpasswort verwendet, welches die Benutzer anschließend anpassen müssen. Vorgaben zur Passwortkomplexität werden nicht gemacht.

Die Benutzeranmeldungen werden protokolliert. Passworte der Benutzer werden nur als Hash in der Datenbank hinterlegt und sind nicht zurückrechenbar.

Für jeden Kunden gibt es eine eigene Datenbank. Die Software ist zusätzlich mandantenfähig. Wenn es die Lizenz es zulässt, können daher mehrere Mandanten angelegt werden. Die Daten der unterschiedlichen Mandanten sind softwareseitig getrennt.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Die technische Grundkonfiguration obliegt der ecovium. Für Einstellungen zur Oberfläche ist der Kunde verantwortlich.

Zu Wartungszwecken kann die ecovium die Server mittels SSH-Clients erreichen. Fernwartungen finden über verschlüsselte Verbindungen statt.

Datensicherungen werden regelmäßig automatisch erstellt. Sie werden sicherheitshalber bei einem Dienstleister extern abgelegt. Dabei ist zu beachten, dass in der Regel keine Transaktionsdaten auf den ecovium-Servern gespeichert werden, da diese direkt an die Kundenserver übertragen werden. Nur wenn die Verbindung zeitweise nicht verfügbar ist, werden die Daten zwischengespeichert.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Düsseldorf (E.3)
- Rechenzentrum DigitalOcean (F.2)

D.16 OnRoad (incl. OnWeb)

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Auf Kundenwunsch kann auch nur der Windows-Benutzername verwendet werden, dann wird auf das Passwort verzichtet. Vorgaben zur Passwortkomplexität werden nicht gemacht. Der Kunde erhält von der ecovium einen Standard-Admin-Account. Es obliegt dem Kunden, die weiteren Zugangsdaten individuell zu vergeben. ecovium wird hierbei lediglich unterstützend tätig.

Die Benutzeranmeldungen werden protokolliert. Passworte der Benutzer werden nur als Hash in der Datenbank hinterlegt und sind nicht zurückrechenbar.

Die Software ist mandantenfähig. Wenn es die Lizenz es zulässt, können daher mehrere Mandanten angelegt werden. Die Daten der unterschiedlichen Mandanten sind softwareseitig getrennt.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Die Endkonfiguration liegt jedoch beim Kunden.

ecovium hat im Falle einer Wartung nur durch vorherige Freischaltung des Kunden Zugriff auf die Systeme. Optional ist auch eine permanente Fernwartungsverbindung möglich. Fernwartungen finden über verschlüsselte Verbindungen statt.

Datensicherungen und Rücksicherungen sind mit dem System möglich. Zum einen können Exportdateien erstellt und zum anderen auch Dumps der Datenbanken erzeugt werden. Rücksicherungen sind auch testweise möglich. Bei Updates können beispielsweise Daten zunächst in ein Testsystem rückgesichert werden. Die Umsetzung der Datensicherung obliegt dem Kunden. ecovium wird hierbei lediglich unterstützend tätig.

Es gibt diverse Dokumentationen zum Produkt. Spezifische Dokumentation der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Düsseldorf (E.3)
- Rechenzentrum Myloc BNS Cloud-Dienste (F.6)
- Fernwartung TeamViewer (G.1)

D.17 Pcalc (On-Premise)

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Passwörter müssen mindestens acht Zeichen lang sein und ein Sonderzeichen und einen Großbuchstaben beinhalten. Die Dauer der Passwortgültigkeit ist einstellbar. Der Kunde erhält von der ecovium einen Standard-Admin-Account. Es obliegt dem Kunden, die weiteren Zugangsdaten individuell zu vergeben.

Die Benutzeranmeldungen werden protokolliert. Passworte der Benutzer werden nur als Hash in der Datenbank hinterlegt und sind nicht zurückrechenbar.

Die Software ist mandantenfähig. Wenn es die Lizenz es zulässt, können daher mehrere Mandanten angelegt werden. Die Daten der unterschiedlichen Mandanten sind softwareseitig getrennt.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Die Endkonfiguration wird durch ecovium nach Vorgaben des Kunden durchgeführt.

ecovium hat im Falle einer Wartung nur durch vorherige Freischaltung des Kunden Zugriff auf die Systeme. Fernwartungen finden über verschlüsselte

Verbindungen statt. Die Art des VPN-Tunnels und auch die Fernwartungssoftware wird vom Kunden vorgegeben.

Eingaben, Änderungen und Löschungen der Daten werden in der Datenbank benutzerbezogen protokolliert.

Datensicherungen und Rücksicherungen sind mit dem System möglich. Zum einen können Exportdateien erstellt und zum anderen auch Dumps der Datenbanken erzeugt werden. Rücksicherungen sind auch testweise möglich. Bei Updates können beispielsweise Daten zunächst in ein Testsystem rückgesichert werden. Die Umsetzung der Datensicherung obliegt dem Kunden.

Es gibt diverse Dokumentationen zum Produkt. Spezifische Dokumentation der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Pforzheim (E.6)

D.18 PcaIc (SaaS)

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Passwörter müssen mindestens acht Zeichen lang sein und ein Sonderzeichen und einen Großbuchstaben beinhalten. Die Dauer der Passwortgültigkeit ist einstellbar. ecovium vergibt die Anzahl der Benutzer nach Rücksprache mit dem Kunden und abhängig von der erworbenen Lizenz. Die Berechtigungen der einzelnen Benutzer kann der Kunde selbst verändern.

Die Benutzeranmeldungen werden protokolliert. Passworte der Benutzer werden nur als Hash in der Datenbank hinterlegt und sind nicht zurückrechenbar.

Die Software ist mandantenfähig. Wenn es die Lizenz es zulässt, können daher mehrere Mandanten angelegt werden. Die Daten der unterschiedlichen Mandanten sind softwareseitig getrennt.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Die Endkonfiguration wird durch ecovium nach Vorgaben des Kunden durchgeführt.

Der Kunde hat über einen Citrix-Client Zugriff auf das System. Die Datenverbindungen sind verschlüsselt. ecovium nutzt ebenso einen Citrix-Client zur Wartung. Systemnahe Wartungen werden per vSphere auf den virtuellen Geräten durchgeführt.

Eingaben, Änderungen und Löschungen der Daten werden in der Datenbank benutzerbezogen protokolliert.

Datensicherungen werden mittels Veam täglich angelegt. Gelegentlich werden Rücksicherungen getestet.

Es gibt diverse Dokumentationen zum Produkt und zur Installation im Rechenzentrum.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Pforzheim (E.6)
- Rechenzentrum PlusServer (F.7)

D.19 PCalc4Erp (On-Premise)

Die wesentlichen Maßnahmen werden über das SAP-System des Kunden vorgegeben: Benutzerverwaltung, Mandantenfähigkeit, Protokollierung, Datensicherung.

ecovium hat im Falle einer Wartung nur durch vorherige Freischaltung des Kunden Zugriff auf die Systeme. Fernwartungen finden über verschlüsselte Verbindungen statt. Die Art des VPN-Tunnels und auch die Fernwartungssoftware wird vom Kunden vorgegeben.

Es gibt diverse Dokumentationen zum Produkt. Spezifische Dokumentation der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Pforzheim (E.6)

D.20 S-Check (SaaS)

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Vorgaben zur Passwortkomplexität sind vorhanden. Neue Benutzer können lediglich durch die ecovium eingerichtet werden.

Die Daten jedes Kunden werden in individuellen Datenbanken abgelegt. Darüber hinaus können innerhalb seiner Datenbank auf Kundenwunsch weitere Mandanten angelegt werden.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Änderungen sind nur der ecovium möglich.

Zu Wartungszwecken kann sich die ecovium über eine Webschnittstelle zugreifen oder direkt auf die Datenbanken aufschalten. Hierfür werden verschlüsselte Verbindungen verwendet.

