Dokumentenhistorie

Version	Bearbeitet durch	Änderungen	Veröffentlichung
1	Pascal Alich (pascal.alich@resourcify.de), Felix Heinricy (felix.heinricy@resourcify.de)	Erstellung der Vorlage des IT-Sicherheitskonzepts für das Resourcify Wertstoff Management System	29.07.2019
2	Pascal Alich (pascal.alich@resourcify.de), Felix Heinricy (felix.heinricy@resourcify.de), Daniel Scheu (daniel.scheu@resourcify.de)	Spezifische Ausgestaltung und Anpassung des IT-Sicherheitskonzepts	29.09.2020

Inhaltsverzeichnis

1 Einführung und Gegenstand des IT-Sicherheitskonzepts

Im Zeitalter der Digitalisierung und Nachhaltigkeit sollen die Prozesse des Abfallmanagements an den einzelnen Standorten des Kunden abgebildet, Abfalldaten digitalisiert und weitere effiziente Funktionalitäten durch eine Software as a Service Lösung unter Berücksichtigung der Anforderungen der Entsorgungsbranche bereitgestellt werden. Die Software as a Service Lösung soll zunächst für die Entsorgung über alle Abfallarten an allen Anfallstellen, Abfallsammelstellen sowie für Baustellen eingesetzt werden.

Resourcify ist Anbieter für digitale Lösungen in der Entsorgungsbranche und wird für den Kunden eine cloud-basierte Software as a Service Lösung mit der Bezeichnung WIP (Waste Information Portal) bereitstellen und betreiben.

IT-Sicherheit stellt einen Teil der Informationssicherheit dar. Sie umfasst die Sicherheit von IT-Systemen, Netzen und Anwendungen sowie der darin gespeicherten Daten durch Realisierung und Aufrechterhaltung geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung der Schutzziele der IT-Sicherheit (Vertraulichkeit, Verfügbarkeit und Integrität).

Es sind technisch-organisatorische Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO zu entwickeln, um die Sicherheit der Verarbeitung der Daten sowie die Durchsetzung der Rechte der Betroffenen (Auskunft, Berichtigung, Einschränkung der Bearbeitung, Löschung sowie Mitteilungs- und Benachrichtigungspflichten) zu gewährleisten, und der Rechenschaftspflicht nachkommen zu können.

Folgende Rahmenbedingungen sollen stets gewährleistet werden:

- Die **Vertraulichkeit** von Daten (z. B. Schutz vor unbefugter Kenntnisnahme von Dateiinhalten),
- die **Verfügbarkeit** der Systeme (z. B. Schutz vor Diebstahl, Zerstörung, Ausfallzeiten, Verlust von Datenträgern),
- die **Integrität** der Software und der Daten (z. B. Schutz vor vorsätzlicher oder fahrlässiger Verfälschung von Programmen, Manipulation von Dateien).

Dieses IT-Sicherheitskonzept dient der Optimierung der Informationssicherheit für die Bereitstellung und den Betrieb von WIP durch Resourcify und soll dazu beitragen, bestehende und künftige Prozesse weiter im Hinblick auf eine sichere Verarbeitung der Daten zu optimieren. In diesem Dokument sind die aktuell getroffenen technisch-organisatorischen IT-Sicherheits-Maßnahmen beschrieben.

2 Lösungsarchitektur

WIP ist eine mandantenfähige, cloudbasierte Web-Anwendung, die durch Resourcify für den Kunden als Software-as-a-Service-Lösung (SaaS) in Form einer Private Cloud Lösung bereitgestellt und betrieben wird.

