ISAE 3000 TYP 1 Bericht

D3EIF GmbH

zum Stichtag 30. September 2023

06. Februar 2025

BDO

D3EIF GmbH, Linz

ISAE 3000 Bericht – Typ 1

Prüfbericht des unabhängigen Prüfers über die Entwicklung und Betrieb der Software „DRIP“ sowie der Konzeption und Einrichtung ausgewählter Kontrollen zum Stichtag 30. September 2023.

BDO Assurance GmbH
Wirtschaftsprüfungs- und Steuerberatungsgesellschaft

Inhaltsverzeichnis

1. BERICHTSBESTANDTEIL I: BESTÄTIGUNGSVERMERK DES UNABHÄNGIGEN PRÜFERS

An die: D3EIF GmbH

Prüfungsauftrag

Mit Schreiben vom 15. Februar 2023 wurden wir, BDO Assurance GmbH Wirtschaftsprüfungs- und Steuerberatungsgesellschaft, von der D3EIF GmbH (kurz „D3EIF“) beauftragt, eine Prüfung des von der D3EIF beschriebenen Dienstleistungssystems in Bezug auf den Geltungsbereich „Entwicklung und Betrieb der Software DRIP“ sowie der Konzeption und Einrichtung der von D3EIF ausgewählten Kontrollen in Bezug auf die dargestellten Kontrollziele nach den Inhalten von ISAE 3000 (Typ I) zum 30. September 2023 durchzuführen.

Verantwortung der D3EIF

Die D3EIF ist verantwortlich für:

- Erbringung der Dienstleistungen, die von der Beschreibung des Dienstleistungssystems umfasst sind
- Vorbereitung einer Beschreibung ihres Dienstleistungssystems, der begleitenden Erklärung der gesetzlichen Vertreter sowie der Vollständigkeit und Richtigkeit und Darstellungsmethode der Beschreibung und der Erklärung
- Darstellung der Funktionen, die bei der Beschreibung des Dienstleistungssystems der Dienstleistungsorganisation umfasst sind
- Festlegung der Kontrollziele (sofern diese nicht zB durch Gesetze oder eine andere Regelung identifiziert wurden)
- Konzeption und Einrichtung der Kontrollen, die - unter Berücksichtigung von Risikoaspekten – zur Erreichung festgelegter Kontrollziele im Einsatz sind
- Auswählen und Festlegen geeigneter Beurteilungskriterien, die als Basis für die Abgabe der Erklärung der gesetzlichen Vertreter herangezogen werden
- Aufsetzen und Unterschreiben der Erklärung der gesetzlichen Vertreter

Verantwortung des Prüfers

Unsere Aufgabe ist es, auf der Grundlage der von uns durchgeführten Prüfung, ein Prüfungsurteil darüber abzugeben, ob

- die Beschreibung des Dienstleistungssystems die tatsächliche Konzeption und Einrichtung des Systems inklusive des internen Kontrollsystems in allen wesentlichen Belangen richtig und klar darstellt,
- die Konzeption der in der Beschreibung dargestellten Kontrollen zur Erreichung der in der Beschreibung des Dienstleistungssystems dargestellten Kontrollziele angemessen war und
- die in der Beschreibung dargestellten Kontrollen eingerichtet waren.

Wir haben unsere Prüfung in Einklang mit dem Fachgutachten des Fachsenats für Unternehmensrecht und Revision der Kammer der Wirtschaftstreuhänder über die Durchführung von sonstigen Prüfungen KFS/PG 13, sowie dem Standard ISAE 3000 (International Standard on Assurance Engagements other than Audits or Reviews of Historical Financial Information) durchgeführt.

Wir haben im Rahmen unserer Prüfung folgende von Sub-Dienstleistungsorganisationen durchgeführte Dienstleistungen in unseren Prüfungshandlungen nicht berücksichtigt (Anwendung der Exklusiv-Methode):

- Rechenzentrumsbetrieb in der Cloud (Microsoft Azure)

Wir haben darüber hinaus keine Prüfungshandlungen mit dem Ziel durchgeführt, die Wirksamkeit von Kontrollen für irgendeinen Zeitraum festzustellen. Dementsprechend geben wir keine Beurteilung über die Wirksamkeit der Kontrollen der D3EIF weder im Einzelnen noch in ihrer Gesamtheit ab.

Immanente Grenzen der Berichterstattung und von Internen Kontrollsystemen

Die Beschreibung der D3EIF zielt auf die typischerweise von ihren Kunden und deren Prüfern erwarteten Inhalte ab. Daher kann es vorkommen, dass einzelne Aspekte des Dienstleistungssystems, die für einzelne Kunden und deren Umgebung als besonders wichtig erachtet werden, nicht zwingend berücksichtigt werden.

Die Beschreibung des Systems der Dienstleistungserbringung sowie die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Konzeption und Einrichtung einzelner Kontrollen erstreckten sich auf den Zeitpunkt zum 30. September 2023. Jede Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr in sich, dass aufgrund von durchgeführten Änderungen die beigefügte Beschreibung der Kontrollen nicht dem aktuellen Stand entspricht. Ebenso wird darauf hingewiesen, dass die Wirksamkeit eines internen Kontrollsystems sowie von einzelnen Kontrollen systemimmanenten Grenzen unterliegt, sodass naturgemäß nicht sämtliche falsche Angaben, Fehler oder Verstöße entdeckt oder verhindert werden können.

Ferner bergen Schlussfolgerungen für die Zukunft auf Grundlage unserer Feststellungen das Risiko, dass aufgrund von Änderungen des internen Kontrollsystems die Zulässigkeit dieser Schlussfolgerungen beeinträchtigt werden kann.

Nutzungsbeschränkung und Haftung

Diese Bestätigung ist ausschließlich zur Nutzung durch die gesetzlichen Vertreter der D3EIF sowie ihrer Kunden und deren Prüfern, die ausreichend Verständnis, zusammen mit sonstiger Information einschließlich der Kenntnis über Kontrollen, die in der auslagernden Organisation selbst durchgeführt werden, für die Evaluierung des Informationssystems des Kunden haben, bestimmt. Ansprüche anderer Personen können daher daraus nicht abgeleitet werden. Dementsprechend darf dieser Bericht weder gänzlich noch auszugsweise ohne unser ausdrückliches Einverständnis an andere Personen weitergegeben werden.

Wir erteilen diese Bestätigung auf Grundlage des von der D3EIF erhaltenen Auftrags, dem, auch mit Wirkung gegenüber Dritten, die beiliegenden Allgemeinen Auftragsbedingungen für Wirtschaftstreuhandberufe in der Fassung vom 18. April 2018 zu Grunde liegen.

Unsere Verantwortlichkeit und Haftung für nachgewiesene Vermögensschäden aufgrund einer fahrlässigen Pflichtverletzung ist bei unserer Beurteilung auf das Zehnfache der Mindestversicherungssumme gemäß § 11 WTBG 2017 jeweils in der geltenden Fassung begrenzt. Die mit dem Auftraggeber vereinbarte und hier offen gelegte Beschränkung unserer Haftung gilt auch gegenüber jedem Dritten, der im Vertrauen auf unseren Bericht über die von uns durchgeführte Beurteilung Handlungen setzt oder unterlässt.

Unsere Haftung für leichte Fahrlässigkeit wird in Übereinstimmung mit den Allgemeinen Auftragsbedingungen für Wirtschaftstreuhandberufe (abrufbar unter https://www.bdo.at/de-at/impressum-datenschutzerklarung-aab/aab), die diesem Auftrag zugrunde liegen, ausgeschlossen.

Prüfungsurteil

Nach unserer Überzeugung stellt die beigefügte Beschreibung der zuvor genannten Dienstleistung in allen wesentlichen Belangen zutreffend die zum 30. September 2023 eingerichteten ausgewählten Kontrollen in Bezug auf den Geltungsbereich „Entwicklung und Betrieb der Software DRIP“ dar. Weiterhin sind wir der Auffassung, dass die in der Beschreibung dargestellten Kontrollen angemessen waren, um mit hinreichender Sicherheit zu gewährleisten, dass die in der Beschreibung genannten Kontrollziele erreicht werden, unter der Voraussetzung, dass diese Kontrollen hinreichend beachtet werden.

Wien, am 06. Februar 2025

BDO Assurance GmbH
Wirtschaftsprüfungs- und Steuerberatungsgesellschaft

p.p.a. Peter

Peter Alfred Gruber, 06.02.2025 16:09
qualifiziert elektronisch signiert

Peter Gruber
Wirtschaftsprüfer, CISA

2. BERICHTSBESTANDTEIL II: ERKLÄRUNG DER GESETZLICHEN VERTRETER DER D3EIF GMBH

Die nachfolgende Beschreibung wurde für Kunden, die Leistungen der D3EIF GmbH beziehen und deren Abschlussprüfer sowie für den Abschlussprüfer und sonstige externe Prüfer der D3EIF GmbH zusammengestellt, welche ausreichende Kenntnis besitzen, um die Beschreibung sowie auch andere relevanten Informationen, insbesondere die vom Kunden selbst eingesetzten Kontrollen und die Informationssysteme, über die der Kunde verfügt, zu beurteilen.

Die D3EIF GmbH bestätigt, dass

(a) die nachfolgende Beschreibung (Berichtsbestandteil III) eine angemessene Darstellung der Entwicklung und des Betriebs der Software „DRIP“ zum 30. September 2023 gibt. Wir geben diese Erklärung auf Basis der Erfüllung folgender Kriterien ab:

(i) Die Beschreibung stellt dar, wie das Dienstleistungssystems entworfen und umgesetzt wurde, einschließlich:

- der zur Verfügung gestellten Services,
- der Verfahren für die relevanten IT-gestützten und manuellen Systeme und Abläufe, die für die Bereitstellung der Services verwendet wurden,
- der wesentlichen Kontrollziele und der Kontrollen, die entwickelt wurden, um diese Ziele zu erreichen,
- anderer Aspekte des Kontrollumfelds der Organisation, des Risikobeurteilungsprozesses, der Informations- und Kommunikationssysteme (einschließlich der relevanten Geschäftsprozesse), der Kontrollaktivitäten, und der für das System relevanten Überwachungskontrollen, die für die zur Verfügung gestellten Dienste und die Verarbeitung relevant waren.

(ii) Die Beschreibung lässt keine relevanten Informationen des dargestellten Systems aus oder stellt diese verfälscht dar – unter der Berücksichtigung, dass die Beschreibung darauf ausgerichtet ist, den üblichen Anforderungen der Kundenorganisationen und deren Abschlussprüfern zu genügen und nicht alle individuellen Aspekte einzelner Kunden oder Prüfer abzudecken.

b) die Kontrollen in Bezug auf die Kontrollziele, welche in der Systembeschreibung angegeben wurden, angemessen ausgestaltet und zum 30. September 2023 entsprechend ihrer Beschreibung eingerichtet waren. Wir geben diese Erklärung auf Basis der Erfüllung folgender Kriterien ab:

(i) Risiken, die die Erreichung der dargestellten Kontrollziele gefährden, wurden identifiziert.

(ii) Die in der Beschreibung angeführten Kontrollen gewährleisten mit hinreichender Sicherheit, dass diese Risiken die Erreichung der Kontrollziele nicht beeinträchtigen können, insofern die Kontrollen entsprechend ihrer Beschreibung durchgeführt werden.

Linz, 05. Februar 2025

D3EIF GmbH

Eduard Peterseil
Geschäftsführer

3. BERICHTSBESTANDTEIL III: BESCHREIBUNG DES DIENSTLEISTUNGSSYSTEMS

3.1. DAS UNTERNEHMEN

Das Startup D3EIF GmbH wurde am 28.9.2017 in Linz gegründet und ist ein österreichisches Softwareentwicklungsunternehmen.

Mit **DRIP** (Digital Realtime Information Platform) revolutioniert das Unternehmen die Logistikbranche, einer innovativen **SaaS-Lösung**, die Transparenz in der Lieferkette auf ein neues Niveau hebt. Diese Plattform verbindet Verlader (Industrie, produzierende Unternehmen), Spediteure und Transportunternehmen in wenigen Minuten und ermöglicht den automatisierten Austausch von GPS-Daten und Transportinformationen – **in Echtzeit** und ohne aufwendige IT-Integration. Damit werden blinde Flecken in der Logistik beseitigt, die Planungssicherheit erhöht und spürbare Effizienzgewinne für Kunden geschaffen.

Das Unternehmen beschäftigt aktuell 11 Mitarbeiter in den Bereichen Softwareentwicklung, Marketing, Sales und Personalmanagement.

