Vereinbarung zur Auftragsverarbeitung

Anlage 1

Auftragsverarbeitungsvertrag

Auftraggeber (Verantwortlicher):

_____

Auftragnehmer (Auftragsverarbeiter):

NAVANDI, Inhaber Beyermann & Kern UG (haftungsbeschränkt)

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen zum Datenschutz im Rahmen der Erhebung und Verarbeitung von personenbezogenen Daten auf der Ortungsplattform telematik.navandi.de. Sie findet Anwendung auf alle im Zusammenhang mit dem Betrieb und der Anwendung der Ortungsplattform erhobenen und verarbeiteten personenbezogenen Daten von Fahrzeugführern oder Personen, die Güter mit Ortungsgeräten bewegen.

1. Gegenstand und Dauer der Vereinbarung

Gegenstand des Auftrags ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

Empfang und Speicherung von durch Ortungsgeräte übertragener Daten, Darstellung der Bewegungsabläufe von Ortungsgeräten, Verwaltung von unterschiedlichen Nutzerkonten und Ortungsgeräten, Führung des Digitalen Fahrtenbuchs einschließlich Änderungsverlauf und Export, Ermöglichen des Zugriffs auf Ortungs- und Fahrtenbuchdaten im Wege einer webbasierten Einheit und einer mobilen App nach Passwortabfrage.

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Dauer des Auftrags

Die Dauer des Vertrages über die Auftragsverarbeitungstätigkeit ist gleichlaufend mit der Dauer des Nutzungsvertrages. Hinsichtlich der Kündigung gelten die Bestimmungen des Nutzungsvertrages entsprechend.

Unabhängig davon kann der Auftraggeber diesen Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers

nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DS-GVO):

Die Verarbeitung der Daten erfolgt im Wege der Übertragung von Ortungsgeräten und der Speicherung in einem nutzerabhängigen Profil. Auf die gespeicherten Daten können der Inhaber des Nutzerkontos sowie die von ihm freigeschalteten Benutzer zugreifen. Mitarbeiter und Administratoren des Auftragnehmers greifen nur auf Weisung des Auftraggebers oder zur Behebung von Störungen zu.

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DSGVO):

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

1) Personenbezogene Daten von Hauptbenutzer:

- Name, E-Mail Adresse, Passwort (verschlüsselt in der Datenbank)
- Telefonnummer
- Individuelle Einstellungen zur Nutzung der Ortungsplattform

2) Personenbezogene Daten von Benutzer (ein Benutzer wird von einem Hauptbenutzer angelegt):

Name, E-Mail Adresse, Passwort (verschlüsselt in der Datenbank)

3) Daten, die von Ortungsgeräten übertragen werden:

- Geräte-ID
- Absendezeitpunkt der Koordinate durch das Ortungsgerät
- Eintreffzeitpunkt der Koordinate an unserem Server
- Längengrad
- Breitengrad
- Höhe über NN
- Schaltzustände der analogen und/oder digitalen Eingänge
- Geschwindigkeit des Ortungsgerätes
- Bewegungsrichtung des Ortungsgerätes
- Bewegungserkennung des Ortungsgerätes
- Werte des Beschleunigungssensor
- Mobilfunkzellendaten (Cell-ID, LAC, MNC, MCC)
- Aktiver GSM Operator
- SIM Karten ICCID
- Datenübertragungs Modus (Heim, Roaming, unbekannt)
- Signalqualität des GPS Signals
- Seriennummer des Gerätes (IMEI)
- Geofence Zonen

- Geschwindigkeit bei überschrittener Obergrenze
- Geofence Zone der Geschwindigkeitsüberschreitung
- Fahrzeug Leerlauferkennung
- Green Driving Daten (starke Beschleunigung, starkes Bremsen, starke Kurvenfahrt)
- Errechnete Wegstrecke Einzelfahrt
- Errechnete Wegstrecke Gesamt
- Abschlepperkennung
- Unfallerkennung
- iButton ID
- Schaltzustände iButton (optionaler Identifikationschip für Wegfahrsperre)
- Ereigniszustand von im Gerät selbstfestgelegten Szenarien
- digitale Daten aus dem CAN-Bus System sofern das Ortungssystem diese Daten auslesen kann
- digitale Daten aus dem FMS System sofern das Ortungssystem diese Daten auslesen kann
- digitale Daten aus dem Tachographen sofern das Ortungssystem diese Daten auslesen kann