Datensicherungen werden auf Basis eines Sicherungskonzepts regelmäßig erstellt.

Es gibt diverse Dokumentationen zum Produkt. Spezifische Dokumentation der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Böbingen (E.2)
- Rechenzentrum Microsoft Azure (F.5)

D.21 S-Check Legacy (On-Premise)

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Vorgaben zur Passwortkomplexität werden nicht gemacht. Der Kunde erhält von der ecovium einen Standard-Admin-Account. Es obliegt dem Kunden, die weiteren Zugangsdaten individuell zu vergeben.

Passworte der Benutzer werden nur als Hash in der Datenbank hinterlegt und sind nicht zurückrechenbar.

Die Software ist mandantenfähig. Wenn es die Lizenz es zulässt, können daher mehrere Mandanten angelegt werden. Die Daten der unterschiedlichen Mandanten sind softwareseitig getrennt.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Die Endkonfiguration liegt jedoch beim Kunden.

ecovium hat im Falle einer Wartung nur durch vorherige Freischaltung des Kunden Zugriff auf die Systeme. Fernwartungen finden über verschlüsselte Verbindungen statt.

Datensicherungen und Rücksicherungen sind mit dem System möglich. Zum einen können Exportdateien erstellt und zum anderen auch Dumps der Datenbanken erzeugt werden. Rücksicherungen sind auch testweise möglich. Bei Updates können beispielsweise Daten zunächst in ein Testsystem rückgesichert werden. Die Umsetzung der Datensicherung obliegt dem Kunden.

Es gibt diverse Dokumentationen zum Produkt. Spezifische Dokumentation der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Böbingen (E.2)
- Fernwartung TeamViewer (G.1)

D.22 S-Check Legacy (SaaS)

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Vorgaben zur Passwortkomplexität werden nicht gemacht. Neue Benutzer können lediglich durch die ecovium eingerichtet werden.

Die Daten jedes Kunden werden in individuellen Datenbanken abgelegt. Darüber hinaus können innerhalb seiner Datenbank auf Kundenwunsch weitere Mandanten angelegt werden.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Änderungen sind nur der ecovium möglich.

Zu Wartungszwecken kann sich die ecovium über eine Webschnittstelle zugreifen oder direkt auf die Datenbanken aufschalten. Hierfür werden verschlüsselte Verbindungen verwendet.

Datensicherungen werden auf Basis eines Sicherungskonzepts regelmäßig erstellt.

Es gibt diverse Dokumentationen zum Produkt. Spezifische Dokumentation der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Böbingen (E.2)
- Rechenzentrum Microsoft Azure (F.5)

D.23 Shiptrack Portal

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen (E-Mail-Adresse) und Passwort anmelden muss. Vorgaben zur Passwortkomplexität sind vorhanden, jedoch wird dem Benutzer die Qualität des gewählten Passworts angezeigt. Die ecovium richtet zunächst nur einen Admin-Account für den Kunden an. Dieser vergibt dann für weitere Benutzer selbstständig die Anmeldedaten. Die Passwörter werden von den Benutzern selbst vergeben. Passworte werden als Hash-Wert in der Datenbank gespeichert, sodass niemand auf das Klartext-Passwort Zugriff hat.

Es gibt ein Berechtigungssystem. Der Kunde bestimmt selbst die Zugriffsrechte der von ihm eingerichteten Benutzer.

Anmeldevorgänge und Zugriffe auf das System werden protokolliert.

Die Daten jedes Kunden werden in einer zentralen Datenbank abgelegt, welche softwareseitig nach Mandanten getrennt wird.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Änderungen sind durch den Kunden möglich.

Zugriffe durch den Kunden laufen mittels HTTPS und sind damit verschlüsselt. Zu Wartungszwecken kann sich auch die ecovium mit Adminrechten anmelden.

Datensicherungen werden auf Basis eines Sicherungskonzepts täglich erstellt.

Es gibt diverse Dokumentationen zum Produkt. Spezifische Dokumentation der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Neustadt (E.4)
- Rechenzentrum AWS (F.1)

D.24 Shiptrack Service

Das System hat eine Rechteverwaltung, in dem durch die ecovium ein Benutzer pro Kunde mit Benutzernamen und Passwort für den Zugriff auf API-Schnittstellen angelegt wird. Dieser Benutzer wird auf Kundenseite für den technischen Zugriff auf die Schnittstellen verwendet.

Passworte werden als Hash-Wert in der Datenbank gespeichert.

Die Daten jedes Kunden werden in einer zentralen Datenbank abgelegt, welche softwareseitig nach Mandanten getrennt wird.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Änderungen sind durch den Kunden möglich.

Zugriffe durch den Kunden laufen mittels HTTPS und sind damit verschlüsselt. Zu Wartungszwecken kann die ecovium mittels Remote-Desktop oder mittels SSH über eine VPN-Verbindung auf die Server zugreifen.

Datensicherungen werden auf Basis eines Sicherungskonzepts täglich erstellt.

Es gibt diverse Dokumentationen zum Produkt bzw. zu den API-Schnittstellen. Spezifische Dokumentation der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Neustadt (E.4)

- Rechenzentrum Microsoft Azure (F.5)

D.25 tEx (On-Premise)

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Vorgaben zur Passwortkomplexität werden gemacht. Der Kunde erhält von der ecovium einen Standard-Admin-Account. Es obliegt dem Kunden, die weiteren Zugangsdaten individuell zu vergeben.

Die Software ist mandantenfähig. Wenn es die Lizenz es zulässt, können daher mehrere Mandanten angelegt werden. Die Daten der unterschiedlichen Mandanten sind softwareseitig getrennt.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Die Endkonfiguration liegt jedoch beim Kunden.

ecovium hat im Falle einer Wartung nur durch vorherige Freischaltung des Kunden Zugriff auf die Systeme. Auf Kundenwunsch kann auch eine permanente Verbindung eingerichtet werden, über die ecovium dann ohne separate Freischaltung zugreifen kann. Fernwartungen finden über verschlüsselte Verbindungen statt. Dabei kommt entweder TeamViewer zum Einsatz oder es gibt eine VPN-Verbindung, über die eine Direktanmeldung am Server möglich wird.

Datensicherungen und Rücksicherungen sind mit dem System möglich. Zum einen können Exportdateien erstellt und zum anderen auch Dumps der Datenbanken erzeugt werden. Rücksicherungen sind auch testweise möglich. Bei Updates können beispielsweise Daten zunächst in ein Testsystem rückgesichert werden. Die Umsetzung der Datensicherung obliegt dem Kunden.

Dokumentationen der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Böbingen (E.2)
- Fernwartung TeamViewer (G.1)

D.26 Transport Hub

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Die Accounts und Zugriffsrechte werden von der ecovium verwaltet.

Die Benutzeranmeldungen werden protokolliert. Passworte der Benutzer werden nur als Hash in der Datenbank hinterlegt und sind nicht zurückrechenbar.

Die Software ist mandantenfähig. Wenn es die Lizenz es zulässt, können daher mehrere Mandanten angelegt werden. Die Daten der unterschiedlichen Mandanten sind softwareseitig getrennt.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Der Kunde hat selbst die Möglichkeit, diese Konfiguration anzupassen.

ecovium greift zu Wartungszwecken mittels Webbrowser zu. Fernwartungen finden über verschlüsselte Verbindungen statt.

Neben den Datensicherungen, die durch Microsoft im Rechenzentrum durchgeführt werden, gibt es parallele Datensicherungen durch einen weiteren Dienstleister für die Datenbanken.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Der Zugriff externer Geschäftspartner auf eine für sie relevante Tour wird über einen individuellen QR-Code abgesichert (Zugriffstoken), der gescannt werden muss.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Rechenzentrum Microsoft Azure (F.5)
- Standort Böbingen (E.23)

D.27 Transroad (On-Premise)

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Vorgaben zur Passwortkomplexität und zur Zwei-Faktor-Authentifizierung können durch den Administrator auf Kunden-Seite optional konfiguriert werden. Die Dauer der Passwortgültigkeit ist einstellbar. Der Kunde erhält von der ecovium einen Standard-Admin-Account. Es obliegt dem Kunden, die weiteren Zugangsdaten individuell zu vergeben.