Die Unternehmensstruktur ist dabei wie folgt definiert:

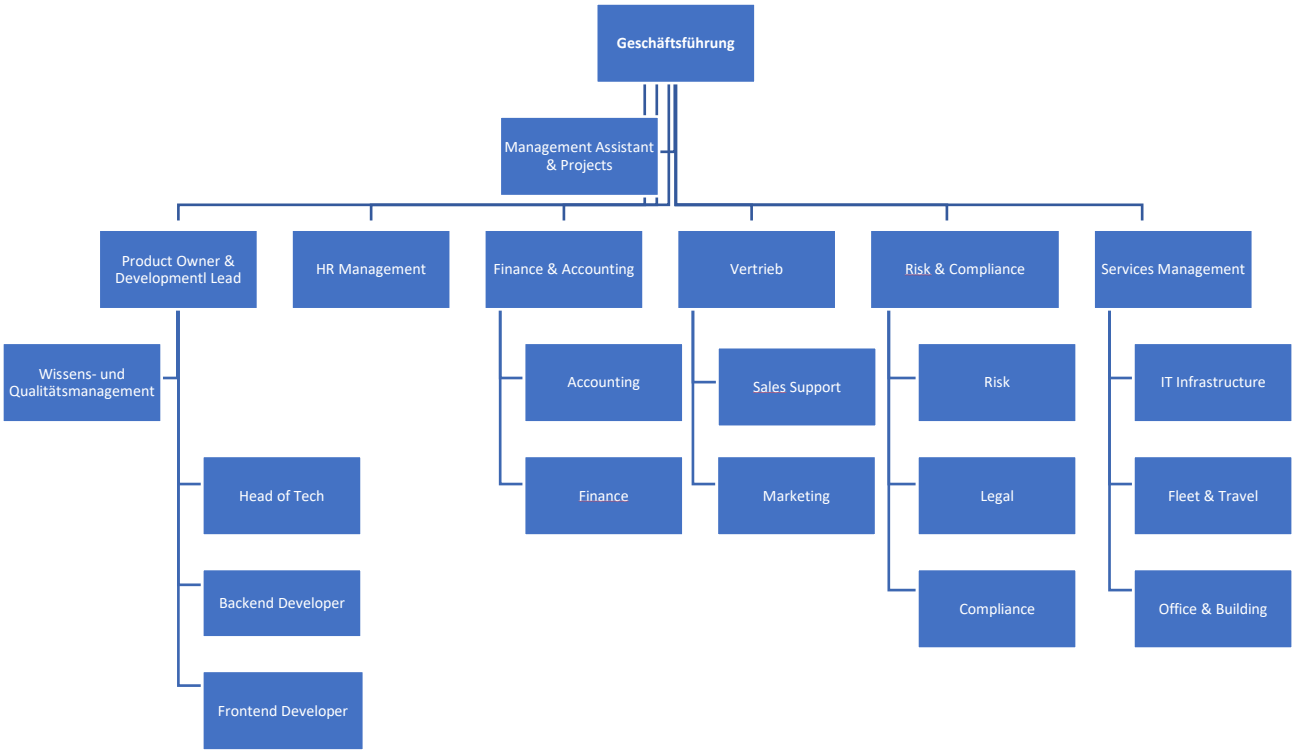


Abbildung 1: Unternehmensstruktur der D3EIF GmbH

Firmenbuch	Firmenstandort und Geschäftsjahr	Nominelles Kapital
Unternehmensgegenstand: Software-Entwicklung UID-Nummer: ATU72641046 Firmenbuchnummer: FN 479511 p	Linz (Austria) 01.01. – 31.12.	EUR 70.686

3.2. DAS GESCHÄFTSMODELL DER D3EIF

Mit DRIP bietet D3EIF eine Cloud-basierte Software as a Service (SaaS) Lösung. Der Einsatz von SaaS ermöglicht Kostenersparnisse, einfache Wartung und flexible Nutzung.

Das Bezahlmodell ist SaaS typisch, bei dem Grundfunktionen kostenlos angeboten werden während erweiterte Funktionen kostenpflichtig sind. Die Kombination von SaaS und Freemium ermöglicht eine breite Marktdurchdringung und profitables Wachstum.

3.3. DIE ANWENDUNG “DRIP”

DRIP steigert die Planbarkeit und die Transparenz in der Transportabwicklung exorbitant. Die Plattform zeigt alle relevanten Auftrags- und Telemetriedaten der unterschiedlichsten Transportflotten auf einen Blick. Egal ob es sich um Fahrzeuge unterschiedlicher Frächter einer Spedition oder einen Eigenfuhrpark mit Fahrzeugen unterschiedlicher Telematik-Systeme handelt.

DRIP gewährleistet die Visualisierung der gesamten Transportabwicklung an einem Ort. Es werden Nutzungsdaten wie GPS, Spritverbrauch, Temperatur, usw. aus unterschiedlichen Systemen harmonisiert und in einer Oberfläche visualisiert. Dadurch bietet DRIP einen Mehrwert zum Status Quo in vielen Unternehmen, in denen für die Beschaffung der gleichen Information eine große Menge an unterschiedlichen (Web-) Plattformen aufgerufen werden muss und somit der administrative Aufwand enorm hoch ist. Jeder Beteiligte in der Transportabwicklung (Spedition, Frächter, Lieferkunde) sieht zu jederzeit und sofort, wo die Fahrzeuge/Ladungen gerade unterwegs sind und in welchem Status sie sich befinden.

Über mobile Endgeräte ist das System an die Fahrerkommunikation angebunden. Es können auch Dokumente digitalisiert, Schäden gemeldet und über DRIP gesendet werden. Auch Fahrzeuge können verbunden werden (LKW und Trailer) um automatisiert Nachweise über Schadensverläufe (wer ist wann mit welchem Trailer gefahren) zu erlangen. Um eine reibungslose Kommunikation zu gewährleisten, bietet DRIP die Möglichkeit in der jeweiligen Landessprache zu kommunizieren. Echtzeitübersetzung in die jeweilige Landessprache verhindert somit Missinterpretation in der Kommunikation.

Durch die Zusammenführung von Transportmanagement Systemen (TMS) und Telematik Systemen können zudem geplante Ankunftszeiten (ETA - Estimated Time of Arrival) berechnet werden. Dazu werden die Termine und Ladestellen des TMS mit den Positionsdaten der Fahrzeuge, den Verkehrsdaten, sowie den Einsatzzeiten der LKW-Lenker verglichen. Dank der Echtzeitdaten können Verspätungen vorhergesagt und Mitarbeiter bzw. Kunden frühzeitig informiert werden. Es können auch weitere Daten (z.B. Temperatur im LKW) getrackt und bei Abweichungen gewarnt werden.

Der USP von DRIP liegt somit auf der technischen Komponente der Zusammenführung unterschiedlicher Telematik Systemen und der darauf aufbauenden Kommunikationsprozesse (Beauftragung, Avisierung, Rückmeldung, Exzeption Handling und Reporting).

3.4. TECHNISCHER ÜBERBLICK

Vor der Nutzung von DRIP ist es notwendig, dass der Kunde sich bei DRIP registriert und damit seinen persönlichen Account erstellt. Dabei ist es wichtig, dass sich pro juristischer Person (Unternehmen) nur ein Account registrieren lässt. Jeder Account in DRIP wird als Company bezeichnet. Innerhalb dieser Company gibt es ein Rollen und Gruppen Sicherheitskonzept.

Es existieren folgende Rollen:

- Administrator
- Subaccounts, eigene Rollen

Ein Unternehmen mit eigenen Fahrzeugen hat nun die Möglichkeit sein eigenes Telematiksystem mit DRIP zu verbinden. Um die Verbindung herzustellen kann es notwendig sein, bei dem Telematiksystem den Datenaustausch zu aktivieren. Anleitungen zu jedem Dritt-System sind in DRIP vorhanden.

Alle Daten, die von Drittsystemen an DRIP übertragen werden, sind immer nur in dem jeweiligen Account verfügbar. Wie beschrieben, regelt das Berechtigungs- und Gruppensystem den Zugriff auf die Daten, der in diesem Account angelegten zusätzlichen Benutzer.

Ein Teil der Informationen ist nur über eine vorherige Verbindung (Trusted Partner) zwischen zwei Accounts möglich. Dazu muss zuerst eine Einladung verschickt und von der empfangenen Partei akzeptiert werden.

3.4.1. REALTIME MONITOR

Ein Teil der Informationen (Position, Kennzeichen etc.) ist nur möglich, wenn zuerst mit dem Partnerunternehmen eine Verbindung (Trusted Partner) hergestellt wurde. Wenn diese Verbindung von beiden Seiten akzeptiert wurde, können einzelne Fahrzeuge bzw. ganze Gruppen von Fahrzeugen geteilt werden.

Das bedeutet, das Partnerunternehmen sieht in Echtzeit die Positionen der geteilten Fahrzeuge. Alle anderen Fahrzeuge, die nicht geteilt wurden, bleiben davon unberührt.

Jede Partei kann zu jeder Zeit die Verbindung trennen und stoppt somit den Informationsaustausch unverzüglich.

3.4.2. ARRIVAL MONITOR

Der Arrival Monitor ist für den Datenaustausch mit TMS-Systemen konzipiert. Hierbei ist es notwendig, dass erfolgreich geplante Transporte (Auftrag, Sendung, Tour) an DRIP über die Standard API übertragen werden. Nach erfolgreicher Übertragung findet ein gesichertes Matching statt. Das bedeutet, dass das geplante Fahrzeug dem Transport in DRIP zugeordnet wird. Eigene Fahrzeuge, die in dem eigenen Unternehmensaccount zugeordnet sind, werden sofort dem Pairing unterzogen. Bei Fremdfahrzeugen wird zuerst geprüft, ob es eine aufrechte Verbindung (Trusted Partner) gibt. Wenn „Ja“, dann findet das Pairing statt. Wenn „Nein“ kann (Einstellung in DRIP) der Unternehmer informiert werden, dass ein Auftrag verfügbar wäre. Es muss dann eine manuelle Bestätigung erfolgen.

Nach erfolgreichem Pairing wird von DRIP der Transport überwacht und mittels Geofence und weiteren Parameter wird schließlich die Freigabe an Dritte aktiviert. Wenn der Transport beendet wird, stoppt die Datenfreigabe automatisch.

3.4.3. DATENWEITERLEITUNG AN DRITTE (KUNDEN, DRITTSOFTWARE RTV)

Mit DRIP ist es möglich Daten nicht nur in bzw über DRIP zu verarbeiten, sondern auch an Dritte (Kunden, RTV-Provider usw.) weiterzuleiten. Dabei wird ganz besonders darauf geachtet, welche Daten weitergeleitet werden sollen. Dies kann von jedem DRIP-Kunden explizit gefordert werden. Hierzu gehört das Maskieren von Kennzeichen oder das Verschlüsseln von Positions- bzw. Unternehmer- und Fahrerdaten. Alle nicht relevanten Informationen werden nicht weitergeleitet.

3.4.4. INFRASTRUKTUR

Die DRIP-Plattform wird in einem Deutschen Microsoft Rechenzentrum betrieben. Microsoft ist verantwortlich für die neuesten Updates der Betriebssysteme auf den VMs sowie der Datenbankversionen. Der Zugriff in das Azure Portal ist mit einem MFA geschützt sowie über einen VPN-Tunnel verschlüsselt. Datenbankzugriffe werden per MFA-Autorisierung geschützt sowie eigener DRIP-spezifischen DB-Rolle. Darüber hinaus werden Zugriffe auf Datenbanken geschützt und protokolliert.

Der Zugriff auf die virtuelle Maschine, die auch in der Azure Cloud betrieben wird, ist via Username / Passwort sowie private Key geschützt.

Alle Verbindungen zu, von und innerhalb von DRIP, werden via HTTPS geschützt. Sprich alle übermittelten Daten werden mittels Zertifikats verschlüsselt. Darüber hinaus werden alle „public“ REST-Schnittstellen via Bearer Token autorisiert.

Alle HTTPS Verbindungen zu DRIP werden zentral geroutet und sind damit die einzigen Schnittstellen zum und vom Public Internet. Alle anderen Verbindungen werden in Azure intern abgewickelt.

3.4.5. INFORMATIONSSICHERHEIT UND DATENSCHUTZ

Informations- und Datensicherheit steht bei DRIP an oberster Stelle. Um sicherzustellen, dass Informationen nur an Berechtigte weitergegeben werden, wurde die Drip Data Privacy Principles entwickelt. Diese veranschaulichen wie Informationen in DRIP geteilt und weitergegeben werden. Sie sind in Anhang 3 detailliert dargestellt.

3.5. GELTUNGSBEREICH DES DIENSTLEISTUNGSBEZOGENEN INTERNEN KONTROLLSYSTEMS (DIKS)

Der Geltungsbereich des DIKS der D3EIF GmbH umfasst die Entwicklung und den Betrieb der Software „DRIP“.

3.6. AUSGELAGERTE DIENSTLEISTUNGEN

Der Rechenzentrumsbetrieb ist ausgelagert und wird in der Cloud bezogen (Microsoft Azure Europa).

3.7. STRUKTUR DES INTERNEN KONTROLLSYSTEMS (IKS)

Das IKS der D3EIF GmbH besteht aus einem Set individueller Kontrollen (das sog. „Kontrollframework“). Jede Kontrolle ist einem der folgenden Bereiche (sog. „Domänen“) zugeordnet:

- Zugriffskontrolle (ACCESS)
- Änderungen an der Software (CHANGE)
- Betrieb (OPERATION)
- Organisation (ORGANIZATION)

Kontrollframework

Die individuellen Kontrollen werden in einem zentralen Microsoft Excel Dokument verwaltet.

Für jede Kontrolle werden die folgenden Informationen gesammelt:

- ID
- Status
- Domäne
- Subdomäne
- Kontrollname
- Kontrollbeschreibung
- Kommentar zur Kontrollbeschreibung
- Nachweise zur Kontrolle
- Kontrollfrequenz
- Kontrollart (manuell, automatisch, etc.)
- Kontrolltyp (präventiv/detektiv)
- Kontrollverantwortlicher

Das interne Kontrollsystem und sein Kontrollframework werden regelmäßig gepflegt und unterliegen einem kontinuierlichen Verbesserungsprozess.

Auf den nachfolgenden Seiten sind die Kontrolldomänen, die Kontroll-Subdomänen sowie deren Ziele dargestellt. Die adressierten Risiken jeder Kontroll-Subdomäne sind im Anhang 1 und die Beschreibung der Kontrollen in Anhang 2 angeführt.