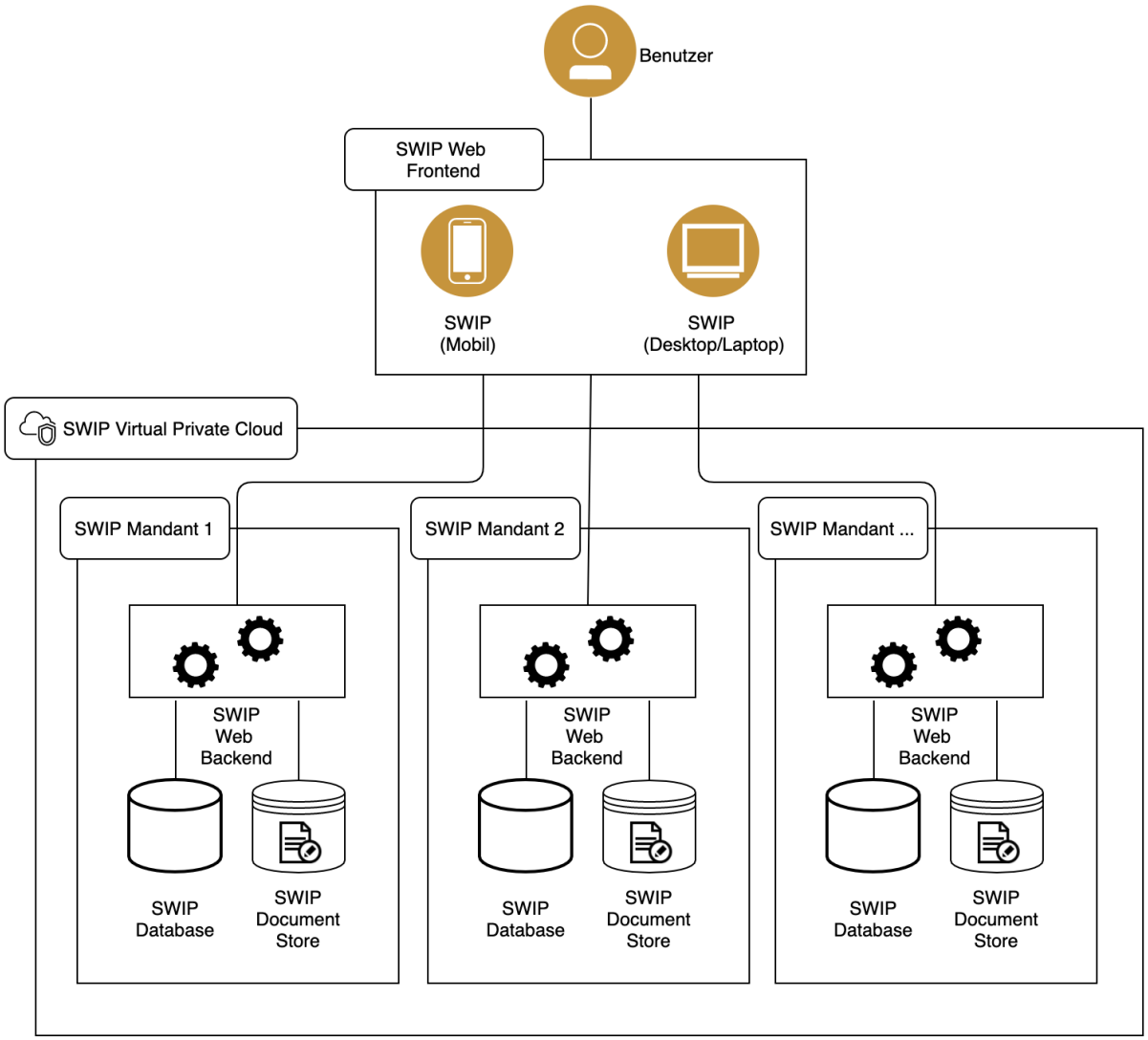

Abbildung: WIP-Lösungsarchitektur

2.1 Virtual Private Cloud

WIP wird in der Open Telekom Cloud (OTC) als virtuelle Umgebung (Virtual Private Cloud) gehostet und ist somit als Web-Anwendung im Internet verfügbar. Der Zugriff auf WIP erfolgt ausschließlich webbasiert von internetfähigen Endgeräten (Smartphone, Tablet, Desktop, Laptop), auf denen ein zu WIP kompatibler Browser installiert ist. Hier ist anzumerken, dass WIP grundsätzlich nur Browser unterstützt, die vom Hersteller noch regelmäßig mit (Sicherheits-)Updates versorgt werden. Sämtliche Datenübertragungen zwischen

Web-Frontend und -Backend sowie Datenübertragungen zu externen Systemen sind mit HTTPS oder äquivalent verschlüsselt und abgesichert. Es findet keine unverschlüsselte Datenübertragung in WIP statt.