Die Benutzeranmeldungen werden protokolliert. Passworte der Benutzer werden nur als Hash in der Datenbank hinterlegt und sind nicht zurückrechenbar.

Die Software ist mandantenfähig. Wenn es die Lizenz es zulässt, können daher mehrere Mandanten angelegt werden. Die Daten der unterschiedlichen Mandanten sind softwareseitig getrennt.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Die Endkonfiguration liegt jedoch beim Kunden.

ecovium hat im Falle einer Wartung nur durch vorherige Freischaltung des Kunden Zugriff auf die Systeme. Fernwartungen finden über verschlüsselte Verbindungen statt.

Datensicherungen und Rücksicherungen sind mit dem System möglich. Zum einen können Exportdateien erstellt und zum anderen auch Dumps der Datenbanken erzeugt werden. Rücksicherungen sind auch testweise möglich. Bei Updates können beispielsweise Daten zunächst in ein Testsystem rückgesichert werden. Die Umsetzung der Datensicherung obliegt dem Kunden.

Es gibt diverse Online-Dokumentationen zum Produkt. Spezifische Dokumentation der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Bielefeld (E.1)
- Fernwartung TeamViewer (G.1)
- Rechenzentrum Myloc BNS Cloud-Dienste (F.6)

D.28 Transroad (SaaS)

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Vorgaben zur Passwortkomplexität und zur Zwei-Faktor-Authentifizierung können durch den Administrator auf Kunden-Seite optional konfiguriert werden. Die Dauer der Passwortgültigkeit ist einstellbar. Der Kunde erhält von der ecovium einen Standard-Admin-Account. Es obliegt dem Kunden, die weiteren Zugangsdaten individuell zu vergeben.

Die Benutzeranmeldungen werden protokolliert. Passworte der Benutzer werden nur als Hash in der Datenbank hinterlegt und sind nicht zurückrechenbar.

Die Software ist mandantenfähig. Je Mandant muss der Kunde eine Lizenz erwerben. Die Daten der unterschiedlichen Mandanten sind softwareseitig getrennt.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen dem Kunden zur Verfügung gestellt. Die Endkonfiguration liegt jedoch beim Kunden.

ecovium ist für die Wartung der Server zuständig und greift auf diese per verschlüsselter VPN-Verbindung mittels SSH zu. Auf die Clients beim Kunden hat ecovium im Falle einer Wartung nur durch vorherige Freischaltung des Kunden Zugriff. Fernwartungen finden über verschlüsselte Verbindungen statt.

Der Kunde greift mittels Web-Anwendung auf die Server zu. Die Verbindungen sind mittels HTTPS verschlüsselt.

ecovium betreibt für die Anwendung mehrere redundante Serversysteme in einem externen Rechenzentrum. Zusätzliche werden regelmäßige Daten-

banksicherungen auf Basis eines Backupkonzepts erstellt, die laufend überwacht und regelmäßig kontrolliert werden. Rücksicherungen werden regelmäßig getestet. Bei Updates werden beispielsweise Daten zunächst in ein Testsystem rückgesichert.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Bielefeld (E.1)
- Rechenzentrum Hetzner (F.4)
- Rechenzentrum Myloc BNS Cloud-Dienste (F.6)
- Fernwartung TeamViewer (G.1)

D.29 TrayCommand

Grundlage des Produkts ist eine Installation von WHM (D.35), dessen TOMs ebenso relevant sind. Zusätzlich sind folgende TOMs zu beachten:

Über eine WEB-API kann auf die Daten des WHM zugegriffen werden. Zur Authentifizierung wird der im WHM hinterlegte Benutzer verwendet. Es obliegt dem Kunden, den für die Schnittstelle notwendigen IP-Port nur intern oder auch extern freizugeben.

Der Zugriff auf die WEB-API kann durch eine HTTPS-Verbindung gesichert.

D.30 V-LOG (On-Premise)

Das System sieht keine eigene Benutzerverwaltung vor. Diese ist auf Seite des Kunden umzusetzen. Zum Zugriff auf die Datenbank ist ein Passwort notwendig, welches vom Kunden definiert und an ecovium übergeben wird.

Die Software ist mandantenfähig und kann verschiedene Tennants zur Verfügung stellen. Wie viele Tennants zur Verfügung gestellt werden ist abhängig von der Lizenz des Kunden.

Je nach Kundenwunsch kann ecovium im Falle einer Wartung über eine permanente Verbindung oder auch nur durch vorherige Freischaltung des Kunden auf die Systeme zugreifen. Fernwartungen finden über verschlüsselte Verbindungen statt.

Datensicherungen und Rücksicherungen sind mit dem System möglich. Zum einen können Exportdateien erstellt und zum anderen auch Dumps der Datenbanken erzeugt werden. Rücksicherungen sind auch testweise möglich. Bei Updates können beispielsweise Daten zunächst in ein Testsystem rückgesichert werden. Die Umsetzung der Datensicherung obliegt dem Kunden.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Neustadt (E.4)
- Fernwartung TeamViewer (G.1)

D.31 V-LOG (On-Premise mit Watchdog)

Die TOMs sind genauso wie in D.30 V-LOG (On-Premise) beschrieben.

Zusätzlich werden in regelmäßigen Abständen Nutzungsinformationen an die ecovium übertragen. Damit hat die ecovium immer aktuell Informationen über die Systemumgebung und kann so im Supportfall schneller unterstützend tätig werden.

D.32 V-LOG SaaS

Die Zugriffsrechte werden über das parallel verwendete eCommerce-Suite-System vergeben. Nur hierüber ist ein Zugriff möglich.

Datensicherungen werden täglich erstellt und liegen für jeweils sieben Tage vor.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Neustadt (E.4)
- Fernwartung TeamViewer (G.1)
- Fernwartung Remote-Desktop (G.2)
- Rechenzentraum Microsoft Azure (F.5)Rechenzentrum Myloc BNS Cloud Dienste (F.6)

D.33 VlogWeb

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Vorgaben zur Passwortkomplexität werden nicht gemacht. Neue Benutzer können lediglich durch die ecovium eingerichtet werden.

Die Daten jedes Kunden werden in individuellen Datenbanken abgelegt. Darüber hinaus können innerhalb seiner Datenbank auf Kundenwunsch weitere Mandanten angelegt werden.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Änderungen sind nur der ecovium möglich.

Zu Wartungszwecken kann sich die ecovium über eine Webschnittstelle zugreifen oder direkt auf die Datenbanken aufschalten. Hierfür werden verschlüsselte Verbindungen verwendet.

Datensicherungen werden auf Basis eines Sicherungskonzepts regelmäßig erstellt.

Es gibt diverse Dokumentationen zum Produkt. Spezifische Dokumentation der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Böbingen (E.2)
- Rechenzentrum Microsoft Azure (F.5)

D.34 WHI

Grundlage des Produkts ist eine Installation von WHM (D.35), dessen TOMs ebenso relevant sind.

D.35 WHM

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Vorgaben zur Passwortkomplexität werden nicht gemacht. Der Kunde erhält von der ecovium einen Standard-Admin-Account. Es obliegt dem Kunden, die weiteren Zugangsdaten individuell zu vergeben.

Die Benutzeranmeldungen werden protokolliert. Passworte der Benutzer werden nur als Hash in der Datenbank hinterlegt und sind nicht zurückrechenbar.