3.7.1. DOMÄNE: ACCESS

Logical Access Management

Sicherstellung, dass die Geschäfts- und Sicherheitsanforderungen in Bezug auf den logischen Zugang zu IT-Systemen und -Anwendungen der Organisation erfüllt werden.

Physical Access Management

Verhindern des unbefugten Zutritts zu Räumlichkeiten und Informationswerten, um sie vor Beschädigung, Unterbrechung, Missbrauch, Zerstörung und Diebstahl zu schützen.

3.7.2. DOMÄNE: CHANGE

Change Management

Gewährleistung der Nachvollziehbarkeit und Sicherheit bei Änderungen am Programmcode vom Zeitpunkt der Idee einer Änderung bis zu ihrer zufriedenstellenden Umsetzung.

Code Quality and Security

Gewährleistung der Sicherheit des Programmcodes durch Tests für sämtliche neue Features. Implementierung in das Live-System erfolgt ausschließlich nach erfolgreicher Freigabe.

3.7.3. DOMÄNE: OPERATION

Backup / Archiving

Sicherstellung, dass alle kritischen Daten der Organisation regelmäßig gesichert und archiviert werden, um Datenverlust zu verhindern und die Geschäftskontinuität zu gewährleisten.

License Management

Sicherstellung, dass alle Softwareanwendungen und Plattformen innerhalb der Organisation ordnungsgemäß lizenziert sind und dass die Nutzung von Software die Lizenzvereinbarungen nicht verletzt.

Mobile Device Management

Sicherstellung, dass alle mobilen Endgeräte, die innerhalb der Organisation verwendet werden, ordnungsgemäß verwaltet und überwacht sind, um die Unternehmensdaten und -ressourcen zu schützen.

Monitoring

Sicherstellung der kontinuierlichen Überwachung von IT-Systemen und Anwendungen, um die ständige Verfügbarkeit der Applikation zu gewährleisten und potenzielle Probleme frühzeitig zu erkennen und zu beheben.

Patch Management

Sicherstellung, dass alle IT-Systeme und Anwendungen der Organisation regelmäßig aktualisiert und mit den neuesten Sicherheitspatches und Updates versorgt werden, um potenzielle Schwachstellen zu schließen und die Systemintegrität zu gewährleisten.

Infrastructure Security

Sicherstellung der Informationssicherheit durch die Nutzung eines ISO 27001-zertifizierten Rechenzentrums sowie durch technische Sicherheitsüberprüfungen.

3.7.4. DOMÄNE: ORGANIZATION

Compliance

Sicherstellung, dass bei jeder Serviceerweiterung innerhalb der Organisation alle relevanten gesetzlichen, regulatorischen und branchenspezifischen Anforderungen erfüllt werden.

IT and Data Protection Risk Management

Sicherstellung der regelmäßigen Durchführung eines Datenschutz-Risiko Assessments im Quartalsrhythmus, um potenzielle Bedrohungen und Schwachstellen frühzeitig zu identifizieren und geeignete Schutzmaßnahmen zu implementieren.

ANHANG 1: BESCHREIBUNG DER KONTROLLDOMÄNEN UND ADRESSIERTEN RISIKEN

Kontroll-Domäne	Kontroll-Subdomäne	Ziel der Kontroll-Subdomäne	Adressierte Risiken
ACCESS	Logical Access	Sicherstellung, dass die Geschäfts- und Sicherheitsanforderungen in Bezug auf den logischen Zugang zu IT-Systemen und -Anwendungen der Organisation erfüllt werden.	• Unbefugte Vergabe von privilegierten Accounts und Benutzerrechten • Unautorisiertes Anmelden innerhalb der Anwendung • Verlust von Daten oder Datendiebstahl
	Physical Access	Verhindern des unbefugten Zutritts zu Räumlichkeiten und Informationswerten, um sie vor Beschädigung, Unterbrechung, Missbrauch, Zerstörung und Diebstahl zu schützen.	• Unbefugter Zutritt zu IT-Systemen • Verletzung der Vertraulichkeit • Nicht vorhandene Protokollierung der Zutritte • Verlust von Daten oder Datendiebstahl
CHANGE	Change-Management	Gewährleistung der Nachvollziehbarkeit und Sicherheit bei Änderungen am Programmcode vom Zeitpunkt der Idee einer Änderung bis zu ihrer zufriedenstellenden Umsetzung.	• unautorisierte Umsetzung von Änderungen • fehlerhafter oder unsicherer Programmcode
	Code Quality and Security	Gewährleistung der Sicherheit des Programmcodes durch Tests für sämtliche neue Features. Implementierung in das Live-System erfolgt ausschließlich nach erfolgreicher Freigabe.	• fehlerhafter oder unsicherer Programmcode • Fehler oder Bugs im Programmcode • Testdurchführung von nicht autorisierten Personen

OPERATION	Backup/Archiving	Sicherstellung, dass alle kritischen Daten der Organisation regelmäßig gesichert und archiviert werden, um Datenverlust zu verhindern und die Geschäftskontinuität zu gewährleisten.	• Verlust kritischer Daten aufgrund von Hardware- oder Softwareausfällen • Unfähigkeit Daten nach eine Sicherheitsvorfall oder Datenverlust wieder herzustellen • Beschädigung oder Verlust von Archivdaten, die für Compliance- oder Geschäftszwecke benötigt werden • Unzureichende oder veraltete Backup- und Archivierungsverfahren, welche die Datenwiederherstellung erschweren • Unautorisiertes Zugreifen oder Manipulieren von Backup- und Archivdaten.
	License Management	Sicherstellung, dass alle Softwareanwendungen und Plattformen innerhalb der Organisation ordnungsgemäß lizenziert sind und dass die Nutzung von Software die Lizenzvereinbarungen nicht verletzt.	• Rechtliche Konsequenzen und Strafen aufgrund von nicht lizenzierten oder falsch lizenzierten Softwareanwendungen • Unvorhergesehene Kosten durch den Kauf zusätzlicher Lizenzen oder Strafgebühren • Betriebsunterbrechungen aufgrund von Lizenzverletzungen • Sicherheitsrisiken durch den Einsatz veralteter oder nicht unterstützter Software-Versionen, für die keine gültige Lizenz vorhanden ist.
	Mobile Device Management	Sicherstellung, dass alle mobilen Endgeräte, die innerhalb der Organisation verwendet werden, ordnungsgemäß verwaltet und überwacht sind, um die Unternehmensdaten und -ressourcen zu schützen.	• Verlust oder Diebstahl von mobilen Endgeräten, die Unternehmensdaten enthalten • Physische oder digitale Angriffe, die die Schwachstellen mobiler Geräte ausnutzen. • Verbreitung von Malware oder anderen schädlichen Softwarekomponenten über mobile Endgeräte
	Monitoring	Sicherstellung der kontinuierlichen Überwachung von IT-Systemen und Anwendungen, um die ständige Verfügbarkeit der Applikation zu gewährleisten und potenzielle Probleme frühzeitig zu erkennen und zu beheben.	• Ungeplante Ausfallzeiten oder Unterbrechungen, die die Geschäftskontinuität beeinträchtigen • Datenverlust oder Datenkorruption aufgrund von nicht erkannten Systemproblemen

			• Nichterkennung von Anomalien oder ungewöhnlichen Aktivitäten, die auf Bedrohungen od. Missbrauch hinweisen könnten.
	Patch Management	Sicherstellung, dass alle IT-Systeme und Anwendungen der Organisation regelmäßig aktualisiert und mit den neuesten Sicherheitspatches und Updates versorgt werden, um potenzielle Schwachstellen zu schließen und die Systemintegrität zu gewährleisten.	• Sicherheitsverletzungen oder -angriffe aufgrund nicht gepatchter oder bekannter Schwachstellen • Datenverlust oder -korruption durch nicht aktualisierte oder unsichere Systeme • Systemausfälle oder -fehler aufgrund inkompatibler oder fehlerhafter Patches
	Infrastructure Security	Sicherstellung der Informationssicherheit durch die Nutzung eines ISO 27001-zertifizierten Rechenzentrums sowie durch technische Sicherheitsüberprüfungen.	• Sicherheitsverletzungen oder Datenlecks aufgrund von Schwachstellen oder Mängeln im Rechenzentrum • Betriebsunterbrechungen oder Systemausfälle aufgrund von Infrastrukturproblemen

ORGANIZATION	Compliance	Sicherstellung, dass bei jeder Serviceerweiterung innerhalb der Organisation alle relevanten gesetzlichen, regulatorischen und branchenspezifischen Anforderungen erfüllt werden.	• Rechtliche Sanktionen, Strafen oder Haftung aufgrund v. Nichteinhaltung gesetzlicher oder regulatorischer Vorschriften • Schädigung des Unternehmensrufs durch Nichteinhaltung von Compliance-Anforderungen • Finanzielle Verluste durch Strafen oder die Notwendigkeit, nicht konforme Serviceerweiterungen zurückzuziehen oder zu ändern
	IT and Data Protection Risk Management	Sicherstellung der regelmäßigen Durchführung eines Datenschutz-Risiko Assessments im Quartalsrhythmus, um potenzielle Bedrohungen und Schwachstellen frühzeitig zu identifizieren und geeignete Schutzmaßnahmen zu implementieren.	• Nichterkennung von Datenschutzrisiken, die zu Datenlecks oder Sicherheitsverletzungen führen könnten • Verzögerte Reaktion auf verändernde Bedrohungs-landschaften oder regulatorische Anforderungen aufgrund unzureichender Risikobewertung

ANHANG 2: BESCHREIBUNG DER KONTROLLEN

1. ACCESS

ID	Kontroll Sub-Domäne	Kontrollbezeichnung	Kontrollbeschreibung	Kontroll-frequenz	Kontrollart	Kontrolltyp
ID01	Logical Access	Nachweisliche Vergabe und Überprüfung privilegierter Accounts	Privilegierte Accounts bzw. Administratorenrechte werden ausschließlich auf Basis nachweislicher und begründeter Anforderungen vergeben.	anlassbezogen	manuell	präventiv
ID02	Logical Access	Überprüfung der Anzahl an Administratoren	Vierteljährlich erfolgt eine nachweisliche Überprüfung der Anzahl vergebener Administratorenrechte. Gegebenenfalls werden Korrekturmaßnahmen vorgenommen.	vierteljährlich	manuell	detektiv
ID03	Logical Access	Sicherstellung der Passwortsicherheit	Halbjährlich erfolgt eine nachweisliche Überprüfung der Einhaltung der Mindestanforderungen gemäß Passwortrichtlinie bezüglich Länge, Komplexitätskriterien und Wechselintervall.	halbjährlich	manuell	detektiv
ID04	Logical Access	Vergabe von Benutzerberechtigungen	Berechtigungen werden ausschließlich auf Gruppenebene basierend auf definierten Rollen vergeben.	n/a	manuell	präventiv
ID05	Logical Access	Single-Sing-On (SSO)	Alle Anwendungen werden, sofern technisch möglich, in das zentrale Access and Identity Management via SSO integriert.	n/a	manuell	präventiv
ID06	Logical Access	Multi-Factor-Authentication (MFA)	Der Zugriff auf die IT-Infrastruktur ist außerhalb des Unternehmensnetzwerks ausschließlich über Benutzername, Passwort und einem 2. Faktor (PIN, Token, Authenticator Freigabe) möglich.	n/a	automatisch	präventiv
ID07	Physical Access	Elektronisches Zutrittssystem	Der Zutritt zu den Büroräumlichkeiten ist durch ein elektronisches Zutrittssystem abgesichert und ausschließlich Personen mit einer zugehörigen Zugangskarte und	n/a	manuell	präventiv

ID	Kontroll Sub-Domäne	Kontrollbezeichnung	Kontrollbeschreibung	Kontroll-frequenz	Kontrollart	Kontrolltyp
			entsprechenden Rechten möglich. Jeder Zutritt wird protokolliert und bei Bedarf können entsprechende Logs beim Betreiber des Zutrittssystems angefordert werden. Alle Personen sind angewiesen das Büro beim Verlassen zu versperren, sollten sie dieses als Letzte(r) verlassen.			
ID08	Physical Access	Videoüberwachung	Der Eingangsbereich des Stiegenhauses im ersten Stock sowie der Gang nach der Bürohaupttüre werden videoüberwacht. Aufzeichnung erfolgen auf Hardware, welche sich in einem getrennten Abschnitt in einem Infrastruktur-Raum befindet.	n/a	automatisch	detektiv

2. CHANGE

ID	Kontroll Sub-Domäne	Kontrollbezeichnung	Kontrollbeschreibung	Kontroll-frequenz	Kontrollart	Kontrolltyp
ID09	Change Management	Software Change Management Prozess	Übernahme von Änderungen an der Software DRIP folgen einem geregelten und nachvollziehbarem Prozess, dessen einzelne Schritte nicht übersprungen werden können (z.B. von "In Progress" direkt zu "Done"). Zunächst wird ein sog. "Pull Request" eingereicht. Dieser muss von mindestens einer weiteren Person bestätigt werden. Nach der Bestätigung wird der Code auf dem Entwicklungs-Server bereitgestellt und dort einer weiteren Überprüfung unterzogen.	anlassbezogen	manuell	präventiv
ID10	Change Management	Funktionstrennung und Nachvollziehbarkeit bei Änderungen an der Software DRIP	Änderungen an der Software DRIP folgen dem Prinzip der Rollentrennung und werden durch eine funktionsseparate Freigabe gewährleistet. Alle Modifikationen werden lückenlos dokumentiert und systematisch archiviert.	anlassbezogen	manuell	präventiv
ID11	Code Quality and Security	Sicherstellung der Qualität der Entwicklung	Das D3EIF Management evaluiert die Anforderungen auf Business-Ebene. Die Compliance-Abteilung ist für die Überprüfung der rechtlichen Rahmenbedingungen zuständig. Nach Freigabe beider Parteien erfolgt eine Priorisierung. Alle	anlassbezogen	manuell	präventiv