4) Daten des Digitalen Fahrtenbuchs:

- Fahrzeug (Name, Kennzeichen, Kraftstoffart), Fahrer (Name, Kennung), Benutzer des Kontos (Name, Kennung der Ortungsplattform)
- Fahrtbeginn und -ende (Datum, Uhrzeit), Kilometerstände, Fahrerzuordnung, Fahrtdaten wie Durchschnitts- und Höchstgeschwindigkeit, Höhe und Kurs, Start- und Zielkoordinaten mit Adressen (bei privat und Arbeitsweg werden die Orte und Fahrtrohdaten beim Festschreiben gelöscht)
- Füllstand oder Ladestand zu Fahrtbeginn und -ende, erkannte Tank- und Ladevorgänge, Menge, Betrag, Notiz
- Einstufung der Fahrt (geschäftlich, privat, Arbeitsweg)
- Wohnort des Fahrers: Koordinaten und Umkreis (100 bis 500 m), nur wenn Heimfahrten erlaubt sind und der Fahrer ihn selbst festlegt und bestätigt; keine Adresse als Text; Protokoll der Bestätigung
- Arbeitszeit (nur wenn der Nutzer sie einschaltet): Zeitstempel für Arbeitsbeginn, Pause und Arbeitsende, bestätigte Tageszeiten, Pausen, Notizen, freie Tage; Protokoll der Kenntnisnahme der Information durch den Mitarbeiter
- Kontrollansicht: Fahrten der letzten 3 bis 30 Tage mit Fahrernamen und, bei Geschäftsfahrten, Reiseziel, Reisezweck und Geschäftspartner; bei QR-Abruf Prüfsumme des Links, Fahrzeug, Zeitraum, Zeitpunkte und Zahl der Abrufe, ohne IP-Adressen
- Reiseziel, Reisezweck, Geschäftspartner, Grund eines Umwegs, Notiz (vom Auftraggeber eingegebene Freitexte)
- Änderungsverlauf und Protokoll: Benutzer, Zeitpunkt, Art der Änderung, Prüfsumme
- Fahrer: freiwillig E-Mail-Adresse und Sprache, Fahrzeugwahl
- Technische Daten: Sitzungen (nur als Prüfwert gespeichert), Einladungscodes (als Prüfwert), Push-Abonnements, Server-Protokolle (Benutzer- und Mandantenkennung, Pfad; IP-Adresse nur bei fehlgeschlagenen Code-Eingaben)
- Problemmeldungen: Text, Sprachnachricht (nach Umwandlung in Text gelöscht, spätestens nach 7 Tagen), Bildschirmfoto (Löschung nach 90 Tagen), Seite, Rolle, Gerät, Bildschirmgröße, letzte

Fehlermeldungen

- Optional: Zugangsdaten zu einem eigenen E-Mail-Server des Auftraggebers (Passwort verschlüsselt gespeichert)

Hinweis: In Freitexten können Namen und Angaben zu Geschäftspartnern des Auftraggebers stehen. Der Auftraggeber entscheidet, was er einträgt.

Hinweis: Art und Umfang der übertragenen Daten können je nach verwendetem Ortungsgerät variieren.

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO):

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

-Mitarbeiter des Auftraggebers

-Fahrer von überwachten Fahrzeugen

-Begleitpersonen von beweglichen Gütern

-Geschäftspartner des Auftraggebers, soweit in Fahrtenbuch-Einträgen genannt

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

Weisungsberechtigte Personen des Auftraggebers sind:

_____

(Vorname, Name, Organisationseinheit, Telefon)

Weisungsempfänger beim Auftragnehmer ist:

Beyermann & Kern UG (haftungsbeschränkt), Ardennenstraße 88, 52355 Düren

Der für die Weisung zu nutzender Kommunikationskanal ist die E-Mail Adresse:

info@navandi.de

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5. Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden nicht erstellt, mit Ausnahme von Sicherungskopien, die für die Wiederherstellung nach Störungen erforderlich sind. Sie werden nach Ziffer 9 gelöscht.

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

(2) Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

(3) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an die oben genannte Stelle des Auftraggebers weiterzuleiten.