Die Software ist mandantenfähig. Wenn es die Lizenz es zulässt, können daher mehrere Mandanten angelegt werden. Die Daten der unterschiedlichen Mandanten sind softwareseitig getrennt.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Die Endkonfiguration liegt jedoch beim Kunden.

ecovium hat für Zwecke des Supports je nach Kundenwunsch entweder eine permanente Verbindung zum Kundensystem oder kann sich erst nach vorheriger Freischaltung des Kunden auf die Systeme zugreifen. Fernwartungen finden über verschlüsselte Verbindungen statt.

Datensicherungen und Rücksicherungen sind mit dem System möglich. Zum einen können Exportdateien erstellt und zum anderen auch Dumps der Datenbanken erzeugt werden. Bei Updates können beispielsweise Daten zu-

nächst in ein Testsystem rückgesichert werden. Die Umsetzung der Datensicherung obliegt dem Kunden.

Es gibt allgemeine Dokumentationen zum Produkt. Spezifische Dokumentation der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Pforzheim (E.6)
- Fernwartung TeamViewer (G.1)

D.36 WOS

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Vorgaben zur Passwortkomplexität werden nicht gemacht. Der Kunde erhält von der ecovium einen Standard-Admin-Account. Es obliegt dem Kunden, die weiteren Zugangsdaten individuell zu vergeben.

Die Benutzeranmeldungen werden protokolliert. Passworte der Benutzer werden nur als Hash in der Datenbank hinterlegt und sind nicht zurückrechenbar.

Die Software ist mandantenfähig. Wenn es die Lizenz es zulässt, können daher mehrere Mandanten angelegt werden. Die Daten der unterschiedlichen Mandanten sind softwareseitig getrennt.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Die Endkonfiguration liegt jedoch beim Kunden.

ecovium hat für Zwecke des Supports je nach Kundenwunsch entweder eine permanente Verbindung zum Kundensystem oder kann sich erst nach vorheriger Freischaltung des Kunden auf die Systeme zugreifen. Fernwartungen finden über verschlüsselte Verbindungen statt.

Datensicherungen und Rücksicherungen sind mit dem System möglich. Zum einen können Exportdateien erstellt und zum anderen auch Dumps der Datenbanken erzeugt werden. Bei Updates können beispielsweise Daten zunächst in ein Testsystem rückgesichert werden. Die Umsetzung der Datensicherung obliegt dem Kunden.

Es gibt allgemeine Dokumentationen zum Produkt. Spezifische Dokumentation der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Norderstedt (E.5)

- Fernwartung TeamViewer (G.1)

D.37 xStorage 3

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Vorgaben zur Passwortkomplexität werden nicht gemacht. Der Kunde erhält von der ecovium einen Standard-Admin-Account. Es obliegt dem Kunden, die weiteren Zugangsdaten individuell zu vergeben.

Die Benutzeranmeldungen werden protokolliert. Passworte der Benutzer werden nur als Hash in der Datenbank hinterlegt und sind nicht zurückrechenbar.

Die Software ist mandantenfähig. Wenn es die Lizenz es zulässt, können daher mehrere Mandanten angelegt werden. Die Daten der unterschiedlichen Mandanten sind softwareseitig getrennt.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Die Endkonfiguration liegt jedoch beim Kunden.

ecovium hat für Zwecke des Supports je nach Kundenwunsch entweder eine permanente Verbindung zum Kundensystem oder kann sich erst nach vorheriger Freischaltung des Kunden auf die Systeme zugreifen. Fernwartungen finden über verschlüsselte Verbindungen statt.

Datensicherungen und Rücksicherungen sind mit dem System möglich. Zum einen können Exportdateien erstellt und zum anderen auch Dumps der Datenbanken erzeugt werden. Bei Updates können beispielsweise Daten zunächst in ein Testsystem rückgesichert werden. Die Umsetzung der Datensicherung obliegt dem Kunden.

Es gibt allgemeine Dokumentationen zum Produkt. Spezifische Dokumentation der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Würzburg (E.7)
- Fernwartung TeamViewer (G.1)

D.38 Z-ATLAS Export (On-Premise)

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Vorgaben zur Passwortkomplexität werden nicht gemacht. Der Kunde erhält von der ecovium einen Standard-Admin-Account. Es obliegt dem Kunden, die weiteren Zugangsdaten individuell zu vergeben.

Die Software ist mandantenfähig. Wenn es die Lizenz es zulässt, können daher mehrere Mandanten angelegt werden. Die Daten der unterschiedlichen Mandanten sind softwareseitig getrennt.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Die Endkonfiguration liegt jedoch beim Kunden.

ecovium hat im Falle einer Wartung nur durch vorherige Freischaltung des Kunden Zugriff auf die Systeme. Auf Kundenwunsch kann auch eine permanente Verbindung eingerichtet werden, über die ecovium dann ohne separate Freischaltung zugreifen kann. Fernwartungen finden über verschlüsselte Verbindungen statt.

Datensicherungen und Rücksicherungen sind mit dem System möglich. Zum einen können Exportdateien erstellt und zum anderen auch Dumps der Datenbanken erzeugt werden. Rücksicherungen sind auch testweise möglich. Bei Updates können beispielsweise Daten zunächst in ein Testsystem rückgesichert werden. Die Umsetzung der Datensicherung obliegt dem Kunden.

Es gibt diverse Dokumentationen zum Produkt. Spezifische Dokumentation der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Böbingen (E.2)
- Fernwartung TeamViewer (G.1)

D.39 Z-ATLAS Export (SaaS)

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Vorgaben zur Passwortkomplexität sind nicht vorhanden. Neue Benutzer können lediglich durch die ecovium eingerichtet werden.

Die Daten jedes Kunden werden in individuellen Datenbankenschemata abgelegt. Darüber hinaus können innerhalb seiner Datenbank auf Kundenwunsch weitere Mandanten angelegt werden.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Änderungen sind nur der ecovium möglich.

Zu Wartungszwecken kann sich die ecovium direkt auf die Datenbanken aufschalten. Hierfür werden verschlüsselte Verbindungen verwendet.

Datensicherungen werden auf Basis eines Sicherungskonzepts regelmäßig erstellt.

Es gibt diverse Dokumentationen zum Produkt. Spezifische Dokumentation der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Böbingen (E.2)
- Rechenzentrum Microsoft Azure (F.5)

D.40 Z-ATLAS Import (On-Premise)

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Vorgaben zur Passwortkomplexität werden gemacht. Der Kunde erhält von der ecovium einen Standard-Admin-Account. Es obliegt dem Kunden, die weiteren Zugangsdaten individuell zu vergeben.

Die Software ist mandantenfähig. Wenn es die Lizenz es zulässt, können daher mehrere Mandanten angelegt werden. Die Daten der unterschiedlichen Mandanten sind softwareseitig getrennt.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Die Endkonfiguration liegt jedoch beim Kunden.

ecovium hat im Falle einer Wartung nur durch vorherige Freischaltung des Kunden Zugriff auf die Systeme. Auf Kundenwunsch kann auch eine permanente Verbindung eingerichtet werden, über die ecovium dann ohne separate Freischaltung zugreifen kann. Fernwartungen finden über verschlüsselte Verbindungen statt.

Datensicherungen und Rücksicherungen sind mit dem System möglich. Zum einen können Exportdateien erstellt und zum anderen auch Dumps der Datenbanken erzeugt werden. Rücksicherungen sind auch testweise möglich. Bei Updates können beispielsweise Daten zunächst in ein Testsystem rückgesichert werden. Die Umsetzung der Datensicherung obliegt dem Kunden.

Dokumentationen der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Böbingen (E.2)
- Fernwartung TeamViewer (G.1)

D.41 Z-ATLAS Import (SaaS)

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Vorga-

ben zur Passwortkomplexität sind vorhanden. Neue Benutzer können lediglich durch die ecovium eingerichtet werden.

Die Daten jedes Kunden werden in individuellen Datenbankenschemata abgelegt. Darüber hinaus können innerhalb seiner Datenbank auf Kundenwunsch weitere Mandanten angelegt werden.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Änderungen sind nur der ecovium möglich.