ID	Kontroll Sub-Domäne	Kontrollbezeichnung	Kontrollbeschreibung	Kontroll-frequenz	Kontrollart	Kontrolltyp
			Entwicklungsarbeiten richten sich strikt nach den Vorgaben den Entwicklerrichtlinien.			
ID12	Code Quality and Security	Definierte Testläufe	Für sämtliche neue Features werden Tests erstellt, die automatisch im System durchgeführt werden. Bei der Integration auf dem Entwicklungs-Server werden alle Tests automatisch ausgeführt.	anlassbezogen	automatisch	detektiv
ID13	Code Quality and Security	Statische Codeanalyse	Zur statischen Codeanalyse wird ein Tool zum sog. "Linting" eingesetzt, welches mit strengen Sicherheitseinstellungen konfiguriert ist.	anlassbezogen	manuell	detektiv
ID14	Code Quality and Security	Funktionstests	Jeder Code-Durchlauf wird hinsichtlich seiner Funktionalität überprüft. Das Ergebnis muss eine nahtlose und fehlerfreie Integration in die zugehörigen Module gewährleisten. Die Testdurchführung darf nicht von der Person vorgenommen werden, die die Implementierung vorgenommen hat.	anlassbezogen	manuell	präventiv
ID15	Code Quality and Security	Sicherstellung der Qualität im Livesystem	Das Deployment auf das Live-System wird ausschließlich nach erfolgreicher Freigabe und nach durchgeführten Tests im Entwicklungssystem vorgenommen.	anlassbezogen	manuell	präventiv
ID16	Code Quality and Security	Abhängigkeitstests	Abhängigkeitschecks (sog. Dependency checks) werden bei jedem Build automatisch durchgeführt.	anlassbezogen	automatisch	detektiv

3. OPERATION

ID	Kontroll Sub-Domäne	Kontrollbezeichnung	Kontrollbeschreibung	Kontroll-frequenz	Kontrollart	Kontrolltyp
ID17	Backup / Archiving	Sicherstellung der Datenverfügbarkeit	Die entsprechenden Systeme und Datenbanken werden automatisch gesichert und es existieren zudem Repliken. E-Mails und Dokumente werden im ELO-System archiviert.	n/a	automatisch	präventiv
ID18	License Management	Sicherstellung der korrekten Lizenzierung	Einmal jährlich wird basierend auf der Microsoft Intune-Liste eine Lizenzüberprüfung durchgeführt. Die IT-Abteilung stellt diese Liste bereit und klärt gemeinsam mit der Geschäftsführung den aktuellen Lizenzierungsstatus.	jährlich	manuell	detektiv
ID19	Mobile Device Management	Sicherheit mobiler Endgeräte	Alle mobilen Endgeräte sind in Microsoft Intune integriert und werden darüber verwaltet. Es existiert eine Richtlinie, die bei längerer Abwesenheit eine automatische Sperrung der Geräte vorsieht, sowie eine Pflicht zur Verschlüsselung der Geräte und einen aktiven Antimalware-Schutz.	n/a	automatisch	präventiv
ID20	Monitoring	Sicherstellung der Verfügbarkeit der DRIP-Applikation	Kernfunktionen der DRIP-Software unterliegen einem Monitoring. Bei Abweichungen in der Funktionsweise erfolgen Benachrichtigen bzw. werden sofern möglich die betroffenen Tasks automatisch neu gestartet.	anlassbezogen	automatisch	detektiv
ID21	Patch Management	Sicherstellung der Aktualität der Systeme	Die Überprüfung der Software-Aktualität der Systeme am Live-System erfolgt alle 14 Tage. In den Feature-Meetings werden die Tickets diskutiert und entsprechend priorisiert. Linux-Maschinen für Entwicklung und Produktion werden in Wartungsfenstern aktualisiert. Für Clients wird das Microsoft Intune Dashboard verwendet, welches den aktuellen Sicherheitsstandard der Geräte ausweist.	2-wöchentlich	manuell	präventiv
ID22	Infrastructure Security	Auslagerung in ein ISO 27001 zertifiziertes Rechenzentrum	Es wird eine durch Microsoft bereitgestellte Infrastruktur genutzt. Die Systeme werden in einem nach ISO 27001 zertifizierten Rechenzentrum betrieben. Es erfolgt jährlich eine Überprüfung, ob der Rechenzentrumsbetreiber weiterhin über die entsprechende Zertifizierung verfügt.	n/a	manuell	präventiv
ID23	Infrastructure Security	Technische Sicherheitsüberprüfung	Jährlich erfolgt eine technische Sicherheitsüberprüfung (z.B. Penetration Test, Vulnerability Scan, etc.) der IT-Infrastruktur.	jährlich	manuell	detektiv

4. ORGANIZATION

ID	Kontroll Sub-Domäne	Kontrollbezeichnung	Kontrollbeschreibung	Kontroll-frequenz	Kontrollart	Kontrolltyp
ID24	Compliance	Prüfung auf Gesetzeskonformität im Falle einer Serviceerweiterung	Bei geplanten technischen Weiterentwicklungen und sonstigen Angebotserweiterungen erfolgt eine anlassbezogene Prüfung der Erlaubnispflichtigkeit. Das Vorhaben solcher Erweiterungen wird im Management-Meeting vorgestellt. Die Überprüfung gesetzlicher Anforderungen wird von der Compliance-Abteilung vorgenommen und in der Risikoliste dokumentiert und entsprechend verwaltet.	anlassbezogen	manuell	präventiv
ID25	IT and Data Protection Risk Management	Quartalweise Durchführung von IT- und Datenschutz-Risiko Assessments	Vierteljährlich erfolgt eine Bewertung bestehender sowie die Identifikation neuer IT-Risiken. Die Risiken werden systematisch dokumentiert und der Geschäftsführung vorgelegt.	vierteljährlich	manuell	präventiv

ANHANG 3: DRIP DATA PRIVACY PRINCIPLES

D^2P^2

DRIP DATA PRIVACY PRINCIPLES

DRIP

DRIP ist eine zentrale Plattform, die es schafft Synergien zu nutzen und alle relevanten Teilnehmer des Transportprozesses in einer Anwendung zu integrieren.

Durch einen hohen Grad an Prozessautomatisierung können die flexiblen Funktionalitäten exakt an die Nutzergruppen angepasst werden und die Effizienz in allen Prozessteilen optimiert werden.

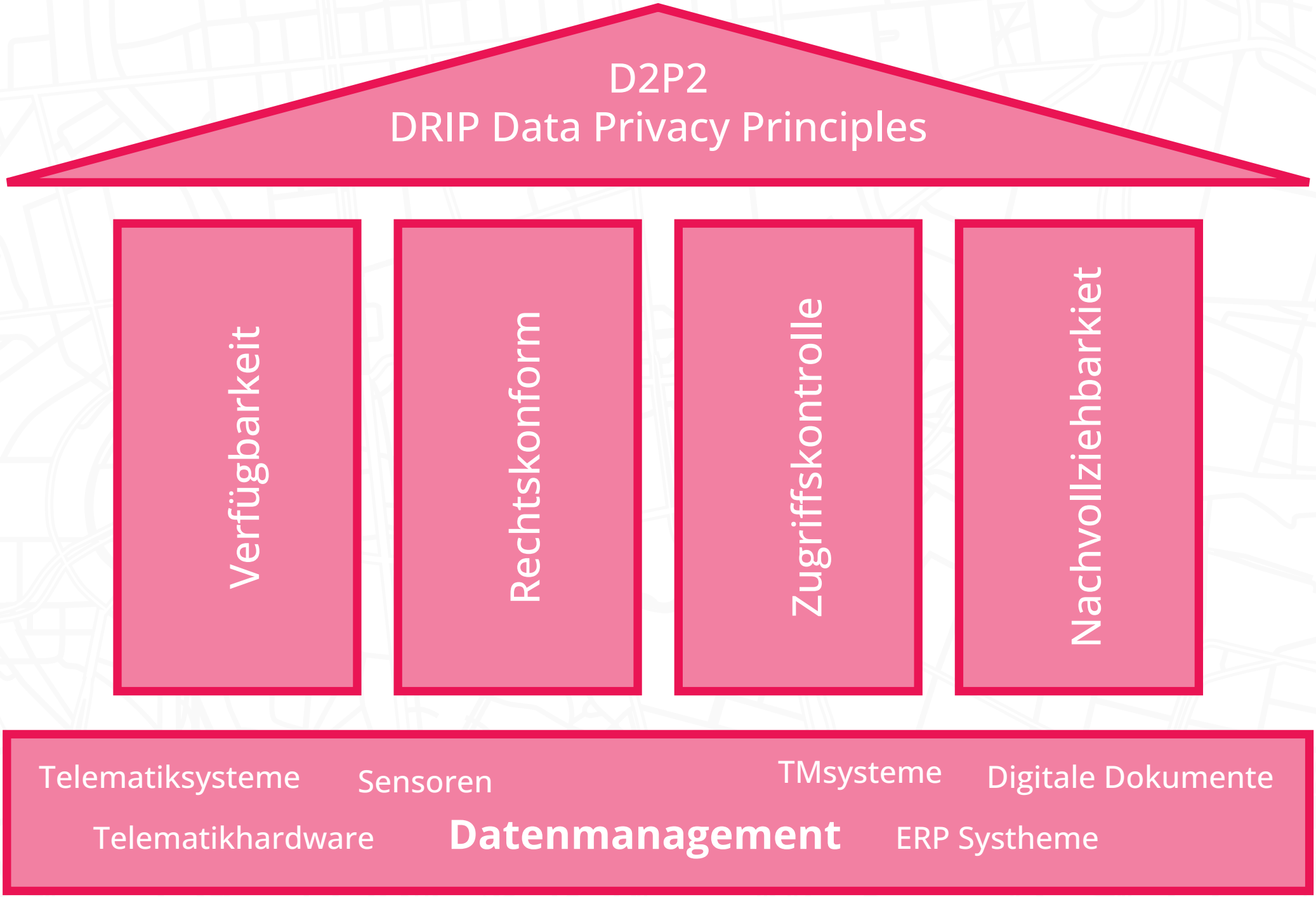
Das „easy to use“ Prinzip, dass sich wie ein roter Faden durch die gesamte Lösung zieht, ermöglicht eine zielgerichtete Steuerung und erhöht dadurch die Effektivität der Nutzer.

Besonders wesentlich sind auch noch die Punkte absolute Transparenz und Verlässlichkeit. Diese werden durch das intelligente Datenmanagement und das lernfähige System gesichert.

All diese Faktoren führen zu höchstmöglichem Vertrauen der Nutzer und enden in einem nachhaltigen Wertschöpfungsprozess im gesamten Transportnetzwerk.

DRIP

- Datensicherheit und Dateneigentum sind die obersten Prinzipien von DRIP
- Gerade in der Transportlogistik ist es wichtig Daten auszutauschen, um Prozesskosten zu optimieren. Um Datenmissbrauch zu vermeiden ist es wichtig, nur jene Daten auszutauschen, die für die Vertragserfüllung bzw. Auftragsabwicklung relevant sind.
- DRIP gibt allen Beteiligten in der Supply Chain die Möglichkeit, individuell Daten auszutauschen, ohne dabei die Kontrolle über ihre Daten zu verlieren.


D2P2
DRIP Data Privacy Principles
Verfügbarkeit
Rechtskonform
Zugriffskontrolle
Nachvollziehbarkiet
Telematiksysteme
Sensoren
TMsysteme
Digitale Dokumente
Telematikhardware
Datenmanagement
ERP Systheme

DRIP

Verfügbarkeit

Hoch Sicherheits Rechenzentrum
Sicheres Webprotokoll für die Kommunikation (SSL)
Sichere Benutzerzugriffskontrolle zusätzlich mit einer autenthischen APP
Datenspeicherung in der EU (Deutschland)

Beachtung

DRIP ist eine SAAS-Plattform (Software as a Service). Jedes Unternehmen verfügt über ein eigenes Konto, in dem die Daten gespeichert werden. DSGVO und Datenschutz sind das Hauptaugenmerk von DRIP. Die Plattform arbeitet nach dem "Need-to-know"-Prinzip. Nur Daten, die zur Erfüllung eines Vertrages benötigt werden, dürfen untereinander geteilt werden

Zugriffskontrolle

Die Weitergabe der Daten wird vom Absender kontrolliert. Der Absender könnte Daten manuell zwischen vertrauenswürdigen Partnern austauschen. Es handelt sich um ein 2-stufiges Sharing-System, um die höchste Datensicherheit zu gewährleisten.
Es gibt 2 Möglichkeiten, Daten zu teilen, automatische/halbautomatische auftragsbasierte Freigabe und die manuelle Fix-Charter-Freigabe mit vertrauenswürdigen Partnern.

Nachvollziehbarkeit

Der Eigentümer eines Assets hat die Möglichkeit zu sehen, wann und an wen die Daten weitergegeben wurden. Es ist auf beide Arten möglich. Die auftragsbasierte Freigabe und die manuelle Freigabe von Asset-Daten

Welche Daten können bzw. werden verarbeitet?

Geospezifische Daten

- Position (Lat/Lon)
- Geschwindigkeit
- Richtung
- ...

