LOGISTIK IM FLUSS.

Auftragsverarbeitungsvertrag (gemäß Art. 28 DS-GVO)

zwischen

dem ***Nutzer*** (wie im Hauptvertrag definiert)

(nachfolgend „***Auftraggeber***“ genannt)

und

der ***TB Digital Services GmbH***, Oskar-Schlemmer-Str. 19 - 21, 80807 München

(nachfolgend „***Auftragnehmer***“ genannt)

(der Auftraggeber und der Auftragnehmer nachfolgend je eine „***Partei***“ und zusammen die „***Parteien***“).

Präambel

(A) Dieser Auftragsverarbeitungsvertrag (nachfolgend „***Vertrag***“) findet Anwendung auf alle Tätigkeiten, bei denen der Auftragnehmer mit personenbezogenen Daten (wie in Ziffer 1.5 unten definiert) des Auftraggebers, von Drittanbietern oder von sonstigen Betroffenen im Zusammenhang mit der in Ziffer 2 beschriebenen Tätigkeit aus den Allgemeinen Rahmenbedingungen zur Plattform-Nutzung (nachfolgend „***Hauptvertrag***“) und ggf. darunter abgeschlossener Einzelverträge für weitere Dienste in Berührung kommt.

(B) Unter diesem Vertrag handelt der Auftraggeber als Verantwortlicher und der Auftragnehmer als Auftragsverarbeiter im Rahmen einer Auftragsverarbeitung gemäß Art. 28 DS-GVO (wie unten definiert).

Die Parteien vereinbaren daher wie folgt:

1 Definitionen und Interpretation

1.1 „***Europäisches Recht***“ ist das anwendbare Recht der Europäischen Union, die anwendbaren Gesetze der derzeitigen Mitgliedstaaten der Europäischen Union sowie die anwendbaren Gesetze eines jeden Staates, der nachträglich ein Mitgliedstaat der Europäischen Union wird.

1.2 „***Europäisches Datenschutzrecht***“ ist das anwendbare Recht der Europäischen Union zur Verarbeitung personenbezogener Daten (insbesondere die DS-GVO), die anwendbaren Gesetze der derzeitigen Mitgliedstaaten der Europäischen Union zur Verarbeitung personenbezogener Daten (insbesondere das BDSG in seiner jeweils geltenden Fassung) sowie die anwendbaren Gesetze eines jeden Staates zur Verarbeitung personenbezogener Daten, der nachträglich ein Mitgliedstaat der Europäischen Union wird.

1.3 „***DS-GVO***“ ist die „VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)“.

1.4 „***BDSG***“ ist das Bundesdatenschutzgesetz.

1.5 „***Personenbezogene Daten***“ hat die Bedeutung wie im BDSG/in der DS-GVO definiert.

2 Gegenstand der Datenverarbeitung / Pflichten des Auftraggebers

2.1 Dieser Vertrag regelt die Verpflichtungen der Parteien in Zusammenhang mit der Verarbeitung personenbezogener Daten des Auftraggebers durch den Auftragnehmer im Rahmen des im Anhang 1 genannten Hauptvertrages und ggf. darunter abgeschlossener Einzelverträge für weitere Dienste.

2.2 Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen ergeben sich aus Anhang 1 dieses Vertrages und der Leistungsbeschreibung des Hauptvertrages sowie den Leistungsbeschreibungen der ggf. darunter abgeschlossenen Einzelverträge für weitere Dienste.

2.3 Der Auftraggeber bleibt Verantwortlicher im Sinne der DS-GVO und gewährleistet die Zulässigkeit der Verarbeitung der personenbezogenen Daten der betroffenen Personen (Fahrer und ggf. weitere Personen). Diesbezüglich kommt der Auftraggeber insbesondere seiner umfassenden Informationspflicht nach und stellt sicher, dass für die Verarbeitung der personenbezogenen Daten eine datenschutzrechtliche Rechtsgrundlage vorliegt (z.B. Abschluss einer Betriebsvereinbarung, Beschränkung der Verarbeitung auf Zwecke des Beschäftigungsverhältnisses).

3 Pflichten des Auftragnehmers

3.1 Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers ausschließlich für die im Anhang 1 genannten Zwecke und im Rahmen des Hauptvertrages und ggf. darunter abgeschlossener Einzelverträge für weitere Dienste im Auftrag und gemäß den im Anhang 1 dokumentierten Weisungen des Auftraggebers; der Auftragnehmer verarbeitet die personenbezogenen Daten unter diesem Vertrag für keine anderen Zwecke. Davon unberührt bleibt die Verarbeitung außerhalb dieses Vertrages für eigene Zwecke nach Ziffer 8.3.4 des Hauptvertrages. Kopien oder Duplikate personenbezogener Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten benötigt werden.

3.2 Nach Abschluss der Erbringung der Verarbeitungsleistungen hat der Auftragnehmer sämtliche personenbezogene Daten des Auftraggebers dem Auftraggeber nach dessen Wahl entweder auszuhändigen und/oder bei sich datenschutzgerecht zu löschen, soweit dem gesetzliche Aufbewahrungsfristen nicht entgegenstehen und soweit der Auftragnehmer sie nicht für eigene Zwecke außerhalb dieses Vertrages nach Ziffer 8.3.4. des Hauptvertrages verarbeitet. Gleiches gilt für Test- und Ausschussmaterial.

3.3 Soweit vom Leistungsumfang erfasst, unterstützt der Auftragnehmer den Auftraggeber bei der Erfüllung der Betroffenenrechte (Auskunft, Berichtigung, Widerspruch, Löschung) nach entsprechender Weisung des Auftraggebers.

3.4 Der Auftragnehmer bestätigt, dass er – soweit gesetzlich erforderlich – einen betrieblichen Datenschutzbeauftragten bestellt hat (vgl. § 38 BDSG, Art. 37 DS-GVO).