2.2 Security Best Practices

WIP wird unter Berücksichtigung gängiger Sicherheits-Best-Practices für die Entwicklung und den Betrieb von Web-Anwendungen bereitgestellt. Dazu zählen beispielsweise:

- Sämtliche Daten-Übertragungen finden nur verschlüsselt statt (HTTPS).
- Geheime Informationen wie Benutzer-Passwörter werden nur stark kryptografisch abgesichert (in Form sog. “salted hashes”) gespeichert, so dass kein direkter Rückschluss auf das Passwort möglich ist.
- WIP-Benutzer haben nur Zugriff auf Daten und Funktionen, auf die sie gemäß der zugeordneten Rollen und Berechtigungen Zugriff haben (Details dazu im Abschnitt “Vertraulichkeit”).
- In der Software sind technische Schutzmaßnahmen, z. B. zum Schutz vor Angriffen wie SQL-Injections oder XSS-Attacken, berücksichtigt und umgesetzt.
- Die Server-Infrastruktur wird in abgeschotteten, virtualisierten Umgebungen mit jeweils minimalen technischen Berechtigungen betrieben (Sandboxing).
- Datenschutz & Compliance des Hosting-Providers: Die Open Telekom Cloud ist DSGVO-konform und verfügt beispielsweise über eine Zertifizierung nach Trusted Cloud Datenschutz Profil (TCPD) 1.0.
- Die Software-Komponenten des WIP-Technologie-Stacks werden regelmäßig aktualisiert, z. B. umfasst dies auch Sicherheits-Updates.

3 Technische Maßnahmen

In den folgenden Abschnitten sind die technischen IT-Sicherheits-Maßnahmen beschrieben.

3.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

3.1.1 Authentifizierung

Die Autorisierung eines Nutzers in WIP erfolgt mandantenspezifisch über das jeweilige WIP-Backend. Sämtliche WIP-Berechtigungen eines Nutzers werden ausschließlich im WIP-Backend des jeweiligen Mandanten gepflegt. Jeder Mandant autorisiert einen Nutzer spezifisch anhand der Rollen und Berechtigungen, die dem Nutzer im jeweiligen Mandanten zugewiesen sind. So kann beispielsweise der gleiche Nutzer in manchen Mandanten Vollzugriff, in anderen Mandanten eingeschränkten Zugriff und in anderen Mandanten gar keinen Zugriff haben.

3.1.2 Autorisierung - Rollen- und Berechtigungskonzept

In WIP erfolgt die Autorisierung eines Nutzers anhand der zugewiesenen Rollen- und Berechtigungen. Somit erhalten Nutzer nur Zugriff auf Daten und Funktionen, für die sich entsprechend berechtigt wurden. WIP bietet dazu ein feingranular steuerbares Rollen- und Berechtigungskonzept, dass sich rein durch Konfiguration flexibel auf die Bedürfnisse der einzelnen Mandanten anpassen lässt. Das Rollen- und Berechtigungskonzept basiert auf **Berechtigungen, Rollen und Berechtigungsebenen**, die flexibel miteinander verknüpft und einem Nutzer zugewiesen werden können.

3.1.3 Weitere Zugriffs-, Speicher- und Benutzerkontrolle

Es erfolgt kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen von Daten und Funktionen innerhalb des Systems:

- Sämtliche Cloud-Server sind nur mit SSH-Schlüsseln zugänglich
- Sämtliche vertrauliche Konfigurationsdaten wie z. B. Passwörter des technischen Datenbanknutzers für die SQL-Datenbank oder geheime Schlüssel zur Ansteuerung von Third-Party-APIs (z.B. OBS[1]) sind verschlüsselt gespeichert und nur denjenigen Mitarbeitern zugänglich, die in Aufgaben der System- und Anwendungsadministration eingewiesen und betraut sind.