Daten der Telematikeinheit

- Zündung
- Heartbeat
- Sensordaten (Temperatur, Erschütterung, EBS)
- ...

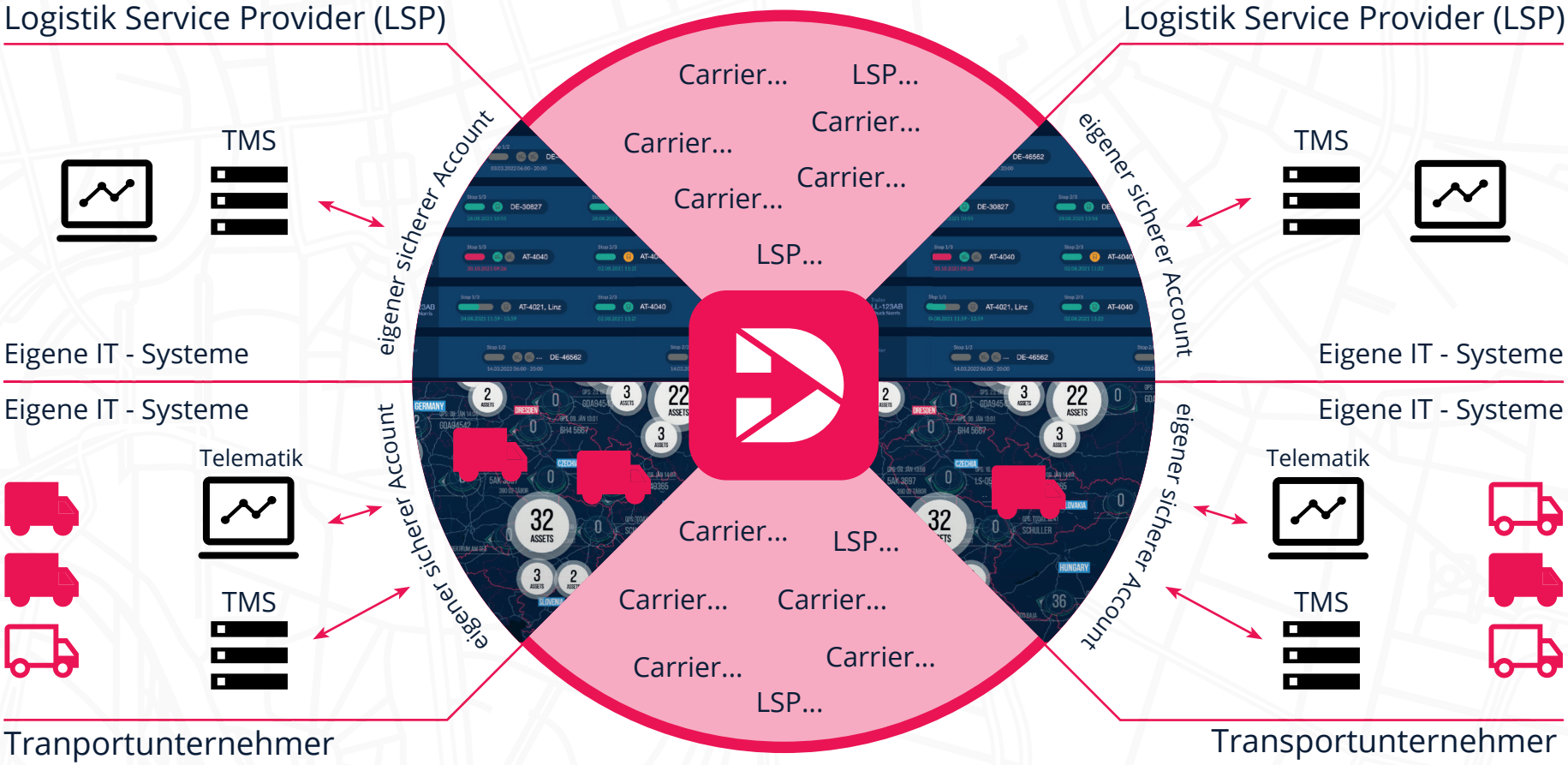
Fahrerdaten

- Name
- Fahrerkartennummer
- Geburtsdatum

Fahrzeugspezifische Daten

- Daten des FMS Buses
  - Motordaten, Servicedaten, VIN ....
  - Anhänger
- TACHO Graph
  - Fahrzeiten, Status, VIN , Kennzeichen
- Kühlaggregatsdaten
  - Temperatur
  - Setpoint
  - ...

MULTI MANDANTEN PLATTFORM

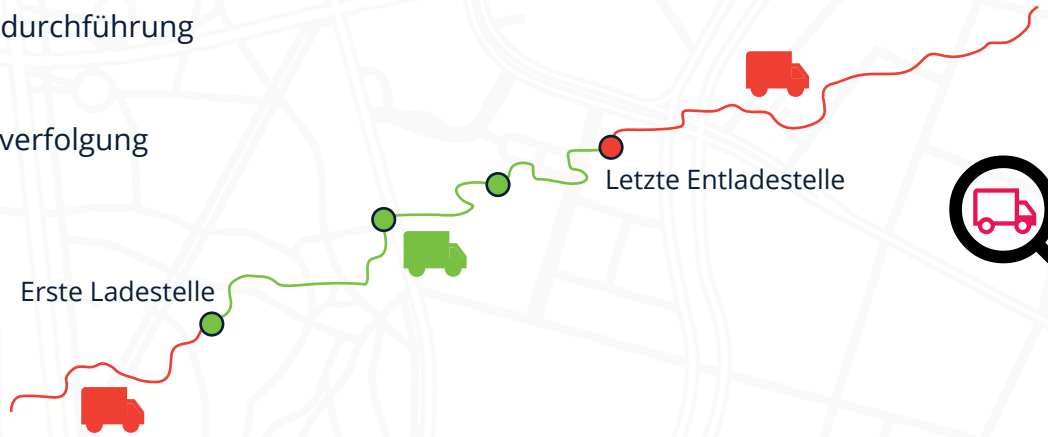


Datenaustausch muss genehmigt werden

AUFTRAGSBEZOGENE DATENVERARBEITUNG

Nur während der Auftragsdurchführung

1 Jahr zu rechtlichen Nachverfolgung



- Position
- Geschwindigkeit
- Kennzeichen
- Richtung
- Anhänger/Trailer
- Temperatur
- Setpoint

Daten* Sichtbarkeit Speicherdauer*

*kundenspezifisch anpassbar

MANUELLE FREIGABE

Für die Dauer in der die Freigabe besteht.

Achtung: Nur durch manuelle Freigabe eines Benutzers möglich!!!
Jeder Truck/Trailer kann einzeln geteilt werden

1 Jahr

- Position
- Geschwindigkeit
- Kennzeichen
- Richtung
- Anhänger/Trailer
- Temperatur
- Setpoint
- ...

Daten* Sichtbarkeit Speicherdauer*

*kundenspezifisch anpassbar

ANHANG 4: ALLGEMEINE AUFTRAGSBEDINGUNGEN FÜR WIRTSCHAFTSTREUHANDBERUFE (AAB 2018)

KAMMER DER STEUERBERATER UND WIRTSCHAFTSPRÜFER

Allgemeine Auftragsbedingungen für Wirtschaftstreuhandberufe (AAB 2018)

Empfohlen vom Vorstand der Kammer der Steuerberater und Wirtschaftsprüfer zuletzt mit Beschluss vom 18.04.2018

Präambel und Allgemeines

(1) Auftrag im Sinne dieser Bedingungen meint jeden Vertrag über vom zur Ausübung eines Wirtschaftstreuhandberufes Berechtigten in Ausübung dieses Berufes zu erbringende Leistungen (sowohl faktische Tätigkeiten als auch die Besorgung oder Durchführung von Rechtsgeschäften oder Rechtshandlungen, jeweils im Rahmen der §§ 2 oder 3 Wirtschaftstreuhandberufsgesetz 2017 (WTBG 2017). Die Parteien des Auftrages werden in Folge zum einen „Auftragnehmer", zum anderen „Auftraggeber" genannt).

(2) Diese Allgemeinen Auftragsbedingungen für Wirtschaftstreuhandberufe gliedern sich in zwei Teile: Die Auftragsbedingungen des I. Teiles gelten für Aufträge, bei denen die Auftragserteilung zum Betrieb des Unternehmens des Auftraggebers (Unternehmer iSd KSchG) gehört. Für Verbrauchergeschäfte gemäß Konsumentenschutzgesetz (Bundesgesetz vom 8.3.1979/BGBl Nr.140 in der derzeit gültigen Fassung) gelten sie insoweit der II. Teil keine abweichenden Bestimmungen für diese enthält.

(3) Im Falle der Unwirksamkeit einer einzelnen Bestimmung ist diese durch eine wirksame, die dem angestrebten Ziel möglichst nahe kommt, zu ersetzen.

I.TEIL

1. Umfang und Ausführung des Auftrages

(1) Der Umfang des Auftrages ergibt sich in der Regel aus der schriftlichen Auftragsvereinbarung zwischen Auftraggeber und Auftragnehmer. Fehlt diesbezüglich eine detaillierte schriftliche Auftragsvereinbarung gilt im Zweifel (2)-(4):

(2) Bei Beauftragung mit Steuerberatungsleistungen umfasst die Beratungstätigkeit folgende Tätigkeiten:
a) Ausarbeitung der Jahressteuererklärungen für die Einkommen- oder Körperschaftsteuer sowie Umsatzsteuer und zwar auf Grund der vom Auftraggeber vorzulegenden oder (bei entsprechender Vereinbarung) vom Auftragnehmer erstellten Jahresabschlüsse und sonstiger, für die Besteuerung erforderlichen Aufstellungen und Nachweise. Wenn nicht ausdrücklich anders vereinbart, sind die für die Besteuerung erforderlichen Aufstellungen und Nachweise vom Auftraggeber beizubringen.
b) Prüfung der Bescheide zu den unter a) genannten Erklärungen.
c) Verhandlungen mit den Finanzbehörden im Zusammenhang mit den unter a) und b) genannten Erklärungen und Bescheiden.
d) Mitwirkung bei Betriebsprüfungen und Auswertung der Ergebnisse von Betriebsprüfungen hinsichtlich der unter a) genannten Steuern.
e) Mitwirkung im Rechtsmittelverfahren hinsichtlich der unter a) genannten Steuern.
Erhält der Auftragnehmer für die laufende Steuerberatung ein Pauschalhonorar, so sind mangels anderweitiger schriftlicher Vereinbarungen die unter d) und e) genannten Tätigkeiten gesondert zu honorieren.

(3) Soweit die Ausarbeitung von einer oder mehreren Jahressteuererklärung(en) zum übernommenen Auftrag zählt, gehört dazu nicht die Überprüfung etwaiger besonderer buchmäßiger Voraussetzungen sowie die Prüfung, ob alle in Betracht kommenden insbesondere umsatzsteuerrechtlichen Begünstigungen wahrgenommen worden sind, es sei denn, hierüber besteht eine nachweisliche Beauftragung.

(4) Die Verpflichtung zur Erbringung anderer Leistungen gemäß §§ 2 und 3 WTBG 2017 bedarf jedenfalls nachweislich einer gesonderten Beauftragung.

(5) Vorstehende Absätze (2) bis (4) gelten nicht bei Sachverständigentätigkeit.

(6) Es bestehen keinerlei Pflichten des Auftragnehmers zur Leistungserbringung, Warnung oder Aufklärung über den Umfang des Auftrages hinaus.

(7) Der Auftragnehmer ist berechtigt, sich zur Durchführung des Auftrages geeigneter Mitarbeiter und sonstiger Erfüllungsgehilfen (Subunternehmer) zu bedienen, als auch sich bei der Durchführung des Auftrages durch einen Berufsbefugten substituieren zu lassen. Mitarbeiter im Sinne dieser Bedingungen meint alle Personen, die den Auftragnehmer auf regelmäßiger oder dauerhafter Basis bei seiner betrieblichen Tätigkeit unterstützen, unabhängig von der Art der rechtsgeschäftlichen Grundlage.

(8) Der Auftragnehmer hat bei der Erbringung seiner Leistungen ausschließlich österreichisches Recht zu berücksichtigen; ausländisches Recht ist nur bei ausdrücklicher schriftlicher Vereinbarung zu berücksichtigen.

(9) Ändert sich die Rechtslage nach Abgabe der abschließenden schriftlichen als auch mündlichen beruflichen Äußerung, so ist der Auftragnehmer nicht verpflichtet, den Auftraggeber auf Änderungen oder sich daraus ergebende Folgen hinzuweisen. Dies gilt auch für in sich abgeschlossene Teile eines Auftrages.

(10) Der Auftraggeber ist verpflichtet dafür Sorge zu tragen, dass die von ihm zur Verfügung gestellten Daten vom Auftragnehmer im Rahmen der Leistungserbringung verarbeitet werden dürfen. Diesbezüglich hat der Auftraggeber insbesondere aber nicht ausschließlich die anwendbaren datenschutz- und arbeitsrechtlichen Bestimmungen zu beachten.

(11) Bringt der Auftragnehmer bei einer Behörde ein Anbringen elektronisch ein, so handelt er – mangels ausdrücklicher gegenteiliger Vereinbarung – lediglich als Bote und stellt dies keine ihm oder einem einreichend Bevollmächtigten zurechenbare Willens- oder Wissenserklärung dar.