3.5 Der Auftragnehmer verpflichtet sich, dem Auftraggeber das Ergebnis von Prüfungen der Datenschutzaufsichtsbehörden unverzüglich bekannt zu geben, soweit diese mit der Verarbeitung der Daten des Auftraggebers in Zusammenhang stehen. Etwa festgestellte Beanstandungen wird der Auftragnehmer innerhalb angemessener Frist beheben und dies dem Auftraggeber mitteilen.

Die Verarbeitung der Daten durch den Auftragnehmer und die vom Auftraggeber genehmigten Unterauftragnehmer (siehe Ziffer 5 dieses Vertrages) findet grundsätzlich ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union, in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder in einem solchen Land statt, für das ein Angemessenheitsbeschluss der Europäischen Kommission gem. Art. 45 DS-GVO vorliegt. Jede Verlagerung der Verarbeitung in ein sonstiges Land (nachfolgend „***unsicheres Drittland***“) darf zudem erfolgen, wenn die gesetzlichen Voraussetzungen für Datenübermittlungen in Drittländer nach den anwendbaren Datenschutzgesetzen (vgl. Art. 46 ff. DS-GVO) erfüllt sind. Wenn die Verarbeitung der Daten durch den Auftragnehmer ausschließlich oder auch in einem unsicheren Drittland erfolgt, gelten die mit dem Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 erlassenen EU-Standardvertragsklauseln.

3.6 Der Auftragnehmer hat die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut zu machen und auf das Datengeheimnis zu verpflichten (vgl. Art. 28 Abs. 3 b DS-GVO) sowie durch geeignete Schritte sicherzustellen, dass jene Mitarbeiter personenbezogene Daten nur auf Anweisung des Auftraggebers verarbeiten.

3.7 Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften dieses Vertrages und der dokumentierten Weisungen des Auftraggebers regelmäßig während der gesamten Vertragslaufzeit. Die Ergebnisse der Kontrollen sind dem Auftraggeber auf Verlangen vorzulegen, soweit diese für die Verarbeitung der Daten des Auftraggebers relevant sind. Die Maßnahmen zur Überwachung sind in einem Datenschutzkonzept beschrieben, das dem Auftraggeber auf Anforderung vorzulegen ist.

3.8 Der Auftragnehmer hat den Auftraggeber angesichts der Art der Verarbeitung und nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DS-GVO genannten Rechte der betroffenen Personen nachzukommen. Der Auftraggeber hat die dabei dem Auftragnehmer entstehenden Kosten zu tragen.

3.9 Der Auftragnehmer hat den Auftraggeber angesichts der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Art. 32 bis 36 DS-GVO genannten Pflichten zu unterstützen.

4 Technische und Organisatorische Maßnahmen zur Datensicherheit

4.1 Der Auftragnehmer wird angemessene technische und organisatorische Maßnahmen zum Datenschutz ergreifen (vgl. Art. 32 DS-GVO). Der Auftragnehmer ist insbesondere verpflichtet, die im Anhang 2 zu diesem Vertrag vertraglich vereinbarten technischen und organisatorischen Maßnahmen umzusetzen. Diese Maßnahmen sind vom Auftragnehmer im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung anzupassen, ohne dabei das Schutzniveau zu senken. Wesentliche Änderungen sind schriftlich zu vereinbaren.

4.2 Der Auftragnehmer ist verpflichtet, eine angemessene Dokumentation der Datenverarbeitung zu führen. Der Nachweis kann auch durch ein genehmigtes Zertifizierungsverfahren gemäß Art. 42 DS-GVO erfolgen.

5 Unterauftragnehmer

5.1 Dem Auftragnehmer wird hiermit die Einschaltung der im Anhang 1 genannten Unterauftragnehmer gestattet.

5.2 Die Einschaltung weiterer Unterauftragnehmer wird hiermit generell genehmigt. Der Auftragnehmer wird den Auftraggeber aber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern informieren. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

5.3 Nimmt der Auftragnehmer einen Unterauftragnehmer in Anspruch, hat der Auftragnehmer sicherzustellen, dass diesem im Wege (i) eines zwischen dem Unterauftragnehmer und dem Auftragnehmer abzuschließenden Vertrages oder (ii) weiteren Rechtsinstruments nach Europäischem Datenschutzrecht dieselben Datenschutzpflichten auferlegt werden, wie sie dem Auftragnehmer nach diesem Vertrag auferlegt werden. Dabei ist durch den Auftragnehmer insbesondere sicherzustellen, dass der Unterauftragnehmer hinreichende Garantien dafür bietet, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung von personenbezogenen Daten entsprechend den Anforderungen der DS-GVO erfolgt.

6 *Kontrollrechte*

6.1 Der Auftraggeber hat das Recht, die Einhaltung der Verpflichtungen aus diesem Vertrag (einschließlich erteilter Weisungen) selbst oder durch einen vom Auftraggeber benannten geeigneten Dritten zu kontrollieren bzw. kontrollieren zu lassen.

6.2 Der Auftragnehmer gewährt dem Auftraggeber bei den Kontrollen angemessen Unterstützung. Insbesondere gewährt der Auftragnehmer Zugang zu Datenverarbeitungsanlagen und erteilt erforderliche Auskünfte.

6.3 Für den Fall, dass eine Kontrolle zu dem Ergebnis führt, dass der Auftragnehmer und/oder die Verarbeitung nicht die Vorgaben dieses Vertrages und/oder Europäischen Datenschutzrechts einhält, wird der Auftragnehmer sämtliche Korrekturmaßnahmen vornehmen, die erforderlich sind, um eine Einhaltung der Vorgaben dieses Vertrages und/oder Europäischen Datenschutzrechts zu gewährleisten.

6.4 Die Kosten, die dem Auftraggeber durch Vornahme einer Kontrolle entstehen, hat er selbst zu tragen. Die Kosten, die dem Auftragnehmer durch Vornahme einer Kontrolle durch den Auftraggeber entstehen, kann er von dem Auftraggeber verlangen.