Zu Wartungszwecken kann sich die ecovium direkt auf die Datenbanken aufschalten oder per Webbrowser auf die Programmumgebung zugreifen. Hierfür werden verschlüsselte Verbindungen verwendet.

Datensicherungen werden auf Basis eines Sicherungskonzepts regelmäßig erstellt.

Es gibt diverse Dokumentationen zum Produkt. Spezifische Dokumentation der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Böbingen (E.2)
- Rechenzentrum Microsoft Azure (F.5)

D.42 Z-ATLAS Import Legacy (On-Premise)

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Vorgaben zur Passwortkomplexität werden nicht gemacht. Der Kunde erhält von der ecovium einen Standard-Admin-Account. Es obliegt dem Kunden, die weiteren Zugangsdaten individuell zu vergeben.

Die Software ist mandantenfähig. Wenn es die Lizenz es zulässt, können daher mehrere Mandanten angelegt werden. Die Daten der unterschiedlichen Mandanten sind softwareseitig getrennt.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Die Endkonfiguration liegt jedoch beim Kunden.

ecovium hat im Falle einer Wartung nur durch vorherige Freischaltung des Kunden Zugriff auf die Systeme. Auf Kundenwunsch kann auch eine permanente Verbindung eingerichtet werden, über die ecovium dann ohne separate Freischaltung zugreifen kann. Fernwartungen finden über verschlüsselte Verbindungen statt.

Datensicherungen und Rücksicherungen sind mit dem System möglich. Zum einen können Exportdateien erstellt und zum anderen auch Dumps der Datenbanken erzeugt werden. Rücksicherungen sind auch testweise möglich.

Bei Updates können beispielsweise Daten zunächst in ein Testsystem rückgesichert werden. Die Umsetzung der Datensicherung obliegt dem Kunden.

Es gibt diverse Dokumentationen zum Produkt. Spezifische Dokumentation der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Böbingen (E.2)
- Fernwartung TeamViewer (G.1)

D.43 Z-ATLAS Import Legacy (SaaS)

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Vorgaben zur Passwortkomplexität sind nicht vorhanden. Neue Benutzer können lediglich durch die ecovium eingerichtet werden.

Die Daten jedes Kunden werden in individuellen Datenbankenschemata abgelegt. Darüber hinaus können innerhalb seiner Datenbank auf Kundenwunsch weitere Mandanten angelegt werden.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Änderungen sind nur der ecovium möglich.

Zu Wartungszwecken kann sich die ecovium direkt auf die Datenbanken oder per Remote-Desktop aufschalten. Hierfür werden verschlüsselte Verbindungen verwendet.

Datensicherungen werden auf Basis eines Sicherungskonzepts regelmäßig erstellt.

Es gibt diverse Dokumentationen zum Produkt. Spezifische Dokumentation der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Böbingen (E.2)
- Rechenzentrum Microsoft Azure (F.5)

D.44 Z-EMCS

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Vorga-

ben zur Passwortkomplexität sind nicht vorhanden. Neue Benutzer können lediglich durch die ecovium eingerichtet werden.

Die Daten jedes Kunden werden in individuellen Datenbankenschemata abgelegt. Darüber hinaus können innerhalb seiner Datenbank auf Kundenwunsch weitere Mandanten angelegt werden.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Änderungen sind nur der ecovium möglich.

Zu Wartungszwecken kann sich die ecovium direkt auf die Datenbanken aufschalten. Hierfür werden verschlüsselte Verbindungen verwendet.

Datensicherungen werden auf Basis eines Sicherungskonzepts regelmäßig erstellt.

Es gibt diverse Dokumentationen zum Produkt. Spezifische Dokumentation der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Böbingen (E.2)
- Rechenzentrum Microsoft Azure (F.5)

D.45 Z-GBS (On-Premise)

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Vorgaben zur Passwortkomplexität sind nicht vorhanden. Der Kunde erhält von der ecovium einen Standard-Admin-Account. Es obliegt dem Kunden, die weiteren Zugangsdaten individuell zu vergeben.

Passworte der Benutzer werden nur als Hash in der Datenbank hinterlegt und sind nicht zurückrechenbar.

Die Software ist mandantenfähig. Wenn es die Lizenz es zulässt, können daher mehrere Mandanten angelegt werden. Die Daten der unterschiedlichen Mandanten sind softwareseitig getrennt.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Die Endkonfiguration liegt jedoch beim Kunden.

ecovium hat im Falle einer Wartung nur durch vorherige Freischaltung des Kunden Zugriff auf die Systeme. Fernwartungen finden über verschlüsselte Verbindungen statt.

Datensicherungen und Rücksicherungen sind mit dem System möglich. Zum einen können Exportdateien erstellt und zum anderen auch Dumps der Datenbanken erzeugt werden. Zusätzlich können auch Datenarchivierungen auf die Festplatte vorgenommen werden. Rücksicherungen sind auch testweise

möglich. Bei Updates können beispielsweise Daten zunächst in ein Testsystem rückgesichert werden. Die Umsetzung der Datensicherung obliegt dem Kunden.

Es gibt diverse Dokumentationen zum Produkt. Spezifische Dokumentation der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Böbingen (E.2)
- Fernwartung TeamViewer (G.1)

D.46 Z-GBS (SaaS)

Das System sieht eine Benutzerverwaltung vor, sodass sich jeder Anwender über einen eigenen Benutzernamen und Passwort anmelden muss. Vorgaben zur Passwortkomplexität sind nicht vorhanden. Neue Benutzer können lediglich durch die ecovium eingerichtet werden.

Die Daten jedes Kunden werden in individuellen Datenbanken abgelegt. Darüber hinaus können innerhalb seiner Datenbank auf Kundenwunsch weitere Mandanten angelegt werden.

Das System wird grundsätzlich mit datenschutzfreundlichen Einstellungen ausgeliefert. Änderungen sind in der Regel nur der ecovium möglich. Je nach Berechtigung kann der Kunde verschiedene Einstellungen auch eigenständig vornehmen.

Zu Wartungszwecken kann sich die ecovium über eine Webschnittstelle zugreifen oder direkt auf die Datenbanken aufschalten. Hierfür werden verschlüsselte Verbindungen verwendet.

Datensicherungen werden auf Basis eines Sicherungskonzepts regelmäßig erstellt. Auf Kundenwunsch können zusätzliche Datenarchivierungen erstellt werden, auf die der Kunde per FTP zugreifen kann.

Es gibt diverse Dokumentationen zum Produkt. Spezifische Dokumentation der tatsächlichen Installation sind vom Kunden selbst zu erstellen.

Teilweise werden Unterauftragsverarbeiter eingesetzt, mit denen eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde.

Für dieses Produkt sind zusätzlich die folgenden TOMs zu beachten:

- Standort Böbingen (E.2)
- Rechenzentrum Microsoft Azure (F.5)

E. Standortbezogene TOMs

Abweichend von den allgemeinen TOMs werden in diesem Abschnitt die spezifischen TOMs einzelner Standorte beschrieben.

E.1 Standort Bielefeld

Der Standort wird mit einer Alarmanlage abgesichert, die auf einen externen Wachschutz aufgeschaltet ist. Die Schar-Unscharf-Schaltung erfolgt per Transponder.

Die Eingänge sind mit einem manuellen Schließsystem ausgestattet. Die Ausgabe der Schlüssel und Transponder an die Mitarbeiter wird protokolliert.

Besucher können das Gebäude nicht frei betreten. Sie müssen schellen und werden durch den Empfang eingelassen. Innerhalb des Gebäudes werden Besucher durch Mitarbeiter begleitet. Handwerker oder andere Techniker, die sich im Gebäude ggf. freier bewegen können, werden auf Geheimhaltung verpflichtet.