(12) Der Auftraggeber verpflichtet sich, Personen, die während des Auftragsverhältnisses Mitarbeiter des Auftragnehmers sind oder waren, während und binnen eines Jahres nach Beendigung des Auftragsverhältnisses nicht in seinem Unternehmen oder in einem ihm nahestehenden Unternehmen zu beschäftigen, widrigenfalls er sich zur Bezahlung eines Jahresbezuges des übernommenen Mitarbeiters an den Auftragnehmer verpflichtet.

2. Aufklärungspflicht des Auftraggebers; Vollständigkeitserklärung

(1) Der Auftraggeber hat dafür zu sorgen, dass dem Auftragnehmer auch ohne dessen besondere Aufforderung alle für die Ausführung des Auftrages notwendigen Unterlagen zum vereinbarten Termin und in Ermangelung eines solchen rechtzeitig in geeigneter Form vorgelegt werden und ihm von allen Vorgängen und Umständen Kenntnis gegeben wird, die für die Ausführung des Auftrages von Bedeutung sein können. Dies gilt auch für die Unterlagen, Vorgänge und Umstände, die erst während der Tätigkeit des Auftragnehmers bekannt werden.

(2) Der Auftragnehmer ist berechtigt, die ihm erteilten Auskünfte und übergebenen Unterlagen des Auftraggebers, insbesondere Zahlenangaben, als richtig und vollständig anzusehen und dem Auftrag zu Grunde zu legen. Der Auftragnehmer ist ohne gesonderten schriftlichen Auftrag nicht verpflichtet, Unrichtigkeiten fest zu stellen. Insbesondere gilt dies auch für die Richtigkeit und Vollständigkeit von Rechnungen. Stellt er allerdings Unrichtigkeiten fest, so hat er dies dem Auftraggeber bekannt zu geben. Er hat im Finanzstrafverfahren die Rechte des Auftraggebers zu wahren.

(3) Der Auftraggeber hat dem Auftragnehmer die Vollständigkeit der vorgelegten Unterlagen sowie der gegebenen Auskünfte und Erklärungen im Falle von Prüfungen, Gutachten und Sachverständigentätigkeit schriftlich zu bestätigen.

(4) Wenn bei der Erstellung von Jahresabschlüssen und anderen Abschlüssen vom Auftraggeber erhebliche Risiken nicht bekannt gegeben worden sind, bestehen für den Auftragnehmer insoweit diese Risiken schlagend werden keinerlei Ersatzpflichten.

(5) Vom Auftragnehmer angegebene Termine und Zeitpläne für die Fertigstellung von Produkten des Auftragnehmers oder Teilen davon sind bestmögliche Schätzungen und, sofern nicht anders schriftlich vereinbart, nicht bindend. Selbiges gilt für etwaige Honorarschätzungen: diese werden nach bestem Wissen erstellt; sie sind jedoch stets unverbindlich.

(6) Der Auftraggeber hat dem Auftragnehmer jeweils aktuelle Kontaktdaten (insbesondere Zustelladresse) bekannt zu geben. Der Auftragnehmer darf sich bis zur Bekanntgabe neuer Kontaktdaten auf die Gültigkeit der zuletzt vom Auftraggeber bekannt gegebenen Kontaktdaten verlassen, insbesondere Zustellung an die zuletzt bekannt gegebene Adresse vornehmen lassen.

3. Sicherung der Unabhängigkeit

(1) Der Auftraggeber ist verpflichtet, alle Vorkehrungen zu treffen, um zu verhindern, dass die Unabhängigkeit der Mitarbeiter des Auftragnehmers gefährdet wird, und hat selbst jede Gefährdung dieser Unabhängigkeit zu unterlassen. Dies gilt insbesondere für Angebote auf Anstellung und für Angebote, Aufträge auf eigene Rechnung zu übernehmen.

(2) Der Auftraggeber nimmt zur Kenntnis, dass seine hierfür notwendigen personenbezogenen Daten sowie Art und Umfang inklusive Leistungszeitraum der zwischen Auftragnehmer und Auftraggeber vereinbarten Leistungen (sowohl Prüfungs- als auch Nichtprüfungsleistungen) zum Zweck der Überprüfung des Vorliegens von Befangenheits- oder Ausschließungsgründen und Interessenkollisionen in einem allfälligen Netzwerk, dem der Auftragnehmer angehört, verarbeitet und zu diesem Zweck an die übrigen Mitglieder dieses Netzwerkes auch ins Ausland übermittelt werden. Hierfür entbindet der Auftraggeber den Auftragnehmer nach dem Datenschutzgesetz und gemäß § 80 Abs 4 Z 2 WTBG 2017 ausdrücklich von dessen Verschwiegenheitspflicht. Der Auftraggeber kann die Entbindung von der Verschwiegenheitspflicht jederzeit widerrufen.

4. Berichterstattung und Kommunikation

(1) (Berichterstattung durch den Auftragnehmer) Bei Prüfungen und Gutachten ist, soweit nichts anderes vereinbart wurde, ein schriftlicher Bericht zu erstatten.

(2) (Kommunikation an den Auftraggeber) Alle auftragsbezogenen Auskünfte und Stellungnahmen, einschließlich Berichte, (allesamt Wissenserklärungen) des Auftragnehmers, seiner Mitarbeiter, sonstiger Erfüllungsgehilfen oder Substitute („berufliche Äußerungen“) sind nur dann verbindlich, wenn sie schriftlich erfolgen. Berufliche Äußerungen in elektronischen Dateiformaten, welche per Fax oder E-Mail oder unter Verwendung ähnlicher Formen der elektronischen Kommunikation (speicher- und wiedergabefähig und nicht mündlich dh zB SMS aber nicht Telefon) erfolgen, übermittelt oder bestätigt werden, gelten als schriftlich; dies gilt ausschließlich für berufliche Äußerungen. Das Risiko der Erteilung der beruflichen Äußerungen durch dazu Nichtbefugte und das Risiko der Übersendung dieser trägt der Auftraggeber.

(3) (Kommunikation an den Auftraggeber) Der Auftraggeber stimmt hiermit zu, dass der Auftragnehmer elektronische Kommunikation mit dem Auftraggeber (zB via E-Mail) in unverschlüsselter Form vornimmt. Der Auftraggeber erklärt, über die mit der Verwendung elektronischer Kommunikation verbundenen Risiken (insbesondere Zugang, Geheimhaltung, Veränderung von Nachrichten im Zuge der Übermittlung) informiert zu sein. Der Auftragnehmer, seine Mitarbeiter, sonstigen Erfüllungsgehilfen oder Substitute haften nicht für Schäden, die durch die Verwendung elektronischer Kommunikationsmittel verursacht werden.

(4) (Kommunikation an den Auftragnehmer) Der Empfang und die Weiterleitung von Informationen an den Auftragnehmer und seine Mitarbeiter sind bei Verwendung von Telefon – insbesondere in Verbindung mit automatischen Anrufbeantwortungssystemen, Fax, E-Mail und anderen Formen der elektronischen Kommunikation – nicht immer sichergestellt. Aufträge und wichtige Informationen gelten daher dem Auftragnehmer nur dann als zugegangen, wenn sie auch physisch (nicht (fern-)mündlich oder elektronisch) zugegangen sind, es sei denn, es wird im Einzelfall der Empfang ausdrücklich bestätigt. Automatische Übermittlungs- und Lesebestätigungen gelten nicht als solche ausdrücklichen Empfangsbestätigungen. Dies gilt insbesondere für die Übermittlung von Bescheiden und anderen Informationen über Fristen. Kritische und wichtige Mitteilungen müssen daher per Post oder Kurier an den Auftragnehmer gesandt werden. Die Übergabe von Schriftstücken an Mitarbeiter außerhalb der Kanzlei gilt nicht als Übergabe.

(5) (Allgemein) Schriftlich meint insoweit in Punkt 4 (2) nicht anderes bestimmt, Schriftlichkeit iSd § 886 ABGB (Unterschriftlichkeit). Eine fortgeschrittene elektronische Signatur (Art. 26 eIDAS-VO, (EU) Nr. 910/2014) erfüllt das Erfordernis der Schriftlichkeit iSd § 886 ABGB (Unterschriftlichkeit), soweit dies innerhalb der Parteiendisposition liegt.

(6) (Werbliche Information) Der Auftragnehmer wird dem Auftraggeber wiederkehrend allgemeine steuerrechtliche und allgemeine wirtschaftsrechtliche Informationen elektronisch (zB per E-Mail) übermitteln. Der Auftraggeber nimmt zur Kenntnis, dass er das Recht hat, der Zusendung von Direktwerbung jederzeit zu widersprechen.

5. Schutz des geistigen Eigentums des Auftragnehmers

(1) Der Auftraggeber ist verpflichtet, dafür zu sorgen, dass die im Rahmen des Auftrages vom Auftragnehmer erstellten Berichte, Gutachten, Organisationspläne, Entwürfe, Zeichnungen, Berechnungen und dergleichen nur für Auftragszwecke (z.B. gemäß § 44 Abs 3 EStG 1988) verwendet werden. Im Übrigen bedarf die Weitergabe schriftlicher als auch mündlicher beruflicher Äußerungen des Auftragnehmers an einen Dritten zur Nutzung der schriftlichen Zustimmung des Auftragnehmers.
(2) Die Verwendung schriftlicher als auch mündlicher beruflicher Äußerungen des Auftragnehmers zu Werbezwecken ist unzulässig; ein Verstoß berechtigt den Auftragnehmer zur fristlosen Kündigung aller noch nicht durchgeführten Aufträge des Auftraggebers.

(3) Dem Auftragnehmer verbleibt an seinen Leistungen das Urheberrecht. Die Einräumung von Werknutzungsbewilligungen bleibt der schriftlichen Zustimmung des Auftragnehmers vorbehalten.

6. Mängelbeseitigung

(1) Der Auftragnehmer ist berechtigt und verpflichtet, nachträglich hervorkommende Unrichtigkeiten und Mängel in seiner schriftlichen als auch mündlichen beruflichen Äußerung zu beseitigen, und verpflichtet, den Auftraggeber hiervon unverzüglich zu verständigen. Er ist berechtigt, auch über die ursprüngliche berufliche Äußerung informierte Dritte von der Änderung zu verständigen.

(2) Der Auftraggeber hat Anspruch auf die kostenlose Beseitigung von Unrichtigkeiten, sofern diese durch den Auftragnehmer zu vertreten sind; dieser Anspruch erlischt sechs Monate nach erbrachter Leistung des Auftragnehmers bzw. – falls eine schriftliche berufliche Äußerung nicht abgegeben wird – sechs Monate nach Beendigung der beanstandeten Tätigkeit des Auftragnehmers.

(3) Der Auftraggeber hat bei Fehlschlägen der Nachbesserung etwaiger Mängel Anspruch auf Minderung. Soweit darüber hinaus Schadenersatzansprüche bestehen, gilt Punkt 7.

7. Haftung

(1) Sämtliche Haftungsregelungen gelten für alle Streitigkeiten im Zusammenhang mit dem Auftragsverhältnis, gleich aus welchem Rechtsgrund. Der Auftragnehmer haftet für Schäden im Zusammenhang mit dem Auftragsverhältnis (einschließlich dessen Beendigung) nur bei Vorsatz und grober Fahrlässigkeit. Die Anwendbarkeit des § 1298 Satz 2 ABGB wird ausgeschlossen.

(2) Im Falle grober Fahrlässigkeit beträgt die Ersatzpflicht des Auftragnehmers höchstens das zehnfache der Mindestversicherungssumme der Berufshaftpflichtversicherung gemäß § 11 Wirtschaftstreuhandberufsgesetz 2017 (WTBG 2017) in der jeweils geltenden Fassung.

(3) Die Beschränkung der Haftung gemäß Punkt 7 (2) bezieht sich auf den einzelnen Schadensfall. Der einzelne Schadensfall umfasst sämtliche Folgen einer Pflichtverletzung ohne Rücksicht darauf, ob Schäden in einem oder in mehreren aufeinander folgenden Jahren entstanden sind. Dabei gilt mehrfaches auf gleicher oder gleichartiger Fehlerquelle beruhendes Tun oder Unterlassen als eine einheitliche Pflichtverletzung, wenn die betreffenden Angelegenheiten miteinander in rechtlichem und wirtschaftlichem Zusammenhang stehen. Ein einheitlicher Schaden bleibt ein einzelner Schadensfall, auch wenn er auf mehreren Pflichtverletzungen beruht. Weiters ist, außer bei vorsätzlicher Schädigung, eine Haftung des Auftragnehmers für entgangenen Gewinn sowie Begleit-, Folge-, Neben- oder ähnliche Schäden, ausgeschlossen.

(4) Jeder Schadenersatzanspruch kann nur innerhalb von sechs Monaten nachdem der oder die Anspruchsberechtigten von dem Schaden Kenntnis erlangt haben, spätestens aber innerhalb von drei Jahren ab Eintritt des (Primär)Schadens nach dem anspruchsbegründenden Ereignis gerichtlich geltend gemacht werden, sofern nicht in gesetzlichen Vorschriften zwingend andere Verjährungsfristen festgesetzt sind.

(5) Im Falle der (tatbestandsmäßigen) Anwendbarkeit des § 275 UGB gelten dessen Haftungsnormen auch dann, wenn an der Durchführung des Auftrages mehrere Personen beteiligt gewesen oder mehrere zum Ersatz verpflichtende Handlungen begangen worden sind und ohne Rücksicht darauf, ob andere Beteiligte vorsätzlich gehandelt haben.

(6) In Fällen, in denen ein förmlicher Bestätigungsvermerk erteilt wird, beginnt die Verjährungsfrist spätestens mit Erteilung des Bestätigungsvermerkes zu laufen.