(4) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird. Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber

erteilen.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO). Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

(5) Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind.

(6) Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb**.**

(7) Der Auftragnehmer verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DS-GVO und den Widerruf einer etwaigen Zertifizierung nach Art. 42 Abs. 7 DS-GVO unverzüglich zu informieren.

6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis, Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

(1) Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer generell gestattet, Art. 28 Abs. 2 DS-GVO.

Derzeit setzt der Auftragnehmer folgende Unterauftragnehmer ein:

- STRATO GmbH, Otto-Ostrowski-Straße 7, 10249 Berlin: Hosting von Website, Shop und Digitalem Fahrtenbuch (Anwendung, Datenbank, Sicherungen) sowie der befristet gespeicherten Datenexporte (auch Daten der Ortungsplattform), Rechenzentrum in Berlin. STRATO setzt eigene Unterauftragnehmer ein, für virtuelle Server insbesondere die IONOS SE (Montabaur), die

Virtuozzo International GmbH (Schaffhausen, Schweiz, Standarddatenschutzklauseln) und die ServerGuard24 GmbH (Bonn).

- 1blu GmbH, Riedemannweg 60, 13627 Berlin: Hosting der Ortungsplattform telematik.navandi.de einschließlich der lokal betriebenen Kartendaten und eines zweiten Servers für die laufende Spiegelung (Hot-Backup), Rechenzentrum in Frankfurt am Main. 1blu setzt eigene Unterauftragnehmer ein: 1blu business GmbH und Greatnet.de GmbH (Berlin) sowie OMCnet Internet Service GmbH (Quickborn).
- Push-Dienste der Browser- und Betriebssystemhersteller (Apple, Google, Mozilla, Microsoft): Zustellung von Push-Mitteilungen des Digitalen Fahrtenbuchs, nur nach Einwilligung des Benutzers; der Inhalt ist verschlüsselt. Die Dienste können auch außerhalb der EU betrieben werden.
- E-Mail-Server von NAVANDI oder, auf Wunsch des Auftraggebers, ein eigener E-Mail-Server des Auftraggebers: Versand von Einladungen und Exporten.

Der Auftragnehmer informiert den Auftraggeber mindestens 30 Tage vor Hinzuziehung oder Ersetzung eines Unterauftragnehmers. Der Auftraggeber kann in dieser Zeit aus wichtigem Grund widersprechen. Bleibt der Widerspruch unberücksichtigt, kann der Auftraggeber den Vertrag außerordentlich kündigen. Der Einsatz eines weiteren Subunternehmers setzt ferner voraus, dass der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit mitteilt und den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Der Server-Standort darf nicht außerhalb der Europäischen Union liegen.

(2) Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

(3) Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

(4) Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO).

8. Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

(1) Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

(2) Das im Anhang 1 beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

(3) Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich. Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

9. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

Nach Abschluss der vertraglichen Arbeiten (Vertragsende, nicht Eingang der Kündigung) stellt der Auftragnehmer dem Auftraggeber die Daten 30 Tage lang zum Export bereit und löscht sie danach einschließlich der erstellten Verarbeitungs- und Nutzungsergebnisse datenschutzgerecht. Sicherungskopien werden spätestens 30 Tage nach der Löschung gelöscht oder überschrieben. Die Löschung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen. Während der Laufzeit löscht der Auftragnehmer Daten auf Weisung des Auftraggebers, soweit keine Aufbewahrungspflicht entgegensteht.

10. Haftung

Auf Art. 82 DS-GVO wird verwiesen.

11. Sonstiges

(1) Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

(2) Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

(3) Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

(4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(5) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Ort, Datum	Ort, Datum
Auftraggeber	Auftragnehmer

Anlage 1 – Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu Räumen zu verwehren, in denen Datenverarbeitungsanlagen untergebracht sind.

• Festlegung von Sicherheitsbereichen

• Realisierung eines wirksamen Zutrittsschutzes

• Protokollierung des Zutritts

• Festlegung Zutrittsberechtigter Personen

• Verwaltung von personengebundenen Zutrittsberechtigungen

• Begleitung von Fremdpersonal

• Überwachung der Räume

1.2 Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden.