6.5 Kontrollen beim Auftragnehmer sind rechtzeitig anzukündigen und dürfen den Geschäftsbetrieb des Auftragnehmers nicht unverhältnismäßig beeinträchtigen.

7 *Hinweispflichten*

Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn eine vom Auftraggeber erteilte Weisung nach Meinung des Auftragnehmers gegen Europäisches Datenschutzrecht verstößt. Die zu Recht beanstandete Weisung braucht nicht befolgt zu werden, solange sie nicht durch den Auftraggeber geändert oder ausdrücklich bestätigt wird. Zu einer materiell-rechtlichen Prüfung von Weisungen ist der Auftragnehmer nicht verpflichtet.

Der Auftragnehmer hat bei der Feststellung von Fehlern oder Unregelmäßigkeiten der Datenverarbeitung oder bei Verdacht eines Datenschutzverstoßes (zusammen nachfolgend ein „***Vorfall***“) unverzüglich den Auftraggeber angemessen zu informieren. Der Auftragnehmer muss den Vorfall einschließlich aller Sachverhaltsumstände, seiner Auswirkungen und sämtlicher Maßnahmen zur Behebung dokumentieren.

8 *Haftung und Freistellung*

8.1 Der Auftragnehmer haftet für Schäden, die durch Vorsatz und/oder grobe Fahrlässigkeit vom Auftragnehmer oder seinen Erfüllungsgehilfen herbeigeführt wurden. Für Schäden, die auf einfacher Fahrlässigkeit des Auftragnehmers oder seiner Erfüllungsgehilfen beruhen, haftet der Auftragnehmer nur, soweit eine

Kardinalpflicht verletzt wird. Kardinalpflichten sind wesentliche Vertragspflichten, die eine ordnungsgemäße Durchführbarkeit des Vertrages erst ermöglichen und auf deren Erfüllung der Auftraggeber vertraut hat und vertrauen durfte. Bei einfacher Fahrlässigkeit hinsichtlich der Verletzung solcher Kardinalpflichten ist die Haftung des Auftragnehmers auf die typischerweise vorhersehbaren Schäden begrenzt.

8.2 Der Auftraggeber stellt den Auftragnehmer von sämtlichen Ansprüchen Dritter (einschließlich betroffener Personen und/oder Datenschutzbehörden), Schäden und Aufwendungen frei, die auf einem Verstoß des Auftraggebers gegen die Bestimmungen dieses Vertrages und/oder gegen Europäisches Datenschutzrecht beruhen; dies gilt nicht, sofern der Auftraggeber den Verstoß nicht verschuldet hat oder soweit der Auftragnehmer zu dem Verstoß beigetragen hat.

9 Laufzeit

Die Laufzeit dieses Vertrages entspricht der Laufzeit des Hauptvertrages. Mit der Beendigung des Hauptvertrages aus welchem Grund auch immer wird dieser Vertrag automatisch beendet. Die Kündigung aus wichtigem Grund bleibt unberührt.

10 Sonstiges

10.1 Die Leistungen des Auftragnehmers nach diesem Vertrag sind durch die im Hauptvertrag und durch die in den ggf. darunter abgeschlossenen Einzelverträgen für weitere Dienste geregelten Vergütungsregelung abgegolten.

10.2 Sind personenbezogene Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch Insolvenz oder Vergleichsverfahren oder durch sonstige vergleichbare Ereignisse gefährdet, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren.

10.3 Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder werden, so berührt dies die Wirksamkeit der übrigen Bestimmungen nicht. Die Parteien werden im Falle der Unwirksamkeit einer Klausel eine in sachlicher und wirtschaftlicher Hinsicht am Zweck des Vertrages orientierte ersatzweise Regelung vereinbaren.

10.4 Dieser Auftragsverarbeitungsvertrag liegt in unterschiedlichen sprachlichen Fassungen vor, wobei die deutsche Originalfassung im Falle von Abweichungen Vorrang hat.

10.5 Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN Kaufrechts. Ausschließlicher Gerichtsstand ist München.

10.6 Die folgenden Anhänge sind Vertragsbestandteil:

Anhang 1 – Beschreibung der Auftragsverarbeitung

Anhang 2 – Technische und organisatorische Maßnahmen

ANHANG 1 – Beschreibung der Auftragsverarbeitung

11 Hauptvertrag

Hauptvertrag im Sinne von Ziffer 2.1 des Hauptteils des Vertrages sind die „Allgemeinen Rahmenbedingungen zur Plattform-Nutzung“.

Titel / Parteien: ***TB Digital Services GmbH***, Oskar-Schlemmer-Str. 19 - 21, 80807 München / ***Nutzer***

12 Gegenstand und Dauer des Auftrags

Der Gegenstand des Auftrags ergibt sich aus Ziffer 1 (*Gegenstand*) und Ziffer 8 (*Daten des Nutzers und Datenschutz*) des Hauptvertrages; die Dauer des Auftrags ergibt sich aus Ziffer 7 (*Vertragsschluss, Vertragsdauer und Kündigungsrechte*) des Hauptvertrages.

13 Umfang, Art und Zweck der Datenverarbeitung / Datenverarbeitungsmaßnahmen

Umfang, Art und Zweck der Verarbeitung personenbezogener Daten ergeben sich aus Ziffer 8 des Hauptvertrages.

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Umfang, Art und Zweck:

Um die vom Auftragnehmer angebotenen Dienste (wie im Hauptvertrag definiert) erbringen zu können, muss der Auftragnehmer personenbezogene Daten des Auftraggebers über Connected Vehicles oder Mobile Devices (und ggf. von einem Drittanbieter, mit dem der Nutzer Drittdienste vereinbart hat, übertragene personenbezogene Daten) im für die Erbringung der Dienste erforderlichen Maß erheben und an die Plattform des Auftragnehmers übertragen und dort speichern. Der Auftragnehmer wird die auf der Plattform gespeicherten Daten im für die Diensteerbringung erforderlichen Umfang verarbeiten (etwa um anhand der personenbezogenen Daten das Fahrverhalten der Fahrer sowie die Nutzung des Connected Vehicle oder Mobile Device zu analysieren und auszuwerten und dem Auftraggeber darauf basierend speziell auf ihn zugeschnittene Angebote wie etwa Fahrertrainings, Ausstattungsdetails sowie Vorschläge zur Effizienzsteigerung zu unterbreiten). Genauer Umfang, Art und Zweck ergeben sich insbesondere aus den zusätzlich abzuschließenden Einzelverträgen.