Serversysteme sind in einem abgeschlossenen Serverraum untergebracht. Zugriff haben nur wenige Administratoren. Außerdem ist die Tür des Serverraums separat über die Alarmanlage gesichert. Der Raum wird bezüglich Feuchtigkeit und Temperatur überwacht. Es gibt eine Klimaanlage und Feuerlöschgeräte. Die Stromversorgung erfolgt über Schutzsteckdosen. Außerdem ist eine Notstromversorgung vorhanden.

Datenträger mobiler Endgeräte werden zusätzlich mittels Bitlocker bzw. Veracrypt verschlüsselt.

Ein Zugriff von außerhalb in das Unternehmensnetzwerk ist mittels verschlüsselter VPN-Verbindung möglich. Der Zugang ist über eine eigenständige Hardware-Firewall gesichert. Auf den Client-Systemen gibt es eine Software-Firewall und einen Virenscanner.

Datenträger werden bei Entsorgung bzw. Wiederverwendung datenschutzgerecht gelöscht bzw. geschreddert. Hierfür wird unter anderem ein externer Auftragsverarbeiter eingesetzt.

Datensicherungen werden auf Basis eines Backupkonzepts erstellt und permanent kontrolliert. Eines testweise Rücksicherung findet regelmäßig statt. Darüber hinaus gibt es einen Notfallplan.

E.2 Standort Böbingen

Der Standort wird mit einer Alarmanlage abgesichert, die auf einen externen Wachschutz aufgeschaltet ist. Die Schar-Unscharf-Schaltung erfolgt per Fingerabdrucksensor.

Die Eingänge sind mit einem manuellen Schließsystem ausgestattet. Die Ausgabe der Schlüssel an die Mitarbeiter wird protokolliert.

Besucher können das Gebäude nicht frei betreten. Sie müssen schellen und werden durch den Empfang eingelassen. Innerhalb des Gebäudes werden Besucher durch Mitarbeiter begleitet. Handwerker oder andere Techniker, die sich im Gebäude ggf. freier bewegen können, werden auf Geheimhaltung verpflichtet.

Serversysteme sind in einem abgeschlossenen Serverraum untergebracht. Zugriff haben nur wenige Administratoren. Der Raum wird bezüglich Feuchtigkeit und Temperatur überwacht. Es gibt eine Klimaanlage und einen Feuerlöscher vor dem Serverraum. Die Stromversorgung erfolgt über Schutzsteckdosen. Außerdem ist eine Notstromversorgung vorhanden.

Ein Zugriff von außerhalb in das Unternehmensnetzwerk ist mittels verschlüsselter VPN-Verbindung möglich. Der Zugang ist über eine eigenständige Hardware-Firewall gesichert. Auf den Client-Systemen gibt es eine Software-Firewall und einen Virenscanner.

Datenträger werden bei Entsorgung bzw. Wiederverwendung datenschutzgerecht gelöscht bzw. geschreddert. Hierfür gibt es eine Datenschutztonne, deren Inhalt durch einen externen Auftragsverarbeiter vernichtet werden.

Datensicherungen werden je nach Anforderung täglich oder teilweise wöchentlich erstellt.

E.3 Standort Düsseldorf

Das Gebäude ist über den Inhaber mit einer Alarmanlage abgesichert, die auf einen externen Wachschutz aufgeschaltet ist.

Für den Zutritt zum Gebäude und den Büroräumen ist ein Transponder notwendig. Einzelne Bereiche/Büros und der Serverraum sind darüber hinaus mit einem manuellen Schließsystem ausgestattet. Die Ausgabe der Schlüssel und Transponder an die Mitarbeiter wird protokolliert.

Besucher können das Gebäude nicht frei betreten. Sie müssen schellen und werden durch den Empfang eingelassen. Innerhalb der Büroräume werden Besucher durch Mitarbeiter begleitet. Handwerker oder andere Techniker, die sich in den Büroräumen ggf. freier bewegen können, werden auf Geheimhaltung verpflichtet. Besucher werden protokolliert.

Serversysteme sind in einem abgeschlossenen Serverraum untergebracht. Zugriff haben nur wenige Administratoren. Außerdem ist die Tür des Serverraums separat über die Alarmanlage gesichert. Der Raum wird bezüglich Feuchtigkeit und Temperatur überwacht. Es gibt eine Klimaanlage und ein Feuerlöschsystem im Serverraum. Die Stromversorgung erfolgt über Schutzsteckdosen. Außerdem ist eine Notstromversorgung vorhanden.

Datenträger mobiler Endgeräte werden zusätzlich mittels Bitlocker bzw. Veracrypt verschlüsselt.

Ein Zugriff von außerhalb in das Unternehmensnetzwerk ist mittels verschlüsselter VPN-Verbindung möglich. Der Zugang ist über eine eigenstän-

dige Hardware-Firewall gesichert. Auf den Client-Systemen gibt es eine Software-Firewall und einen Virenscanner.

Datenträger werden bei Entsorgung bzw. Wiederverwendung datenschutzgerecht gelöscht bzw. geschreddert. Dafür gibt es Datenschutztonnen, deren Inhalt über einen externen Auftragsverarbeiter entsorgt und vernichtet wird.

Datensicherungen werden auf Basis eines Backupkonzepts erstellt und permanent kontrolliert. Eines testweise Rücksicherung findet regelmäßig statt. Darüber hinaus gibt es einen Notfallplan.

E.4 Standort Neustadt

Die Eingänge sind mit einem manuellen Schließsystem ausgestattet. Die Türen können alternativ aber auch mit einem Transponder geöffnet werden. Die Ausgabe der Schlüssel und Transponder an die Mitarbeiter wird protokolliert.

Besucher können das Gebäude nicht frei betreten. Sie müssen schellen und werden durch den Empfang eingelassen. Innerhalb des Gebäudes werden Besucher durch Mitarbeiter begleitet. Handwerker oder andere Techniker, die sich im Gebäude ggf. freier bewegen können, werden auf Geheimhaltung verpflichtet.

Serversysteme sind in einem abgeschlossenen Serverraum untergebracht. Zugriff haben nur wenige Administratoren. Der Raum wird bezüglich Temperatur überwacht. Es gibt zwei redundante Klimaanlage und vor dem Serverraum Feuerlöschgeräte (CO2- und Trockenlöscher). Die Stromversorgung erfolgt über Schutzsteckdosen. Außerdem ist eine Notstromversorgung vorhanden.

Datenträger mobiler Endgeräte werden mittels Bitlocker verschlüsselt.

Ein Zugriff von außerhalb in das Unternehmensnetzwerk ist mittels verschlüsselter VPN-Verbindung möglich. Der Zugang ist über eine eigenständige Hardware-Firewall gesichert. Auf den Client-Systemen gibt es eine Software-Firewall und einen Virenscanner.

Ein Zugriff per Fernwartung von Dienstleistern kann nur mit vorheriger Freischaltung erfolgen. Die Verbindungen sind verschlüsselt.

Datenträger werden bei Entsorgung bzw. Wiederverwendung datenschutzgerecht gelöscht bzw. geschreddert. Hierfür wird unter anderem ein externer Auftragsverarbeiter eingesetzt. Vor Ort gibt es hierfür Container (Papier und elektronische Datenträger), die dann vom Dienstleister abgeholt werden.

Datensicherungen werden auf Basis eines Backupkonzepts erstellt und permanent kontrolliert.

E.5 Standort Norderstedt

Der Standort wird mit einer Alarmanlage abgesichert, die auf einen externen Wachschutz aufgeschaltet ist. Die Schar-Unscharf-Schaltung erfolgt per Schlüsselschalter.

Die Eingänge sind mit einem manuellen Schließsystem ausgestattet. Die Ausgabe der Schlüssel und Transponder an die Mitarbeiter wird protokolliert.