[1] Object Storage Service - hochverfügbarer Dienst für die Datenspeicherung in der Open Telekom Cloud

3.1.4 Trennbarkeit

In WIP erfolgt eine getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden. Unterschiedliche Organisationseinheiten und Legal Entities können als separate Mandanten innerhalb der WIP Private Cloud eingerichtet werden. Jeder WIP-Mandant verfügt über eine dedizierte virtuelle Umgebung mit einer dedizierten Instanz des WIP-Web-Backends sowie eigener Datenbank (für Stamm- und Bewegungsdaten) und eigenem Document Store (für Dokumente/Binärdaten).

Jeder Mandant erhält eine eigene URL, über die das webbasierte WIP-Web-Frontend abgerufen werden kann.

Pro Mandant stehen getrennte Systeme, Datenbanken und Document Stores für Test, Demo und Produktion zur Verfügung.

3.1.5 Gesicherte Datenübertragung

Im Rahmen des Projektverlaufs und späteren Betriebs werden Resourcify und der Kunde außerhalb der Web-Anwendung WIP Daten austauschen (Stammdaten zur Aufbereitung und zum Import, Daten im Rahmen von Support-Anfragen, Schulungs-Dokumente etc.). Eine Übertragung dieser Daten erfolgt nur über ausreichend gesicherte Kommunikationskanäle, wie z. B. verschlüsselte E-Mails, einem Microsoft Teams Workspace oder Projektmanagement-Tools wie Basecamp oder Jira. Die genaue Auswahl der Kommunikations- und Kollaborations-Tools erfolgt im weiteren Verlauf des Projekts und Berücksichtigung der IT-Sicherheitsanforderungen.

3.1.6 IT-Service Continuity Management

Sollte es zu einer Unterbrechung des WIP-Service aufgrund eines Konfigurationsfehlers oder einer technischen Störung kommen, wird Resourcify über die Unterbrechung und sofern bekannt die Störungsursache sowie voraussichtliche Dauer informieren. In der Regel sollte es durch den vorübergehenden Ausfall einer Server-, Netzwerk- oder Speicher-Komponente nicht zu einem Datenverlust kommen und der Service steht nach Beseitigung der Störung wieder zur Verfügung.

Die virtualisierten Infrastruktur-Services sind auf ein hohes Maß an Verfügbarkeit und Redundanz ausgelegt. Sollte es dennoch im Rahmen einer Störung notwendig werden, einen WIP-Mandanten komplett wiederherzustellen, steht dazu ein tagesaktuelles Backup bzw. datiert vor dem letzten Release-Deployment zur Verfügung. Durch die Kombination mit dem Infrastructure-As-Code-Ansatz kann so im Worst-Case-Szenario kurzfristig ein WIP-Mandant wiederhergestellt werden.

3.2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

3.2.1 Transportkontrolle

Zum Schutz vor unbefugtem Lesen, Kopieren, Verändern oder Entfernen von Daten bei der elektronischer Übertragung oder Transport gelten folgende Maßnahmen:

- SSL/TLS-Transportverschlüsselung zwischen Endgerät und Server.
- Zugang für Administratoren nur über SSH.

3.2.2 Eingabekontrolle

WIP bietet die Möglichkeit, festzustellen, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eine Nachverfolgung von Änderungen an Stamm- und Bewegungsdaten erfolgt mit Hilfe der Audit-Logging-Funktion in WIP.

3.2.3 Datenintegrität

In WIP sind folgende Maßnahmen umgesetzt, die eine Beschädigung von Daten durch Fehlfunktionen des Systems verhindern:

- Ein technischer Fehler innerhalb der Software führt zu einem “Rollback” der Transaktion. Änderungen werden gemäß ACID[2]-Prinzip ganz oder gar nicht ausgeführt, um die Datenintegrität auch im Fehlerfall zu gewährleisten.
- Ein tägliches Backup der Datenbank-Inhalte wird auf einem separaten System vorgehalten, mit dessen Hilfe das System bei Bedarf vollständig wiederhergestellt werden kann.