14 Kreis der Betroffenen (Kategorien betroffener Personen)

Von der Auftragsverarbeitung sind folgende Personenkreise betroffen:

- ***Fahrer und sonstige Mitarbeiter des Nutzers*** (Mitarbeiter der eigenen Gesellschaft des Auftraggebers, z.B. Arbeitnehmer, Auszubildende, Bewerber, ehem. Beschäftigte);
- ***Fahrer***, die keine Mitarbeiter sind;
- ***Ansprechpartner*** von Verladern/Entladern oder sonstigen Geschäftspartnern des Auftraggebers; und
- ***Konzern-Mitarbeiter*** (Mitarbeiter einer anderen Gruppengesellschaft des Auftraggebers).

15 Art der personenbezogenen Daten

Die Auftragsverarbeitung umfasst die folgenden Arten personenbezogener Daten:

- Name und Unternehmensbezeichnung des Nutzers;
- Name des Fahrers und Fahreridentifikationsnummer;
- Fahrzeugidentifikationsnummer;
- Zustandsdaten des Connected Vehicle;
- Standortdaten;
- Daten zu Lenk- und Ruhezeiten;
- Daten zum Fahrverhalten;
- Zustandsdaten von Auf- bzw. Anbauten, Aggregaten und weiteren Fahrzeugbauteilen;
- Zustandsdaten von ggf. verbundenen IOT-Devices;
- Zustandsdaten von Mobile Devices;
- Ladungsdaten;
- Auftragsdaten; und
- Kontaktdaten zu Ansprechpartnern von Verladern/Entladern oder sonstigen Geschäftspartnern des Auftraggebers.

16 Dokumentierte Weisungen

Der Auftraggeber weist den Auftragnehmer hiermit an, die personenbezogenen Daten wie in Ziffer 8 des Hauptvertrages und ggf. darunter abgeschlossener Einzelverträge für weitere Dienste zu verarbeiten. Dies schließt insbesondere die folgende Verarbeitung mit ein:

- Die personenbezogenen Daten werden über das Connected Vehicle oder Mobile Device an die cloud-basierte Plattform des Auftragnehmers übertragen und dort gespeichert.
- Die personenbezogenen Daten werden unter diesem Vertrag nur verarbeitet, soweit es für die Erfüllung des Hauptvertrages erforderlich ist; Ziffer 8.3.4 des Hauptvertrages bleibt unberührt.
- Der Auftragnehmer übermittelt die personenbezogenen Daten an einen Drittanbieter (wie im Hauptvertrag definiert), sofern und soweit eine derartige Übermittlung an den Drittanbieter erforderlich ist, damit dieser seine Drittdienste (wie im Hauptvertrag definiert) an den Auftraggeber erbringen kann.
- Der Auftragnehmer wird anhand der personenbezogenen Daten das Fahrverhalten der Fahrer sowie die Nutzung des Connected Vehicles analysieren und auswerten und dem Auftraggeber darauf basierend speziell auf ihn zugeschnittene Angebote wie etwa Fahrertrainings, Ausstattungsdetails sowie Vorschläge zur Effizienzsteigerung unterbreiten.

17 Ort der Verarbeitung

- Bundesrepublik Deutschland.
- Mitgliedsstaat der Europäischen Union oder Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum.
- Länder für die ein Angemessenheitsbeschluss der Europäischen Kommission gem. Art. 45 DS-GVO vorliegt.
- Sofern der Auftragnehmer Unterauftragnehmer in einem unsicheren Drittland einsetzt, erfolgt die Übermittlung von personenbezogenen Daten auf Grundlage der zwischen dem Auftragnehmer und dem Unterauftragnehmer abgeschlossenen EU-Standardvertragsklauseln, welche mit Durchführungsbeschluss (EU) 2021/914 der EU-Kommission vom 4. Juni 2021 erlassen wurden.

18 Unterauftragnehmer

Der Auftragnehmer setzt folgende Unterauftragnehmer (die ggf. weitere Unterauftragnehmer einsetzen können) ein:

Unterauftragnehmer	***Land***	***Art der Dienstleistung***
AEB SE Sigmaringer Str. 109 70567 Stuttgart	Deutschland	Abgleich von Nutzer-Adressen mit Sanktionslisten/Anti-Terrorlisten zur Herstellung von Rechtskonformität im Umfeld von einschlägigen Antiterrorverordnungen.
Amazon Web Services EMEA Sàrl Avenue John F. Kennedy 38 1855 Luxemburg	Luxemburg	Plattform-Hosting / IT-Support bzgl. Plattform-Hosting (Datenspeicherung erfolgt ausschließlich auf Servern innerhalb der Europäischen Union)
Datadog, Inc. 620 8th Avenue, 45th Floor New York, NY 10018	Vereinigte Staaten von Amerika	Analyse und Monitoring von Cloud-Diensten (Datenspeicherung erfolgt ausschließlich auf Servern innerhalb der Europäischen Union)
Dogwood Labs, Inc. DBA Statuspage (ein Unternehmen der Atlassian, Inc.) 465 Pine St, Floor 13 San Francisco, CA 94104	Vereinigte Staaten von Amerika	Information über Plattformstörungen, Berichterstattung bzgl. Betriebszeiten und Wartungsmanagement (sofern der Plattform-Nutzer diesen Benachrichtigungsdienst selbst abonniert hat)