Das Gebäude, in dem auch andere Unternehmen angesiedelt sind, kann während der Arbeitszeiten durch Besucher frei betreten werden. Diese können sich aber nur im Treppenhaus frei bewegen. Die Türen zu den Bürotrakten sind versperrt und Besucher müssen schellen. Sie werden durch einen Beschäftigten eingelassen. Innerhalb des Bürotraktes werden Besucher durch Mitarbeiter begleitet. Handwerker oder andere Techniker, die sich im Gebäude ggf. freier bewegen können, werden auf Geheimhaltung verpflichtet.

Serversysteme sind in einem abgeschlossenen Serverraum untergebracht. Zugriff haben nur wenige Administratoren. Außerdem ist die Tür des Serverraums separat über die Alarmanlage gesichert. Der Raum wird bezüglich Feuchtigkeit und Temperatur überwacht. Es gibt eine Klimaanlage und Feuerlöschgeräte. Die Stromversorgung erfolgt über Schutzsteckdosen. Außerdem ist eine Notstromversorgung vorhanden.

Ein Zugriff von außerhalb in das Unternehmensnetzwerk ist mittels verschlüsselter VPN-Verbindung möglich. Der Zugang ist über eine eigenständige Hardware-Firewall gesichert. Auf den Client-Systemen gibt es eine Software-Firewall und einen Virenscanner.

Datenträger werden bei Entsorgung bzw. Wiederverwendung datenschutzgerecht gelöscht bzw. geschreddert. Hierfür gibt es Datentonnen, deren Inhalt von einem externen Auftragsverarbeiter vernichtet werden.

Datensicherungen werden auf Basis eines Backupkonzepts erstellt und permanent kontrolliert. Eines testweise Rücksicherung findet regelmäßig statt. Darüber hinaus gibt es einen Notfallplan.

E.6 Standort Pforzheim

Die Eingänge sind mit einem manuellen Schließsystem ausgestattet. Die Ausgabe der Schlüssel und Transponder an die Mitarbeiter wird protokolliert.

Das Gebäude, in dem auch andere Unternehmen angesiedelt sind, kann während der Arbeitszeiten durch Besucher frei betreten werden. Diese können sich aber nur im Treppenhaus frei bewegen. Die Türen zu den Bürotrakten sind versperrt und Besucher müssen schellen. Sie werden durch einen Beschäftigten eingelassen. Innerhalb des Bürotraktes werden Besucher durch Mitarbeiter begleitet. Handwerker oder andere Techniker, die sich im Gebäude ggf. freier bewegen können, werden auf Geheimhaltung verpflichtet.

Serversysteme sind in einem abgeschlossenen Serverraum untergebracht. Zugriff haben nur wenige Administratoren. Der Raum wird bezüglich Feuchtigkeit und Temperatur überwacht. Es gibt eine Klimaanlage und einen Feuerlöscher im Serverraum. Die Stromversorgung erfolgt über Schutzsteckdosen. Außerdem ist eine Notstromversorgung vorhanden.

Datenträger mobiler Endgeräte werden mittels Bitlocker verschlüsselt.

Ein Zugriff von außerhalb in das Unternehmensnetzwerk ist mittels verschlüsselter VPN-Verbindung möglich. Der Zugang ist über eine eigenständige Hardware-Firewall gesichert. Auf den Client-Systemen gibt es eine Software-Firewall und einen Virenscanner.

Datenträger werden bei Entsorgung bzw. Wiederverwendung datenschutzgerecht gelöscht bzw. geschreddert. Hierfür gibt es Datentonnen, deren Inhalt von einem externen Auftragsverarbeiter vernichtet werden.

Datensicherungen werden regelmäßig erstellt und permanent kontrolliert. Eines testweise Rücksicherung findet sporadisch statt. Darüber hinaus gibt es einen Notfallplan.

E.7 Standort Würzburg

Die Eingänge sind mit einem manuellen Schließsystem ausgestattet. Die Ausgabe der Schlüssel an die Mitarbeiter wird protokolliert.

Besucher können das Gebäude nicht frei betreten. Sie müssen schellen und werden durch den Empfang eingelassen. Innerhalb des Gebäudes werden Besucher durch Mitarbeiter begleitet. Handwerker oder andere Techniker, die sich im Gebäude ggf. freier bewegen können, werden auf Geheimhaltung verpflichtet.

Serversysteme (Testsysteme zur Entwicklung von Kundenanwendungen) sind in einem abgeschlossenen Serverraum untergebracht. Zugriff haben nur wenige Administratoren. Es gibt eine Klimaanlage sowie vor dem Serverraum Feuerlöschgeräte (CO2- und Trockenlöscher). Die Stromversorgung erfolgt über Schutzsteckdosen. Außerdem ist eine Notstromversorgung vorhanden.

Datenträger mobiler Endgeräte werden mittels Bitlocker verschlüsselt.

Ein Zugriff von außerhalb in das Unternehmensnetzwerk ist mittels verschlüsselter VPN-Verbindung möglich. Der Zugang ist über eine Hardware-Firewall gesichert. Auf den Client-Systemen gibt es eine Software-Firewall und einen Virenscanner.

Ein Zugriff per Fernwartung von Dienstleistern kann nur mit vorheriger Freischaltung erfolgen. Die Verbindungen sind verschlüsselt.

Datenträger werden bei Entsorgung bzw. Wiederverwendung datenschutzgerecht gelöscht bzw. geschreddert. Vor Ort gibt es hierfür Container (Papier und elektronische Datenträger), die dann vom Dienstleister abgeholt werden.

F. Rechenzentren

In diesem Abschnitt sind die TOMs verschiedener Rechenzentren beschrieben.

F.1 Rechenzentrum AWS

Innerhalb des Rechenzentrums sind mehrere virtuelle Server installiert. Auf diesen werden die Datenbanken und Anwendungen zur Verfügung gestellt. Gehostet werden alle Leistungen am Rechenzentrumsstandort Frankfurt. Lediglich ein FTP-Server zum Datenaustausch mit Kunden liegt in Irland.

Die ecovium greift über die Weboberfläche AWS-Console mittels verschlüsselter Verbindung zu Administrationszwecken zu. Für den Zugriff ist eine Zwei-Faktor-Authentifizierung notwendig.

Darüber hinaus kann mittels SSH über einen verschlüsselten VPN-Zugang auf die Server zugegriffen werden.

Weitere Informationen zu den Sicherheitsvorkehrungen bei AWS finden Sie unter folgenden Links:

- https://aws.amazon.com/de/compliance/eu-data-protection/
- https://aws.amazon.com/de/compliance/gdpr-center/
- https://aws.amazon.com/de/professional-services/security-assurance-services/

F.2 Rechenzentrum DigitalOcean

Beim Dienstleister DigitalOcean hat die ecovium mehrere virtuelle Server im Rechenzentrum Frankfurt im Einsatz. Die zugehörigen Host-Systeme werden vom Dienstleister verwaltet.

Über eine Weboberfläche kann die ecovium die virtuellen Server administrieren. Auf die virtuellen Maschinen (Linux) hat die ecovium Root-Zugriff per SSH. Zugriff haben nur wenige Administratoren.

Datensicherungen der virtuellen Maschinen erfolgen regelmäßig über den Betreiber.

Für dieses Rechenzentrum sind zusätzlich die folgenden TOMs zu beachten:

- Standort Düsseldorf (E.3)

Weitere Informationen zu den Sicherheitsvorkehrungen bei DigitalOcean finden Sie unter folgenden Links:

- https://www.digitalocean.com/security
- https://www.digitalocean.com/legal/data-processing-agreement

F.3 Rechenzentrum docuware

Die SaaS-Lösung docuware wird direkt vom Anbieter gehostet. Die ecovium hat selbst keinen Zugriff auf diese Daten. Für Unterstützungsleistungen muss die ecovium per TeamViewer auf Client-Rechner des Kunden zugreifen, was nur mit dessen Zustimmung möglich ist.