• Festlegung des Schutzbedarfs

• Zugangsschutz

• Umsetzung sicherer Zugangsverfahren, starke Authentisierung

• Umsetzung einfacher Authentisierung per Username Passwort

• Protokollierung des Zugangs

• Monitoring bei kritischen IT-Systemen

• Gesicherte (verschlüsselte) Übertragung von Authentisierungsgeheimnissen

• Sperrung bei Fehlversuchen/Inaktivität und Prozess zur Rücksetzung gesperrter Zugangskennungen

• Verbot Speicherfunktion für Passwörter und/oder Formulareingaben (Server/Clients)

• Festlegung befugter Personen

• Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und Zugangsberechtigungen

• Automatische Zugangssperre und Manuelle Zugangssperre

1.3 Zugriffskontrolle

Es kann nur auf die Daten zugegriffen werden, für die eine Zugriffsberechtigung besteht. Daten können bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

• Erstellen eines Berechtigungskonzepts

• Umsetzung von Zugriffsbeschränkungen

• Vergabe minimaler Berechtigungen

• Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen

• Vermeidung der Konzentration von Funktionen

1.4 Verwendungszweckkontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

• Datensparsamkeit im Umgang mit personenbezogenen Daten

• Getrennte Verarbeitung verschiedener Datensätze

• Regelmäßige Verwendungszweckkontrolle und Löschung

• Trennung von Test- und Entwicklungsumgebung

1.5 Datenschutzfreundliche Voreinstellungen

Sofern Daten zur Erreichung des Verwendungszwecks nicht erforderlich sind, werden die technischen Voreinstellungen so festgelegt, dass Daten nur durch eine Aktion der betroffenen Person erhoben, verarbeitet, weitergegeben oder veröffentlicht werden.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

Ziel der Weitergabekontrolle ist es, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Daten träger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass über prüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

• Festlegung empfangs- /weitergabeberechtigter Instanzen/Personen

• Prüfung der Rechtmäßigkeit der Übermittlung ins Ausland

• Protokollierung von Übermittlungen gemäß Protokollierungskonzept

• Sichere Datenübertragung zwischen Server und Client

• Sicherung der Übertragung im Backend

• Sichere Übertragung zu externen Systemen

• Risikominimierung durch Netzseparierung

• Implementation von Sicherheitsgateways an den Netzübergabepunkten

• Härtung der Backendsysteme

• Beschreibung der Schnittstellen

• Umsetzung einer Maschine-Maschine-Authentisierung

• Sichere Ablage von Daten, inkl. Backups

• Gesicherte Speicherung auf mobilen Datenträgern

• Einführung eines Prozesses zur Datenträgerverwaltungen

• Prozess zur Sammlung und Entsorgung

• Datenschutzgerechter Lösch- und Zerstörungsverfahren

• Führung von Löschprotokollen

2.2 Eingabekontrolle

Zweck der Eingabekontrolle ist es, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

• Protokollierung der Eingaben

• Dokumentation der Eingabeberechtigungen

3. Verfügbarkeit, Belastbarkeit, Desaster Recovery

3.1 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

• Brandschutz

• Redundanz der Primärtechnik

• Redundanz der Stromversorgung

• Redundanz der Kommunikationsverbindungen

• Monitoring

• Resourcenplanung und Bereitstellung

• Abwehr von systembelastendem Missbrauch

• Digitales Fahrtenbuch: tägliche, verschlüsselte Datensicherung der Datenbank (14 Tage auf dem Server, 30 Tage auf einem weiteren Speicher)

• Ortungsplattform: laufende Spiegelung der Datenbank auf einen zweiten Server (Hot-Backup) zur Ausfallsicherheit; die Spiegelung folgt Änderungen und Löschungen in Echtzeit, eine zeitversetzte Sicherung früherer Stände findet nicht statt

3.2 Desaster Recovery – Rasche Wiederherstellung nach Zwischenfall (Art. 32 Abs. 1 lit. c DSGVO)

• Wiederherstellung des Digitalen Fahrtenbuchs aus der verschlüsselten Datensicherung; Wiederanlauf der Ortungsplattform auf dem gespiegelten zweiten Server