MAN Service und Support GmbH Dachauer Straße 667 80995 München	Deutschland	Bearbeitung von Nutzer-Anfragen / First Level Support
MAN Truck & Bus SE Dachauer Str. 667 80995 München	Deutschland	Bereitstellung von MAN-Diensten, Unterstützung bei und Durchführung von Marketing, Sales sowie After-Sales-Aktivitäten
MongoDB Limited Building Two Number One Ballsbridge, Dublin 4	Irland	Bereitstellung eines Nosql-Datenbanksystems
Salesforce.com EMEA Limited Floor 26 Salesforce Tower 110 Bishopsgate London, EC2N 4AY	Vereinigtes Königreich	Verwaltung von Kundendaten und Bereitstellung von vertriebsrelevanten Kennzahlen (Datenspeicherung erfolgt ausschließlich auf Servern innerhalb der Europäischen Union)
Volkswagen AG Berliner Ring 2 38440 Wolfsburg	Deutschland	Unterstützung bei der Erbringung des RIO Dienstes WebTMS (sofern der Dienst WebTMS vom Plattform-Nutzer gebucht wurde)
Workato, Inc. 215 Castro St Mountain View, CA 94041	Vereinigte Staaten von Amerika	Bereitstellung einer Schnittstellensoftware für die Bearbeitung von Nutzer-Anfragen / Nutzer-Support-Anfragen (Datenspeicherung erfolgt auf Servern innerhalb der Europäischen Union)
Zuora, Inc. 3050 S. Delaware Street, Suite 301 San Mateo, CA 94403	Vereinigte Staaten von Amerika	Unterstützung bei der Rechnungstellung sowie buchhalterischen Prozessen (Datenspeicherung erfolgt auf Servern des Unternehmens Amazon Web Services innerhalb der Europäischen Union)

ANHANG 2 - Technische und organisatorische Maßnahmen

Die vom Auftragnehmer zu treffenden technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, sind im Datenschutzkonzept zur RIO-Plattform beschrieben und schließen insbesondere ein:

1. Pseudonymisierung

Soweit die personenbezogenen Daten für Auswertungszwecke genutzt werden, die auch mit pseudonymisierten Daten durchführbar sind, werden Pseudonymisierungstechniken eingesetzt. Dabei wird zunächst für jedes Datenfeld im Voraus definiert, ob es pseudonymisiert werden muss, weil es einen Rückschluss auf eine Person ermöglichen würde. Die Pseudonymisierungsschlüssel wer-den in einem „Data Safe“ abgelegt, für den eine maximal mögliche Zugriffsbeschränkung eingerichtet wird.

2. Verschlüsselung

Die mobilen Endgeräte kommunizieren verschlüsselt mit dem Endpunkt anhand eines geräteindividuellen Gerätezertifikats. Die Daten werden innerhalb der RIO Plattform verschlüsselt weitertransportiert („Ubiquitous encryption“ oder „encryption everywhere“).

3. Gewährleistung der Vertraulichkeit

Alle Mitarbeiter sind und werden auf Ihre Verpflichtung zur Verschwiegenheit hingewiesen und schriftlich auf das Datengeheimnis verpflichtet.

Die verwendete IT Infrastruktur wird durch Amazon Web Services (im Folgenden AWS) im Rahmen einer Cloud (IaaS & PaaS) zur Verfügung gestellt. Die Zutrittskontrolle stellt der AWS Data-Center-Betreiber zur Verfügung: die hochsicheren AWS-Rechenzentren verwenden elektronische Überwachungsmaßnahmen auf dem Stand der Technik und mehrstufige Zugangskontrollsysteme. Die Rechenzentren sind rund um die Uhr mit ausgebildetem Sicherheitspersonal besetzt, und der Zugriff wird streng nach dem Prinzip der geringsten Rechte und ausschließlich zum Zweck der Systemadministration gewährt.

Der Zutritt zu den Hardwarekomponenten (Clients) bei der TB Digital Services GmbH erfolgt gemäß geltender, jeweils im Einzelfall geeigneter Standard-Maßnahmen. Dies sind z.B. Zutrittsbeschränkungen durch Vereinzelungsanlagen (Drehkreuze), Videoüberwachungsanlagen, Alarmanlage und/oder Wachdienst, elektronisch oder mechanisch gesicherte Türen, einbruchsgesicherte Gebäude, dokumentierte Zutrittsberechtigungen (Besucher, Fremdkräften) oder deklarierte Sicherheitsbereiche.

Die Zugangskontrollen umfassen Maßnahmen zur Gerätesicherung, Netzwerksicherung und Anwendungssicherung.

Als Maßnahmen der Gerätesicherung im Fahrzeug werden verschiedene Maßnahmen umgesetzt: Die mobilen Endgeräte sind fest im Fahrzeug verbaut und verfügen über Secure Boot, d.h. es gibt keine Möglichkeit, ein fremdes Betriebssystem zu laden und zu starten. Die mobilen Endgeräte kommunizieren verschlüsselt mit dem Endpunkt anhand eines geräteindividuellen Gerätezertifikats. Die Daten werden innerhalb der RIO Plattform verschlüsselt weitertransportiert („Ubiquitous encryption oder „encryption everywhere“). Die Endgeräte sind durch die regelmäßige Einspielung von Sicherheitsupdates auf einem aktuellen Sicherheitsstand (Patch-Management).

Als Maßnahmen der Netzwerksicherung werden ebenfalls verschiedene Standardmaßnahmen umgesetzt: Es sind angemessene (dem Stand der Technik entsprechende) Passwortvorgaben implementiert (Passwortlänge, -komplexität, -gültigkeitsdauer, etc.). Die wiederholte fehlerhafte Eingabe von Benutzerkennung/Passwort-Kombination führt zu einer (temporären) Sperrung der Benutzerkennung. Das Unternehmensnetzwerk ist durch eine Firewall gegenüber unsicheren offenen Netzwerken abgeschottet. Ein Prozess ist etabliert, der die regelmäßige Versorgung von mobilen Geräten mit Sicherheitsupdates (OTA – Prozess) sicherstellt. Zur Aufdeckung bzw. Vermeidung von Angriffen auf das Unternehmensnetzwerk (Intranet) werden geeignete Technologien (z.B. Intrusion Detection Systeme) eingesetzt. Die Mitarbeiter werden regelmäßig bzgl. der Gefahren und Risiken sensibilisiert.