3.2.4 Deployment Management

Die Software-Verteilung (Deployment Management) verfügt über einen hohen Automatisierungsgrad und verschiedene Staging und Qualitätssicherungs-Mechanismen. Hierzu setzt Resourcify eine Versionsverwaltung mit einer Continuous Integration/Deployment (CI/CD) Pipeline ein.

3.2.5 Infrastructure und Platform Management

Das technische Management der IT-Infrastruktur und IT-Plattformen (Infrastructure and Platform Management), insb. der physischen Infrastruktur an sich erfolgt zu einem großen Teil durch den Hosting Provider Open Telekom Cloud und wird Resourcify als virtualisierte Infrastruktur (Infrastructure-as-a-Service) bereitgestellt. Dies umfasst die benötigten Speicher-, Server- und Netzwerkressourcen und ermöglicht eine schnelle, hochgradig

[2] ACID - Atomicity, Consistency, Isolation und Durability

verfügbare und skalierbare Bereitstellung der benötigten IT-Ressourcen, die passgenau auf die Anforderungen zugeschnitten werden kann.

Darauf basierend verwaltet Resourcify die gesamte virtuelle Infrastruktur nach dem Infrastructure-as-Code Prinzip in verschlüsselten Repositories. Das bedeutet, dass die benötigte Infrastruktur so wie Programmcode beschrieben wurde. Dies lässt sich sich jederzeit anpassen und versionieren, so dass sämtliche Änderungen an der virtuellen Infrastruktur transparent sind und sich jederzeit detailliert nachvollziehen lassen. Die Infrastruktur wird somit in gleichem Maße „testbar“ wie die Software selbst. Neben der technischen Infrastruktur (Speicher, Server, Netzwerk) umfasst der Ansatz auch sämtliche Konfigurationseinstellungen eines WIP-Mandanten (wie z. B. technische Parameter, Software-Version, Schnittstellen-Konfiguration, Feature-Toggles), die Bestandteil der externen Konfiguration des WIP-Mandanten sind. Durch die hier beschriebenen Mechanismen werden ebenso das Release- und Deployment Management sowie die Service Asset und Konfigurationsverwaltung abgebildet.

3.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

3.3.1 Verfügbarkeitskontrolle

Zum Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, werden regelmäßige Backups wie im Punkt “Datenintegrität” beschrieben erstellt.

3.3.2 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Das System kann aus dem letzten Backup unter Zuhilfenahme des Infrastructure-As-Code-Prinzips schnell wiederhergestellt werden. Das Vorgehen dafür ist gut protokolliert und wird durch Resourcify regelmäßig getestet.

3.3.3 Monitoring

Die Funktionalität des Systems wird durch diverse Monitoring-Tools (z. B. SMS- und E-Mail-Benachrichtigung bei Nichtverfügbarkeit, automatische Neustarts bei Ausfall eines Services) überwacht.

4 Organisatorische Maßnahmen

In den folgenden Abschnitten sind die organisatorischen IT-Sicherheits-Maßnahmen beschrieben. Die organisatorischen Maßnahmen gelten für alle internen und externen Mitarbeiterinnen und Mitarbeiter von Resourcify, die mit der Implementierung und dem Betrieb von WIP betraut sind.

4.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

4.1.1 Zugangskontrolle

Mit folgenden Maßnahmen wird einem unbefugten Zutritt zu Datenverarbeitungsanlagen vorgebeugt:

- Die Büroräume sind durch Chipkarte + elektronische Schlüssel gesichert
- Zeitgesteuerter Zugang des Haupteingangs

4.1.2 Datenträgerkontrolle

Mit folgendem Maßnahmen wird einem unbefugtem Lesen, Kopieren, Verändern oder Löschen von Datenträgern vorgebeugt:

- Für Laptops und verwendete externe Dienste ist die Verwendung von sicheren Kennwörtern notwendig.
- Bei Verlassen des Büros müssen Laptops gesperrt werden.
- Zur Absicherung bei Diebstahl/Verlust kommt eine Festplattenverschlüsselung zum Einsatz.