(7) Wird die Tätigkeit unter Einschaltung eines Dritten, z.B. eines Daten verarbeitenden Unternehmens, durchgeführt, so gelten mit Benachrichtigung des Auftraggebers darüber nach Gesetz oder Vertrag be- oder entstehende Gewährleistungs- und Schadenersatzansprüche gegen den Dritten als an den Auftraggeber abgetreten. Der Auftragnehmer haftet, unbeschadet Punkt 4. (3), diesfalls nur für Verschulden bei der Auswahl des Dritten.

(8) Eine Haftung des Auftragnehmers Dritten gegenüber ist in jedem Fall ausgeschlossen. Geraten Dritte mit der Arbeit des Auftragnehmers wegen des Auftraggebers in welcher Form auch immer in Kontakt hat der Auftraggeber diese über diesen Umstand ausdrücklich aufzuklären. Soweit

ein solcher Haftungsausschluss gesetzlich nicht zulässig ist oder eine Haftung gegenüber Dritten vom Auftragnehmer ausnahmsweise übernommen wurde, gelten subsidiär diese Haftungsbeschränkungen jedenfalls auch gegenüber Dritten. Dritte können jedenfalls keine Ansprüche stellen, die über einen allfälligen Anspruch des Auftraggebers hinausgehen. Die Haftungshöchstsumme gilt nur insgesamt einmal für alle Geschädigten, einschließlich der Ersatzansprüche des Auftraggebers selbst, auch wenn mehrere Personen (der Auftraggeber und ein Dritter oder auch mehrere Dritte) geschädigt worden sind; Geschädigte werden nach ihrem Zuvorkommen befriedigt. Der Auftraggeber wird den Auftragnehmer und dessen Mitarbeiter von sämtlichen Ansprüchen Dritter im Zusammenhang mit der Weitergabe schriftlicher als auch mündlicher beruflicher Äußerungen des Auftragnehmers an diese Dritte schad- und klaglos halten.

(9) Punkt 7 gilt auch für allfällige Haftungsansprüche des Auftraggebers im Zusammenhang mit dem Auftragsverhältnis gegenüber Dritten (Erfüllungs- und Besorgungsgehilfen des Auftragnehmers) und den Substituten des Auftragnehmers.

8. Verschwiegenheitspflicht, Datenschutz

(1) Der Auftragnehmer ist gemäß § 80 WTBG 2017 verpflichtet, über alle Angelegenheiten, die ihm im Zusammenhang mit seiner Tätigkeit für den Auftraggeber bekannt werden, Stillschweigen zu bewahren, es sei denn, dass der Auftraggeber ihn von dieser Schweigepflicht entbindet oder gesetzliche Äußerungspflichten entgegen stehen.

(2) Soweit es zur Verfolgung von Ansprüchen des Auftragnehmers (insbesondere Ansprüche auf Honorar) oder zur Abwehr von Ansprüchen gegen den Auftragnehmer (insbesondere Schadenersatzansprüche des Auftraggebers oder Dritter gegen den Auftragnehmer) notwendig ist, ist der Auftragnehmer von seiner beruflichen Verschwiegenheitspflicht entbunden.

(3) Der Auftragnehmer darf Berichte, Gutachten und sonstige schriftliche berufliche Äußerungen über die Ergebnisse seiner Tätigkeit Dritten nur mit Einwilligung des Auftraggebers aushändigen, es sei denn, dass eine gesetzliche Verpflichtung hierzu besteht.

(4) Der Auftragnehmer ist datenschutzrechtlich Verantwortlicher im Sinne der Datenschutz-Grundverordnung („DSGVO“) hinsichtlich aller im Rahmen des Auftrages verarbeiteter personenbezogenen Daten. Der Auftragnehmer ist daher befugt, ihm anvertraute personenbezogene Daten im Rahmen der Grenzen des Auftrages zu verarbeiten. Dem Auftragnehmer überlassene Materialien (Papier und Datenträger) werden grundsätzlich nach Beendigung der diesbezüglichen Leistungserbringung dem Auftraggeber oder an vom Auftraggeber namhaft gemachte Dritte übergeben oder wenn dies gesondert vereinbart ist vom Auftragnehmer verwahrt oder vernichtet. Der Auftragnehmer ist berechtigt Kopien davon aufzubewahren soweit er diese zur ordnungsgemäßen Dokumentation seiner Leistungen benötigt oder es rechtlich geboten oder berufsüblich ist.

(5) Sofern der Auftragnehmer den Auftraggeber dabei unterstützt, die den Auftraggeber als datenschutzrechtlich Verantwortlichen treffenden Pflichten gegenüber Betroffenen zu erfüllen, so ist der Auftragnehmer berechtigt, den entstandenen tatsächlichen Aufwand an den Auftraggeber zu verrechnen. Gleiches gilt, für den Aufwand der für Auskünfte im Zusammenhang mit dem Auftragsverhältnis anfällt, die nach Entbindung von der Verschwiegenheitspflicht durch den Auftraggeber gegenüber Dritten diesen Dritten erteilt werden.

9. Rücktritt und Kündigung („Beendigung“)

(1) Die Erklärung der Beendigung eines Auftrags hat schriftlich zu erfolgen (siehe auch Punkt. 4 (4) und (5)). Das Erlöschen einer bestehenden Vollmacht bewirkt keine Beendigung des Auftrags.

(2) Soweit nicht etwas anderes schriftlich vereinbart oder gesetzlich zwingend vorgeschrieben ist, können die Vertragspartner den Vertrag jederzeit mit sofortiger Wirkung beendigen. Der Honoraranspruch bestimmt sich nach Punkt 11.

(3) Ein Dauerauftrag (befristeter oder unbefristeter Auftrag über, wenn auch nicht ausschließlich, die Erbringung wiederholter Einzelleistungen, auch mit Pauschalvergütung) kann allerdings, soweit nichts anderes schriftlich vereinbart ist, ohne Vorliegen eines wichtigen Grundes nur unter Einhaltung einer Frist von drei Monaten („Beendigungsfrist“) zum Ende eines Kalendermonats beendet werden.

(4) Nach Erklärung der Beendigung eines Dauerauftrags – sind, soweit im Folgenden nicht abweichend bestimmt, nur jene einzelnen Werke vom Auftragnehmer noch fertigzustellen (verbleibender Auftragsstand), deren vollständige Ausführung innerhalb der Beendigungsfrist (grundsätzlich) möglich ist, soweit diese innerhalb eines Monats nach Beginn des Laufs der Beendigungsfrist dem Auftraggeber schriftlich im Sinne des Punktes 4 (2) bekannt gegeben werden. Der verbleibende Auftragsstand ist innerhalb der Beendigungsfrist fertig zu stellen, sofern sämtliche erforderlichen Unterlagen rechtzeitig zur Verfügung gestellt werden und soweit nicht ein wichtiger Grund vorliegt, der dies hindert.

(5) Wären bei einem Dauerauftrag mehr als 2 gleichartige, üblicherweise nur einmal jährlich zu erstellende Werke (z.B. Jahresabschlüsse, Steuererklärungen etc.) fertig zu stellen, so zählen die über 2 hinaus gehenden Werke nur bei ausdrücklichem Einverständnis des Auftraggebers zum verbleibenden Auftragsstand. Auf diesen Umstand ist der Auftraggeber in der Bekanntgabe gemäß Punkt 9 (4) gegebenenfalls ausdrücklich hinzuweisen.

10. Beendigung bei Annahmeverzug und unterlassener Mitwirkung des Auftraggebers und rechtlichen Ausführungshindernissen

(1) Kommt der Auftraggeber mit der Annahme der vom Auftragnehmer angebotenen Leistung in Verzug oder unterlässt der Auftraggeber eine ihm nach Punkt 2. oder sonst wie obliegende Mitwirkung, so ist der Auftragnehmer zur fristlosen Beendigung des Vertrages berechtigt. Gleiches gilt, wenn der Auftraggeber eine (auch teilweise) Durchführung des Auftrages verlangt, die, nach begründetem Dafürhalten des Auftragnehmers, nicht der Rechtslage oder berufsüblichen Grundsätzen entspricht. Seine Honoraransprüche bestimmen sich nach Punkt 11. Annahmeverzug sowie unterlassene Mitwirkung seitens des Auftraggebers begründen auch dann den Anspruch des Auftragnehmers auf Ersatz der ihm hierdurch entstandenen Mehraufwendungen sowie des verursachten Schadens, wenn der Auftragnehmer von seinem Kündigungsrecht keinen Gebrauch macht.

(2) Bei Verträgen über die Führung der Bücher, die Vornahme der Personalsachbearbeitung oder Abgabenverrechnung ist eine fristlose Beendigung durch den Auftragnehmer gemäß Punkt 10 (1) zulässig, wenn der Auftraggeber seiner Mitwirkungspflicht gemäß Punkt 2. (1) zweimal nachweislich nicht nachkommt.

11. Honoraranspruch

(1) Unterbleibt die Ausführung des Auftrages (z.B. wegen Rücktritt oder Kündigung), so gebührt dem Auftragnehmer gleichwohl das vereinbarte Entgelt (Honorar), wenn er zur Leistung bereit war und durch Umstände, deren Ursache auf Seiten des Auftraggebers liegen, ein bloßes Mitverschulden des Auftragnehmers bleibt diesbezüglich außer Ansatz, daran gehindert worden ist; der Auftragnehmer braucht sich in diesem Fall nicht anrechnen zu lassen, was er durch anderweitige Verwendung seiner und seiner Mitarbeiter Arbeitskraft erwirbt oder zu erwerben unterlässt.

(2) Bei Beendigung eines Dauerauftrags gebührt das vereinbarte Entgelt für den verbleibenden Auftragsstand, sofern er fertiggestellt wird oder dies aus Gründen, die dem Auftraggeber zuzurechnen sind, unterbleibt (auf Punkt 11. (1) wird verwiesen). Vereinbarte Pauschalhonorare sind gegebenenfalls zu aliquotieren.

(3) Unterbleibt eine zur Ausführung des Werkes erforderliche Mitwirkung des Auftraggebers, so ist der Auftragnehmer auch berechtigt, ihm zur Nachholung eine angemessene Frist zu setzen mit der Erklärung, dass nach fruchtlosem Verstreichen der Frist der Vertrag als aufgehoben gelte, im Übrigen gelten die Folgen des Punkt 11. (1).

(4) Bei Nichteinhaltung der Beendigungsfrist gemäß Punkt 9. (3) durch den Auftraggeber, sowie bei Vertragsauflösung gemäß Punkt 10. (2) durch den Auftragnehmer behält der Auftragnehmer den vollen Honoraranspruch für drei Monate.

12. Honorar

(1) Sofern nicht ausdrücklich Unentgeltlichkeit vereinbart ist, wird jedenfalls gemäß § 1004 und § 1152 ABGB eine angemessene Entlohnung geschuldet. Höhe und Art des Honoraranspruchs des Auftragnehmers ergeben sich aus der zwischen ihm und seinem Auftraggeber getroffenen Vereinbarung. Sofern nicht nachweislich eine andere Vereinbarung getroffen wurde sind Zahlungen des Auftraggebers immer auf die älteste Schuld anzurechnen.

(2) Die kleinste verrechenbare Leistungseinheit beträgt eine Viertelstunde.

(3) Auch die Wegzeit wird im notwendigen Umfang verrechnet.

(4) Das Aktenstudium in der eigenen Kanzlei, das nach Art und Umfang zur Vorbereitung des Auftragnehmers notwendig ist, kann gesondert verrechnet werden.

(5) Erweist sich durch nachträglich hervorgekommene besondere Umstände oder auf Grund besonderer Inanspruchnahme durch den Auftraggeber ein bereits vereinbartes Entgelt als unzureichend, so hat der Auftragnehmer den Auftraggeber darauf hinzuweisen und sind Nachverhandlungen zur Vereinbarung eines angemessenen Entgelts zu führen (auch bei unzureichenden Pauschalhonoraren).

(6) Der Auftragnehmer verrechnet die Nebenkosten und die Umsatzsteuer zusätzlich. Beispielhaft aber nicht abschließend im Folgenden (7) bis (9):

(7) Zu den verrechenbaren Nebenkosten zählen auch belegte oder pauschalierte Barauslagen, Reisespesen (bei Bahnfahrten 1. Klasse), Diäten, Kilometergeld, Kopierkosten und ähnliche Nebenkosten.

(8) Bei besonderen Haftpflichtversicherungserfordernissen zählen die betreffenden Versicherungsprämien (inkl. Versicherungssteuer) zu den Nebenkosten.

(9) Weiters sind als Nebenkosten auch Personal- und Sachaufwendungen für die Erstellung von Berichten, Gutachten uä. anzusehen.

(10) Für die Ausführung eines Auftrages, dessen gemeinschaftliche Erledigung mehreren Auftragnehmern übertragen worden ist, wird von jedem das seiner Tätigkeit entsprechende Entgelt verrechnet.

(11) Entgelte und Entgeltvorschüsse sind mangels anderer Vereinbarungen sofort nach deren schriftlicher Geltendmachung fällig. Für Entgeltzahlungen, die später als 14 Tage nach Fälligkeit geleistet werden, können Verzugszinsen verrechnet werden. Bei beiderseitigen Unternehmergeschäften gelten Verzugszinsen in der in § 456 1. und 2. Satz UGB festgelegten Höhe.

(12) Die Verjährung richtet sich nach § 1486 ABGB und beginnt mit Ende der Leistung bzw. mit späterer, in angemessener Frist erfolgter Rechnungslegung zu laufen.