Als Maßnahmen der Anwendungssicherung werden einige Standardmaßnahmen umgesetzt:

Die relevanten Anwendungen sind durch angemessene Authentisierungs- und Autorisierungsmechanismen gegen unbefugten Zugang gesichert. Es sind angemessene (dem Stand der Technik entsprechende) Passwortvorgaben implementiert (Passwortlänge, -komplexität, -gültigkeitsdauer, etc.). Für Anwendungen mit besonderem Schutzbedarf werden starke Authentisierungsmechanismen verwendet (z.B. Token, PKI). Die wiederholte fehlerhafte Eingabe von Benutzerkennung/Passwort-Kombination führt zu einer (temporären) Sperrung der Benutzerkennung. Die im relevanten Verfahren verwendeten Daten liegen in verschlüsselter Form auf einem mobil genutzten Datenträger. Die erfolgten Zugänge und Zugangsversuche zu den Anwendungen werden protokolliert. Die erzeugten Protokolldateien werden für einen geeigneten Zeitraum (mind. 90 Tage) aufbewahrt und (stichprobenartig) geprüft.

Benutzerberechtigungen (für Zugang und Zugriff) werden mit verschiedenen Maßnahmen sichergestellt, wobei diese grundsätzlich einer bestimmbaren Person zugeordnet sind. Die Vergabe der Berechtigungen liegt in der Verantwortlichkeit des Plattform-Verantwortlichen und wird regelmäßig überprüft. Die Erteilung der Zugangsberechtigungen erfolgt nur nach einem definierten und dokumentierten Prozess. Änderungen an den Zugangsberechtigungen erfolgen nach dem Vier-Augen-Prinzip und werden in einem versionierten Logfile dokumentiert.

Als Maßnahmen zur Zugriffskontrolle bzw. -steuerung werden unterschiedliche Maßnahmen umgesetzt: Die Zugriffsrechte werden im Rahmen eines Rollen-/Berechtigungskonzeptes definiert und dokumentiert und sind entsprechend der aufgabenbedingten Erfordernisse den jeweiligen Rollen zugeordnet. Es sind spezifische Rollen/Berechtigungen für technische Administratoren eingerichtet (die, insofern technisch möglich, keinen Zugriff auf personenbezogene Daten ermöglichen). Es sind spezifische Rollen/Berechtigungen für den fachlichen Support eingerichtet (die keine technischen Administrationsrechte beinhalten).

Die Definition von Rollen/Berechtigungen und die Zuordnung von Rollen/Berechtigungen erfolgt, insofern technisch und organisatorisch möglich, nicht durch dieselben Personen und in einem revisionssicheren (Genehmigungs-)Verfahren und ist zeitlich begrenzt. Direkte Datenbankzugriffe unter Umgehung des Rollen-/Berechtigungskonzepts sind nur durch autorisierte Datenbankadministratoren möglich. Es gibt eine Regelung zum Einsatz privater Datenträger bzw. der Einsatz privater Datenträger ist verboten. Es liegen verbindliche Regelungen hinsichtlich der Datenzugriffe bei externen Wartungen, Fernwartungen und Telearbeit vor. Es erfolgt eine datenschutzgerechte Vernichtung/Entsorgung von Dokumenten und Datenträgern (z.B. Schredder, Datenschutztonne) durch zuverlässige Entsorgungsunternehmen.

Das Rollen-/Berechtigungskonzept wird regelmäßig den sich ändernden arbeitsorganisatorischen Strukturen mit angepasst (z.B. neue Rollen), und die zugeordneten Rollen/Berechtigungen werden regelmäßig überprüft (z.B. durch die Vorgesetzten) und ggf. angepasst bzw. entzogen. Es findet eine regelmäßige zentrale Kontrolle bzgl. zugewiesener Standardprofile statt. Die ändernden Zugriffe (Schreiben, Löschen) werden protokolliert, und die erzeugten Protokolldateien werden für einen geeigneten Zeitraum (mind. 90 Tage) aufbewahrt und (stichprobenartig) geprüft.

Als allgemeine Maßnahmen zur Sicherung der Weitergabe werden verschiedene Standardmaßnahmen umgesetzt:

Die mit der Weitergabe beauftragten Personen werden im Voraus mit den zu ergreifenden Sicherungsmaßnahmen vertraut gemacht. Der Empfängerkreis wird im Voraus festgelegt, so dass eine entsprechende Kontrolle (Authentifizierung) möglich ist. Der Gesamt-Prozess der Datenweitergabe ist festgelegt und dokumentiert, und die Durchführung der konkreten Datenweitergabe wird protokolliert bzw. dokumentiert (z.B. Empfangsbestätigung, Quittung). Die mit der Weitergabe beauftragten Personen führen vorab eine Plausibilitäts-; Vollständigkeits- und Richtigkeitsprüfung durch.

Vor der Durchführung der konkreten Datenübertragung erfolgt eine Überprüfung der Empfänger-Adresse (z.B. E-Mail-Adresse). Die Übertragung der Daten über das Internet erfolgt in verschlüsselter Form (z.B. Dateiverschlüsselung). Die Integrität der weitergegebenen Daten wird, insofern technisch möglich, durch den Einsatz von Signatur-Verfahren (Digitale Signatur) gewährleistet. Elektronische Empfangsbestätigungen werden in geeigneter Form archiviert. Unerwünschte Datenübertragungen im Internet werden durch geeignete Technologien (z.B. Proxy, Firewall) unterbunden.