4. Datenschutzorganisation

• Festlegung von Verantwortlichkeiten

• Umsetzung und Kontrolle geeigneter Prozesse

• Melde- und Freigabeprozess

• Umsetzung von Schulungsmaßnahmen

• Verpflichtung auf Vertraulichkeit

• Regelungen zur internen Aufgabenverteilung

• Beachtung von Funktionstrennung und –zuordnung

• Einführung einer geeigneten Vertreterregelung

5. Auftragskontrolle

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

• Auswahl weiterer Auftragnehmer nach geeigneten Garantien

• Abschluss einer Vereinbarung zur Auftragsverarbeitung mit weiteren Auftragnehmern

• Abschluss einer Vereinbarung zur Auftragsverarbeitung

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

• Die Rechenzentren der eingesetzten Hosting-Dienstleister sind nach ISO 27001 zertifiziert. Der Auftragnehmer richtet seine Maßnahmen an dieser Norm aus.

• Prozess zur Evaluation der Technischen und Organisatorischen Maßnahmen

• Prozess Sicherheitsvorfall-Management

• Durchführung von technischen Überprüfungen

7. Digitales Fahrtenbuch

• Verschlüsselte Übertragung (HTTPS); Sitzungs-Cookies mit HttpOnly und Secure; nur technisch notwendige Cookies, kein Tracking

• Anmeldung der Verwaltung über das Konto der Ortungsplattform, Fahrer per Einladungscode oder QR-Code (7 Tage gültig, höchstens 3 Anmeldungen); Sitzung 30 Tage ab letzter Nutzung; Sperren meldet auf allen Geräten ab

• Rollen: Fahrer, Fahrzeugverwalter, Buchhaltung, Hauptbenutzer; Trennung der Daten verschiedener Auftraggeber auch in der Datenbank (Row-Level-Security)

• Einträge nur anfügbar (Datenbankbenutzer ohne Änderungs- und Löschrechte, Sperre durch Trigger), SHA-256-Kette je Fahrzeug, Storno mit Begründung, Prüfbericht rechnet die Kette nach

• Protokoll sicherheitsrelevanter Vorgänge (Anmeldung, Einrichtung, Export, Festschreiben, Storno, Benutzer- und Rollenänderungen, Stammdatenänderungen)

• Zugangsdaten zur Ortungsplattform und zu E-Mail-Servern werden verschlüsselt gespeichert (AES-256-GCM)

• Tägliche, verschlüsselte Datensicherung der Datenbank (age) und der Konfiguration (AES-256); Aufbewahrung 14 Tage auf dem Server, 30 Tage auf einem weiteren Speicher von NAVANDI

• Spracherkennung läuft auf dem eigenen Server; Aufnahmen verlassen ihn nicht

• Wohnort des Fahrers nur als Koordinaten mit Umkreis in der Datenbank des Digitalen Fahrtenbuchs; Hauptbenutzer und Verwaltung sehen nur, ob er festgelegt ist; Löschung durch den Fahrer, bei Entzug der Erlaubnis und mit dem Konto

• Arbeitszeitdaten nur anfügbar (Korrekturen als neue Version), je Nutzer einschaltbar, Zugriff nach Rolle

• Kontrollansicht per QR: Einwilligung des Fahrers, Link 2 Stunden gültig und höchstens 10 Abrufe, nur Prüfsumme des Links gespeichert, Protokoll ohne IP-Adressen, Zwischenspeicher der Ansicht auf dem Gerät wird beim Abmelden oder nach Ablauf der Sitzung gelöscht

8. Datenexport bei Rückgabe und Vertragsende

• Der Lesezugang auf die Konten der Ortungsplattform (nur Lesen und Nachrichten, keine Änderungsrechte) ist verschlüsselt in der Datenbank gespeichert (AES-256-GCM, Schlüssel in der Konfiguration des Servers), erscheint nicht im Protokoll und kann in der Ortungsplattform widerrufen werden

• Exportdateien werden verschlüsselt abgelegt (AES-256-GCM), der Schlüssel liegt getrennt von den Dateien in der Konfiguration des Servers; Zugriff auf Ordner und Dateien nur für den Anwendungsbenutzer; die Exportdateien sind nicht in den Datensicherungen enthalten

• Download nur nach Anmeldung und nur für Benutzer des eigenen Kontos; Löschung der Exportdateien nach Ablauf der Bereitstellung, spätestens bei der Löschung des Kunden