(13) Gegen Rechnungen kann innerhalb von 4 Wochen ab Rechnungsdatum schriftlich beim Auftragnehmer Einspruch erhoben werden. Andernfalls gilt die Rechnung als anerkannt. Die Aufnahme einer Rechnung in die Bücher gilt jedenfalls als Anerkenntnis.

(14) Auf die Anwendung des § 934 ABGB im Sinne des § 351 UGB, das ist die Anfechtung wegen Verkürzung über die Hälfte für Geschäfte unter Unternehmern, wird verzichtet.

(15) Falls bei Aufträgen betreffend die Führung der Bücher, die Vornahme der Personalsachbearbeitung oder Abgabenverrechnung ein Pauschalhonorar vereinbart ist, so sind mangels anderweitiger schriftlicher Vereinbarung die Vertretungstätigkeit im Zusammenhang mit abgaben- und beitragsrechtlichen Prüfungen aller Art einschließlich der Abschluss von Vergleichen über Abgabenbemessungs- oder Beitragsgrundlagen, Berichterstattung, Rechtsmittelerhebung uä gesondert zu honorieren. Sofern nichts anderes schriftlich vereinbart ist, gilt das Honorar als jeweils für ein Auftragsjahr vereinbart.

(16) Die Bearbeitung besonderer Einzelfragen im Zusammenhang mit den im Punkt 12. (15) genannten Tätigkeiten, insbesondere Feststellungen über das prinzipielle Vorliegen einer Pflichtversicherung, erfolgt nur aufgrund eines besonderen Auftrages.

(17) Der Auftragnehmer kann entsprechende Vorschüsse verlangen und seine (fortgesetzte) Tätigkeit von der Zahlung dieser Vorschüsse abhängig machen. Bei Daueraufträgen darf die Erbringung weiterer Leistungen bis zur Bezahlung früherer Leistungen (sowie allfälliger Vorschüsse gemäß Satz 1) verweigert werden. Bei Erbringung von Teilleistungen und offener Teilhonorierung gilt dies sinngemäß.

(18) Eine Beanstandung der Arbeiten des Auftragnehmers berechtigt, außer bei offenkundigen wesentlichen Mängeln, nicht zur auch nur teilweisen Zurückhaltung der ihm nach Punkt 12. zustehenden Honorare, sonstigen Entgelte, Kostenersätze und Vorschüsse (Vergütungen).

(19) Eine Aufrechnung gegen Forderungen des Auftragnehmers auf Vergütungen nach Punkt 12. ist nur mit unbestrittenen oder rechtskräftig festgestellten Forderungen zulässig.

13. Sonstiges

(1) Im Zusammenhang mit Punkt 12. (17) wird auf das gesetzliche Zurückbehaltungsrecht (§ 471 ABGB, § 369 UGB) verwiesen; wird das Zurückbehaltungsrecht zu Unrecht ausgeübt, haftet der Auftragnehmer grundsätzlich gemäß Punkt 7. aber in Abweichung dazu nur bis zur Höhe seiner noch offenen Forderung.

(2) Der Auftraggeber hat keinen Anspruch auf Ausfolgung von im Zuge der Auftragserfüllung vom Auftragnehmer erstellten Arbeitspapieren und ähnlichen Unterlagen. Im Falle der Auftragserfüllung unter Einsatz elektronischer Buchhaltungssysteme ist der Auftragnehmer berechtigt, nach Übergabe sämtlicher vom Auftragnehmer auftragsbezogen damit erstellter Daten, für die den Auftraggeber eine Aufbewahrungspflicht trifft, in einem strukturierten, gängigen und maschinenlesbaren Format an den Auftraggeber bzw. an den nachfolgenden Wirtschaftstreuhänder, die Daten zu löschen. Für die Übergabe dieser Daten in einem strukturierten, gängigen und maschinenlesbaren Format hat der Auftragnehmer Anspruch auf ein angemessenes Honorar (Punkt 12 gilt sinngemäß). Ist eine Übergabe dieser Daten in einem strukturierten, gängigen und maschinenlesbaren Format aus besonderen Gründen unmöglich oder untunlich, können diese ersatzweise im Vollausdruck übergeben werden. Eine Honorierung steht diesfalls dafür nicht zu.

(3) Der Auftragnehmer hat auf Verlangen und Kosten des Auftraggebers alle Unterlagen herauszugeben, die er aus Anlass seiner Tätigkeit von diesem erhalten hat. Dies gilt jedoch nicht für den Schriftwechsel zwischen dem Auftragnehmer und seinem Auftraggeber und für die Schriftstücke, die der Auftraggeber in Urschrift besitzt und für Schriftstücke, die einer Aufbewahrungspflicht nach den für den Auftragnehmer geltenden rechtlichen Bestimmungen zur Verhinderung von Geldwäsche unterliegen. Der Auftragnehmer kann von Unterlagen, die er an den Auftraggeber zurückgibt, Abschriften oder Fotokopien anfertigen. Sind diese Unterlagen bereits einmal an den Auftraggeber übermittelt worden so hat der Auftragnehmer Anspruch auf ein angemessenes Honorar (Punkt 12. gilt sinngemäß).

(4) Der Auftraggeber hat die dem Auftragsnehmer übergebenen Unterlagen nach Abschluss der Arbeiten binnen 3 Monaten abzuholen. Bei Nichtabholung übergebener Unterlagen kann der Auftragnehmer nach zweimaliger nachweislicher Aufforderung an den Auftraggeber, übergebene Unterlagen abzuholen, diese auf dessen Kosten zurückstellen und/oder ein angemessenes Honorar in Rechnung stellen (Punkt 12. gilt sinngemäß). Die weitere Aufbewahrung kann auch auf Kosten des Auftraggebers durch Dritte erfolgen. Der Auftragnehmer haftet im Weiteren nicht für Folgen aus Beschädigung, Verlust oder Vernichtung der Unterlagen.

(5) Der Auftragnehmer ist berechtigt, fällige Honorarforderungen mit etwaigen Depotguthaben, Verrechnungsgeldern, Treuhandgeldern oder anderen in seiner Gewahrsame befindlichen liquiden Mitteln auch bei ausdrücklicher Inverwahrungnahme zu kompensieren, sofern der Auftraggeber mit einem Gegenanspruch des Auftragnehmers rechnen musste.

(6) Zur Sicherung einer bestehenden oder künftigen Honorarforderung ist der Auftragnehmer berechtigt, ein finanzamtliches Guthaben oder ein anderes Abgaben- oder Beitragsguthaben des Auftraggebers auf ein Anderkonto zu transferieren. Diesfalls ist der Auftraggeber vom erfolgten Transfer zu verständigen. Danach kann der sichergestellte Betrag entweder im Einvernehmen mit dem Auftraggeber oder bei Vollstreckbarkeit der Honorarforderung eingezogen werden.

14. Anzuwendendes Recht, Erfüllungsort, Gerichtsstand

(1) Für den Auftrag, seine Durchführung und die sich hieraus ergebenden Ansprüche gilt ausschließlich österreichisches Recht unter Ausschluss des nationalen Verweisungsrechts.

(2) Erfüllungsort ist der Ort der beruflichen Niederlassung des Auftragnehmers.

(3) Gerichtsstand ist – mangels abweichender schriftlicher Vereinbarung – das sachlich zuständige Gericht des Erfüllungsortes.

II. TEIL

15. Ergänzende Bestimmungen für Verbrauchergeschäfte

(1) Für Verträge zwischen Wirtschaftstreuhändern und Verbrauchern gelten die zwingenden Bestimmungen des Konsumentenschutzgesetzes.

(2) Der Auftragnehmer haftet nur für vorsätzliche und grob fahrlässig verschuldete Verletzung der übernommenen Verpflichtungen.

(3) Anstelle der im Punkt 7 Abs 2 normierten Begrenzung ist auch im Falle grober Fahrlässigkeit die Ersatzpflicht des Auftragnehmers nicht begrenzt.

(4) Punkt 6 Abs 2 (Frist für Mängelbeseitigungsanspruch) und Punkt 7 Abs 4 (Geltendmachung der Schadenersatzansprüche innerhalb einer bestimmten Frist) gilt nicht.

(5) Rücktrittsrecht gemäß § 3 KSchG:

Hat der Verbraucher seine Vertragserklärung nicht in den vom Auftragnehmer dauernd benützten Kanzleiräumen abgegeben, so kann er von seinem Vertragsantrag oder vom Vertrag zurücktreten. Dieser Rücktritt kann bis zum Zustandekommen des Vertrages oder danach binnen einer Woche erklärt werden; die Frist beginnt mit der Ausfolgung einer Urkunde, die zumindest den Namen und die Anschrift des Auftragnehmers sowie eine Belehrung über das Rücktrittsrecht enthält, an den Verbraucher, frühestens jedoch mit dem Zustandekommen des Vertrages zu laufen. Das Rücktrittsrecht steht dem Verbraucher nicht zu,

1. wenn er selbst die geschäftliche Verbindung mit dem Auftragnehmer oder dessen Beauftragten zwecks Schließung dieses Vertrages angebahnt hat,

2. wenn dem Zustandekommen des Vertrages keine Besprechungen zwischen den Beteiligten oder ihren Beauftragten vorangegangen sind oder

3. bei Verträgen, bei denen die beiderseitigen Leistungen sofort zu erbringen sind, wenn sie üblicherweise von Auftragnehmern außerhalb ihrer Kanzleiräume geschlossen werden und das vereinbarte Entgelt € 15 nicht übersteigt.

Der Rücktritt bedarf zu seiner Rechtswirksamkeit der Schriftform. Es genügt, wenn der Verbraucher ein Schriftstück, das seine Vertragserklärung oder die des Auftragnehmers enthält, dem Auftragnehmer mit einem Vermerk zurückstellt, der erkennen lässt, dass der Verbraucher das Zustandekommen oder die Aufrechterhaltung des Vertrages ablehnt. Es genügt, wenn die Erklärung innerhalb einer Woche abgesendet wird.

Tritt der Verbraucher gemäß § 3 KSchG vom Vertrag zurück, so hat Zug um Zug

1. der Auftragnehmer alle empfangenen Leistungen samt gesetzlichen Zinsen vom Empfangstag an zurückzuerstatten und den vom Verbraucher auf die Sache gemachten notwendigen und nützlichen Aufwand zu ersetzen,

2. der Verbraucher dem Auftragnehmer den Wert der Leistungen zu vergüten, soweit sie ihm zum klaren und überwiegenden Vorteil gereichen.

Gemäß § 4 Abs 3 KSchG bleiben Schadenersatzansprüche unberührt.

(6) Kostenvoranschläge gemäß § 5 KSchG:

Für die Erstellung eines Kostenvoranschlages im Sinn des § 1170a ABGB durch den Auftragnehmer hat der Verbraucher ein Entgelt nur dann zu zahlen, wenn er vorher auf diese Zahlungspflicht hingewiesen worden ist.

Wird dem Vertrag ein Kostenvoranschlag des Auftragnehmers zugrunde gelegt, so gilt dessen Richtigkeit als gewährleistet, wenn nicht das Gegenteil ausdrücklich erklärt ist.

(7) Mängelbeseitigung: Punkt 6 wird ergänzt:

Ist der Auftragnehmer nach § 932 ABGB verpflichtet, seine Leistungen zu verbessern oder Fehlendes nachzutragen, so hat er diese Pflicht zu erfüllen, an dem Ort, an dem die Sache übergeben worden ist. Ist es für den Verbraucher tunlich, die Werke und Unterlagen vom Auftragnehmer gesendet zu erhalten, so kann dieser diese Übersendung auf seine Gefahr und Kosten vornehmen.

(8) Gerichtsstand: Anstelle Punkt 14. (3) gilt:

Hat der Verbraucher im Inland seinen Wohnsitz oder seinen gewöhnlichen Aufenthalt oder ist er im Inland beschäftigt, so kann für eine Klage gegen ihn nach den §§ 88, 89, 93 Abs 2 und 104 Abs1 JN nur die Zuständigkeit eines Gerichtes begründet werden, in dessen Sprengel der Wohnsitz, der gewöhnliche Aufenthalt oder der Ort der Beschäftigung liegt.

(9) Verträge über wiederkehrende Leistungen:

(a) Verträge, durch die sich der Auftragnehmer zu Werkleistungen und der Verbraucher zu wiederholten Geldzahlungen verpflichten und die für eine unbestimmte oder eine ein Jahr übersteigende Zeit geschlossen worden sind, kann der Verbraucher unter Einhaltung einer zweimonatigen Frist zum Ablauf des ersten Jahres, nachher zum Ablauf jeweils eines halben Jahres kündigen.

(b) Ist die Gesamtheit der Leistungen eine nach ihrer Art unteilbare Leistung, deren Umfang und Preis schon bei der Vertragsschließung bestimmt sind, so kann der erste Kündigungstermin bis zum Ablauf des zweiten Jahres hinausgeschoben werden. In solchen Verträgen kann die Kündigungsfrist auf höchstens sechs Monate verlängert werden.

(c) Erfordert die Erfüllung eines bestimmten, in lit. a) genannten Vertrages erhebliche Aufwendungen des Auftragnehmers und hat er dies dem Verbraucher spätestens bei der Vertragsschließung bekannt gegeben, so können den Umständen angemessene, von den in lit. a) und b) genannten abweichende Kündigungstermine und Kündigungsfristen vereinbart werden.

(d) Eine Kündigung des Verbrauchers, die nicht fristgerecht ausgesprochen worden ist, wird zum nächsten nach Ablauf der Kündigungsfrist liegenden Kündigungstermin wirksam.