4.1.3 Sensibilisierung der Mitarbeiter

Alle Mitarbeiter sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis verpflichtet bzw. darüber unterrichtet. Sie und sonstige relevante Personen (extern Beschäftigte und Kooperationspartner) werden systematisch und zielgruppengerecht zu Datenschutzfragen sensibilisiert und zum Umgang mit personenbezogenen Daten geschult.

4.2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

4.2.1 Software-Qualität

Zur Wahrung der Integrität und zur Sicherung der Softwarequalität hat Resourcify folgende Elemente fest in den Service-Prozessen verankert:

- **Review der Anforderungen**: Eingehende Business-Anforderungen (Change Requests) werden durch Reviews qualitätsgesichert, bevor entsprechende Lösungskonzepte erarbeitet werden.
- **Review der Lösungskonzepte**: Erarbeitete fachliche sowie technische Lösungskonzepte werden zusammen mit dem Kunden durch Reviews qualitätsgesichert, bevor diese in die technische Implementierung gehen.
- **Technische Implementierung mit automatisierten Modultest**: Bei der technischen Implementierung werden automatisierte Modultests entwickelt, die regelmäßig durch Entwickler sowie bei Release-Erstellung innerhalb der CI Pipeline ausgeführt werden.
- **Code-Reviews**: Entwickelter Quellcode wird durch min. einen erfahrenen Entwickler geprüft, bevor dieser Bestandteil eines Release wird.
- **Automatisierte Integrations- und Systemtests:** Für grundlegende Funktionalität werden automatisierte Integrations- und Systemtests entwickelt, die sowohl durch Entwickler als auch in der CI Pipeline automatisiert ausgeführt werden.
- **Interne Release-Abnahme**: Nach der Release-Erstellung erfolgt zunächst eine interne Abnahme auf dem Entwicklungssystem durch das Produktmangement.
- **Externe Release-Abnahme:** Nach der internen Release-Freigabe erfolgt eine externe Abnahme auf dem Demo-System.
- **Automatisiertes Produktiv-Deployment**: Nach erfolgter externer Abnahme erfolgt (manuell angestoßen) ein automatisiertes Deployment auf das Produktivsystem inkl. Erstellung von Backups.

4.2.2 4-Augen-Prinzip für Konfigurationsänderungen

Da Fehler in der Systemkonfiguration im schlimmsten Fall zum Ausfall eines Mandanten führen können, erfolgen sämtliche Änderungen an der System-Konfiguration nur nach dem 4-Augen-Prinzip, um Fehler zu vermeiden.

4.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

4.3.1 Verfügbarkeitskontrolle

Mit folgenden Maßnahmen werden die Daten und System gegen gegen zufällige oder mutwillige Zerstörung bzw. Verlust geschützt:

- Nutzung von zuverlässigen Cloud-Hosting-Anbietern.

4.3.2 Zuverlässigkeit

Mit folgenden Maßnahmen wird die Verfügbarkeit aller Funktionen des Systems und eine standardisierte Fehlermeldung im Fehlerfall sichergestellt:

- Vor der Inbetriebnahme jeder neuen Software-Version erfolgt systematisches Testen.
- Für Nutzerfragen und die Meldung von Fehlern ist eine Support-E-Mail-Adresse und -Telefonnummer verfügbar. Die Abwicklung von Support-Anfragen inkl. Dokumentation von Lösungen und Workarounds erfolgt über ein Support-Tool (JIRA Service Desk).

4.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

4.4.1 Datenschutz-Management

Für das Datenschutz-Management verfügt Resourcify über einen Datenschutzbeauftragen.

4.4.2 Incident-Response-Management

Das Incident-Response-Management wird durch den Datenschutzbeauftragten unterstützt.

4.4.3 Auftragskontrolle

Es erfolgt keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers:

- Die Auswahl von Dienstleistern erfolgt anhand strenger Kriterien.
- Mit Dienstleistern erfolgt eine eindeutige Vertragsgestaltung im Sinne der Auftragsverarbeitung.
- Es finden diesbezüglich regelmäßige Nachkontrollen der Dienstleister statt.