Weiterhin werden als Maßnahmen zur Durchführung des Trennungsgebots die nachfolgenden Standardmaßnahmen umgesetzt:

Es liegen verbindliche Regelungen bzgl. der Zweckbindung der Verarbeitung zur Einhaltung des Trennungsgebots vor. Die zu bestimmten Zwecken erhobenen Daten werden gesondert von zu anderen Zwecken erhobenen Daten gespeichert. Die eingesetzten IT-Systeme erlauben die getrennte Speicherung von Daten (durch Mandantenfähigkeit oder Zugriffskonzepte). Es erfolgt eine Trennung der Daten in Test- und Produktivsystemen. Bei pseudonymisierten Daten wird die Schlüsselbrücke, die eine Re-Identifizierbarkeit ermöglicht, getrennt gespeichert bzw.

aufbewahrt. Bei Auftragsverarbeitung oder Funktionsübertragung erfolgt eine getrennte Verarbeitung der Daten unterschiedlicher Auftraggeber beim Auftragnehmer. Die vorhandenen Rollen-/Berechtigungskonzepte ermöglichen durch ihre Gestaltung die logische Trennung der verarbeiteten Daten.

4. Gewährleistung der Integrität

Als Maßnahmen zur Durchführung der Eingabeprotokollierung werden verschiedene Standardmaßnahmen umgesetzt:

Es werden Änderungen der Zugriffsrechte sowie sämtliche Administratortätigkeiten protokolliert. Es werden schreibende Zugriffe (Eingaben, Änderungen, Löschungen) und die Veränderungen an Datenfeldern protokolliert (z.B. Inhalt des neu eingegebenen oder geänderten Datensatzes). Es erfolgt eine Protokollierung von Übermittlungen (z.B. Download) und eine Login-Protokollierung.

Die genutzten Erfassungsunterlagen werden zur Nachvollziehbarkeit der Eingaben dokumentiert und archiviert. Die Protokollierung erfolgt mit Datum und Uhrzeit, Benutzer, Art der Aktivität, Anwendungsprogramm und Ordnungsnummer des Datensatzes. Die Protokollierungseinstellungen werden dokumentiert.

Es wird ausschließlich ein lesender Zugriff auf die Protokolldateien gewährt. Der Kreis der Zugriffsberechtigten auf Protokolldateien ist eng begrenzt (z.B. auf den Administrator, den Datenschutzbeauftragten, den Revisor). Die Protokolldateien werden für einen festgelegten Zeitraum (z.B. 1 Jahr) aufbewahrt und dann datenschutzgerecht gelöscht. Die Protokolldateien werden regelmäßig automatisiert ausgewertet. Auswertungen der Protokolldateien werden soweit möglich in pseudonymisierter Form erstellt.

5. Gewährleistung der Verfügbarkeit

Die Architektur ist durch interne Replizierungsmechanismen innerhalb der AWS Plattform per se gegen Datenverlust gesichert. Weiterhin werden als Maßnahmen der Objektsicherung die nachfolgenden Standardmaßnahmen der AWS umgesetzt:

Es werden Brandschutzmaßnahmen durchgeführt (z.B. Feuerschutztüren, Rauchmelder, Brandschutzwände, Rauchverbot). Die Rechneranlagen sind vor Überschwemmungen geschützt (z.B. Rechnerraum im 1. Stockwerk, Wassermelder). Es werden Maßnahmen gegen Erschütterungen durchgeführt (z.B. Rechnerraum nicht in der Nähe von Fernverkehrsstraßen, Zuggleisen, Maschinenräumen). Die Rechneranlagen sind gegen elektromagnetische Felder gesichert (z.B. Stahlplatten in Außenwänden). Es werden Maßnahmen gegen Vandalismus und Diebstahl durchgeführt (vgl. Zutrittskontrolle). Die Rechneranlagen befinden sich in klimatisierten Räumlichkeiten (Temperatur und Luftfeuchtigkeit werden durch Klimaanlage geregelt). Die Rechneranlagen sind mit einem Überspannungsschutz gegen Überspannungsspitzen gesichert. Es werden Maßnahmen zur Sicherstellung einer störungsarmen und kontinuierlichen Stromversorgung durchgeführt (z.B. USV-Geräte, Notstromaggregate).

Die Datenbestände werden regelmäßig in Form von Backup-Kopien innerhalb der AWS Plattform gesichert. Das Backup-Konzept ist dokumentiert und wird regelmäßig überprüft und aktualisiert. Backup-Medien sind vor unbefugtem Zugriff geschützt. Die eingesetzten Backup-Programme entsprechen den aktuellen Qualitätsstandards und werden diesbezüglich regelmäßig aktualisiert. Ein Redundanz-Rechenzentrum (entfernt vom Verarbeitungsort) ist eingerichtet und kann im Katastrophenfall die Datenverarbeitung fortsetzen. Die verschiedenen Maßnahmen zur Verfügbarkeitskontrolle sind in einem Notfallmanagement-Plan von AWS dokumentiert.

Bevor ein Auftrag zur Datenverarbeitung vergeben wird, wird der Auftragnehmer sorgfältig und nach festgelegten Kriterien (technische und organisatorische Maßnahmen) überprüft. Hierzu wird insbesondere eine detaillierte Darlegung der vom Auftragnehmer durchgeführten technischen/organisatorischen Datenschutzmaßnahmen eingefordert (Beantwortung Fragenkatalog oder Datenschutzkonzept) und geprüft. In Abhängigkeit von der Menge und Sensibilität der verarbeiteten Daten erfolgt diese Überprüfung ggf. auch vor Ort beim Auftragnehmer. Geeignete Zertifizierungen (z.B. ISO 27001) werden bei der Auswahl von Auftragnehmern berücksichtigt. Die Feststellung der Eignung des Auftragnehmers wird in angemessener und nachvollziehbarer Form dokumentiert.