Für dieses Rechenzentrum sind zusätzlich die folgenden TOMs zu beachten:

- Standortbezogene TOMs (E)
- Fernwartung TeamViewer (G.1)

Weitere Informationen zu den Sicherheitsvorkehrungen bei docuware finden Sie unter folgenden Links:

- http://go.docuware.com/TOMs-EMEA
- https://go.docuware.com/Subcontractors-cloud

F.4 Rechenzentrum Hetzner

Beim Dienstleister Hetzner hat die ecovium mehrere dedizierte Server im Rechenzentrum Falkenstein angemietet. Diese werden zwar vom Dienstleister hardwaremäßig betreut, jedoch hat der Dienstleister keine Zugangsdaten zum Server auf Betriebssystem- oder Softwareebene.

Zu Wartungszwecken wird mittels SSH direkt auf die Server zugegriffen. Die Verbindungen sind verschlüsselt. Zugriff haben nur wenige Administratoren.

Die Server sind überwiegend redundant ausgelegt. Datensicherungen der Server erfolgen täglich und werden auf den eigenen Servern bei Hetzner abgelegt. Zusätzlich erfolgt eine Spiegelung zum Standort Bielefeld.

Für dieses Rechenzentrum sind zusätzlich die folgenden TOMs zu beachten:

- Standort Bielefeld (E.1)

Weitere Informationen zu den Sicherheitsvorkehrungen bei Hetzner finden Sie unter folgenden Links:

- https://www.hetzner.com/de/unternehmen/rechenzentrum/
- https://www.hetzner.com/de/unternehmen/zertifizierung
- https://www.hetzner.com/de/assets/Uploads/downloads/Sicherheit.pdf
- https://www.hetzner.com/AV/TOM.pdf

F.5 Rechenzentrum Microsoft Azure

Es gibt zwei verschiedene Arten, wie ecovium das Rechenzentrum von Microsoft nutzt:

- Azure Managed Services

  Microsoft stellt über die eigene Infrastruktur verschiedene Ressourcen zur Verfügung: Rechenzeit, Storage, bereitgestellte Applikationen. Diese werden von ecovium verwendet, um die eigenen Anwendungen zu betreiben und Daten zu speichern. Nur Microsoft hat Kontrolle darüber, auf welchen physikalischen Systemen Daten gespeichert und verteilt werden.

  Der Zugriff auf die Ressourcen erfolgt über von Microsoft betriebene APIs und Web-UIs. Alle Verbindungen zwischen Microsoft und ecovium sind dabei verschlüsselt.

  Datensicherungen werden von der ecovium eigenständig erstellt und in anderen Bereichen der Microsoft-Azure-Umgebung gespeichert.

  Es gibt für jeden Administrator bei der ecovium einen eigenen Benutzer. Änderungen an den Applikationen werden zusammen mit dem Benutzernamen protokolliert.

- Virtuelle Server

  Innerhalb des Rechenzentrums sind mehrere virtuelle Server installiert. Auf diesen werden die Datenbanken und Anwendungen zur Verfügung gestellt. Gehostet werden alle Leistungen an dem Rechenzentrumsstandort Europe West (Niederlande).

  Zu administrativen Zwecken wird über eine verschlüsselte VPN-Verbindung mittels Remote-Desktop auf diese zugegriffen.

Für dieses Rechenzentrum sind zusätzlich die folgenden TOMs zu beachten:

- Standortbezogene TOMs (E)
- Fernwartung Remote-Desktop (G.2)

Weitere Informationen zu den Sicherheitsvorkehrungen bei Microsoft finden Sie unter folgenden Links:

- https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security
- https://learn.microsoft.com/en-us/azure/storage/common/storage-service-encryption
- https://azure.microsoft.com/en-gb/blog/advancing-indatacenter-critical-environment-infrastructure-availability/
- https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-bearing-device-destruction

F.6 Rechenzentrum Myloc BNS Cloud-Dienste

Beim Dienstleister myLoc managed IT AG hat die ecovium mehrere dedizierte Server im Rechenzentrum Düsseldorf angemietet. Diese werden zwar vom Dienstleister hardwaremäßig betreut, jedoch hat der Dienstleister keine Zugangsdaten zum Server auf Betriebssystem- oder Softwareebene.

Für den Wartungszugriff auf die Server greift ecovium mittels Remote-Desktop zu. Die Firewall des Dienstleisters ist so konfiguriert, dass nur mittels der IP-Adresse des ecovium-Strandorts Düsseldorf zugegriffen werden kann. Zugriff haben nur wenige Administratoren.

Datensicherungen der Server erfolgen täglich und werden extern bei einem Backup-Dienstleister gespeichert.

Für dieses Rechenzentrum sind zusätzlich die folgenden TOMs zu beachten:

- Standort Düsseldorf (E.3)
- Fernwartung Remote-Desktop (G.2)

Weitere Informationen zu den Sicherheitsvorkehrungen bei myLoc finden Sie unter folgenden Links:

- https://www.myloc.de/colocation/rechenzentrum-duesseldorf.html

F.7 Rechenzentrum PlusServer

Beim Dienstleister PlusServer hat die ecovium mehrere dedizierte Server im Rechenzentrum Köln angemietet. Diese werden zwar vom Dienstleister hardwaremäßig betreut, jedoch hat der Dienstleister keine Zugangsdaten zum Server auf Betriebssystem- oder Softwareebene.

Für den Wartungszugriff wird aus dem internen Netzwerk der ecovium per Citrix über verschlüsselte Verbindungen zugegriffen. Darüber lassen sich per vSphere und mittels Remote-Desktop die Server ansteuern. Zugriff haben nur wenige Administratoren.

Datensicherungen der Server erfolgen täglich und werden bei PlusServer auf einem separaten Storage-System gespeichert.

Für dieses Rechenzentrum sind zusätzlich die folgenden TOMs zu beachten:

- Standortbezogene TOMs (E)
- Fernwartung Remote-Desktop (G.2)

Weitere Informationen zu den Sicherheitsvorkehrungen bei PlusServer finden Sie unter folgenden Links:

- https://www.plusserver.com/mehr-entdecken/ressourcen

G. Fernwartungstools

In diesem Abschnitt sind die TOMs der eingesetzten Fernwartungstools beschrieben.

G.1 Fernwartung TeamViewer

Zur Fernwartung von Kundeninstallationen (OnPremise) oder auch Servern der ecovium wird je nach Anwendung das Fernwartungstool des Unterauftragsverarbeiters TeamViewer verwendet. Hierbei sind alle Datenverbindungen verschlüsselt.

Je nach Kundenanforderung ist der Zugriff auf Kundensysteme per TeamViewer durch die ecovium in jedem Einzelfall durch den Kunden freizugeben. Auf Kundenwunsch kann die Verbindung auch so eingerichtet werden, dass ecovium zu jeder Zeit ohne Einzelfreigabe des Kunden zugreifen kann.

Weitere Informationen zur TeamViewer-Lösung und den damit verbunden Sicherheitsmaßnahmen des Unterauftragsverarbeiters finden Sie unter folgenden Links:

- https://www.teamviewer.com/de/trust-center/

G.2 Fernwartung Remote-Desktop

Zur Fernwartung von Kundeninstallationen (OnPremise) oder auch Servern der ecovium wird je nach Anwendung per Remote-Desktop zugegriffen. Hierbei sind alle Datenverbindungen verschlüsselt.

Je nach Kundenanforderung ist der Zugriff auf Kundensysteme durch die ecovium in jedem Einzelfall durch den Kunden freizugeben. Auf Kundenwunsch kann die Verbindung auch so eingerichtet werden, dass ecovium zu jeder Zeit ohne Einzelfreigabe des Kunden zugreifen kann.

Weitere Informationen zur Remote-Desktop und den damit verbunden Sicherheitsmaßnahmen finden Sie unter folgenden Links:

- https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-rdpbcgr