Zur Begründung des Auftragsverhältnisses wird ein Auftragsverarbeitungsvertrag zwischen Auftraggeber und Auftragnehmer abgeschlossen. Dieser legt detailliert und schriftlich die Zuständigkeiten und Verantwortlichkeiten sowie die Pflichten beider Parteien fest. Falls ein beauftragter Dienstleister seinen Sitz außerhalb der EU bzw. des EWR hat, werden die EU-Standardvertragsklauseln angewendet. Es ist vertraglich festgelegt, dass die Datenverarbeitung durch den Auftragnehmer nur im Rahmen der Weisungen des Auftraggebers erfolgen darf. Der Auftragnehmer wird verpflichtet, den Auftraggeber unverzüglich darauf hinzuweisen, wenn eine seiner Weisungen nach Ansicht des Auftragnehmers gegen Vorschriften des Datenschutzes verstößt. Um den Rechten der Betroffenen gerecht zu werden, wird im Auftragsverarbeitungsvertrag vereinbart, dass der Auftragnehmer den Auftraggeber angemessen zu unterstützen hat, soweit dies z.B. im Fall der Erteilung von Auskünften an Betroffene erforderlich ist.

Im weiteren Verlauf der Auftragsverarbeitung kontrolliert der Auftraggeber die Arbeitsergebnisse des Auftragnehmers formal und inhaltlich. Die Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen wird regelmäßig überprüft. Hierfür wird vornehmlich die Vorlage von aktuellen Testaten oder geeigneten Zertifizierungen bzw. der Nachweis von durchgeführten IT-Sicherheits- oder Datenschutzaudits genutzt. Soweit Unterauftragnehmer eingesetzt werden, ist vertraglich bestimmt, dass diese entsprechend kontrolliert werden.

6. Gewährleistung der Belastbarkeit der Systeme

Die AWS Cloud-Infrastruktur wurde als eine der flexibelsten und sichersten Cloud Computing-Umgebungen geschaffen. Sie wurde für ein Optimum an Verfügbarkeit bei vollständiger Kundentrennung konzipiert. Sie liefert eine extrem skalierbare, sehr betriebssichere Plattform, die es den Kunden erlaubt, Anwendungen und Inhalte bei Bedarf schnell und sicher weltweit auszubringen. Die AWS-Services sind insofern inhalteunabhängig, als sie allen Kunden dasselbe hohe Sicherheitsniveau bieten, unabhängig von der Art der Inhalte oder von der geographischen Region, in der die Inhalte gespeichert werden.

Die hochsicheren AWS-Rechenzentren auf Weltklasseniveau verwenden elektronische Überwachungsmaßnahmen auf dem Stand der Technik und mehrstufige Zugangskontrollsysteme. Die Rechenzentren sind rund um die Uhr mit ausgebildetem Sicherheitspersonal besetzt, und der Zugriff wird streng nach dem Prinzip der geringsten Rechte und ausschließlich zum Zweck der Systemadministration gewährt.

7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

Die AWS-Rechenzentren werden in Clustern in verschiedenen Regionen der Welt errichtet. Alle Rechenzentren sind online und bedienen Kunden; kein Rechenzentrum ist abgeschaltet. Bei einem Ausfall verschieben automatische Prozesse den Kundendatenverkehr weg von den betroffenen Bereichen. Die Kernanwendungen werden in einer N+1-Konfiguration bereitgestellt, sodass im Falle eines Rechenzentrumsausfalls ausreichend Kapazität vorhanden ist, um den Datenverkehr lastverteilt an die verbleibenden Standorte zu verteilen.

AWS bietet die Flexibilität, Instanzen zu platzieren und Daten innerhalb mehrerer geografischer Regionen sowie über mehrere Availability Zones innerhalb der einzelnen Regionen zu speichern. Jede Availability Zone wurde als unabhängige Ausfallszone entwickelt. Dies bedeutet, dass Availability Zones innerhalb einer typischen Stadtregion physisch verteilt sind und sich z.B. in Gebieten mit niedrigerem Überschwemmungsrisiko befinden (je nach Region gibt es unterschiedliche Überschwemmungszonenkategorisierungen). Zusätzlich zu einer eigenständigen unterbrechungsfreien Stromversorgung und Notstromgeneratoren vor Ort werden alle Availability Zones über unterschiedliche Stromnetze von unabhängigen Stromversorgern gespeist, um Einzelfehlerstellen zu minimieren. Sämtliche Availability Zones sind redundant mit mehreren Tier-1-Transit-Providern verbunden.

Das Amazon-Team zur Verwaltung von Vorfällen wendet branchenübliche diagnostische Verfahren an, um die Behebung unternehmenskritischer Vorfälle voranzutreiben. Das Betriebspersonal bietet eine kontinuierliche Besetzung rund um die Uhr, sieben Tage die Woche und an 365 Tagen im Jahr, um Störfälle zu erkennen und deren Auswirkungen und Behebung zu verwalten.

8. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Die im Unternehmen vorhandenen Richtlinien und Anweisungen bzw. die implementierten Standards zur Informationssicherheit werden auch in Bezug auf die Einführung und den Betrieb der RIO Plattform angewendet. Betriebliche Funktionen für Datenschutz und Informationssicherheit sind vorhanden (Datenschutzbeauftragter und Information Security Officer). Die Beschäftigten werden auf das Datengeheimnis verpflichtet und über Datensicherheits- bzw. IT-Sicherheitsmaßnahmen durch Broschüren, Flyer, Intranet-Hinweise etc. informiert.

Die internen Prozesse werden in Bezug auf die Einhaltung von technischen und organisatorischen Maßnahmen zur Datensicherheit durch Revision, Informationssicherheit und Datenschutz überprüft.

Die Verarbeitungsvorgänge und Datensicherheitsmaßnahmen werden in einem Verzeichnis der Verarbeitungstätigkeiten dokumentiert. Es findet regelmäßig eine Prüfung (intern und extern) auf Wirksamkeit der Maßnahmen statt.