Annex Auftragsverarbeitung

Im Rahmen der Nutzung des von der Telefónica Germany GmbH & Co. OHG bereitgestellten Smart Mobility Dienstes Geotab werden regelmäßig personenbezogene Daten verarbeitet. Sie sind gemäß gesetzlicher Regelungen dazu verpflichtet, mit der Telefónica Germany GmbH & Co. OHG (nachfolgend Auftragnehmer) einen Vertrag über die Auftragsverarbeitung abzuschließen.

Vertragspartner sind die Telefónica Germany GmbH & Co. OHG, Georg-Brauchle-Ring 50, 80992 München, und der Kunde.

Dieser Annex konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragspartner, die sich aus der Beauftragung des Auftragnehmers („**Hauptvertrag**“) ergeben. Der Annex findet Anwendung auf alle Tätigkeiten, bei denen der Auftragnehmer personenbezogene Daten oder Daten, die dem Fernmeldegeheimnis unterliegen („**Auftraggeber-Daten**“), verarbeitet. Für diesen Annex gelten die Begriffsbestimmungen der EU-Datenschutzgrundverordnung („DS-GVO“) sowie des Bundesdatenschutzgesetzes 2017 („BDSG 2017“), sofern nichts Abweichendes bestimmt wurde.

§ 1 Vertragsgegenstand, Zweck der Datenverarbeitung, Verantwortlichkeit

(1) Zweck, Art und Umfang der Verarbeitung von Auftraggeber-Daten im Sinne dieses Vertrags sowie die Art der Daten und der Kreis der betroffenen Personen ergeben sich aus den **Anlagen 1 und 2**.

(2) Der Auftraggeber bleibt im Rahmen dieses Vertrages Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO. 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.
(3) Die Inhalte dieses Vertrags gelten auch für Tätigkeiten des Auftragnehmers im Auftrag des Auftraggebers, bei denen ein Zugriff auf Auftraggeber-Daten durch den Auftragnehmer nicht ausgeschlossen werden kann (bspw. Prüfung oder Wartung automatisierter Verfahren oder Datenverarbeitungsanlagen im Auftrag).

§ 2 Dauer des Auftrags
(1) Die Laufzeit dieses Vertrages entspricht – sofern ein Hauptvertrag geschlossen wurde – der im Hauptvertrag vereinbarten Laufzeit. Dieser Vertrag endet mit dem Hauptvertrag, ohne dass es einer separaten Kündigung dieses Vertrages bedarf. Die Parteien können diesen Vertrag nur mit dem zugrunde liegende Hauptvertrag kündigen; sofern im Hauptvertrag nichts Abweichendes vereinbart wurde.

(2) Sofern kein Hauptvertrag geschlossen wurde wird dieser Vertrag auf unbestimmte Zeit geschlossen. Die Kündigungsfrist beträgt in diesem Fall drei (3) Monate.

§ 3 Weisungsgebundene Verarbeitung und Mitteilungspflicht bei vermuteten Verstößen

(1) Der Auftragnehmer darf Auftraggeber-Daten nur auf dokumentierte Weisung des Auftraggebers – auch in Bezug auf die Übermittlung von Auftraggeber-Daten an ein Drittland oder eine internationale Organisation – verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Weisungen werden vom Auftraggeber grundsätzlich in Textform (z.B. per E-Mail) erteilt. Soweit eine Weisung ausnahmsweise mündlich erfolgt, wird diese vom Auftraggeber entsprechend in Textform (z.B. per E-Mail) bestätigt.

(3) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf hinweisen, wenn die Befolgung einer vom Auftraggeber erteilten Weisung nach seiner Ansicht gegen die DS-GVO oder eine andere Vorschrift über den Datenschutz verstößt.

§ 4 Vertraulichkeits-/ Verschwiegenheitspflicht

Der Auftragnehmer wird zur Durchführung des Vertrages nur Personen beschäftigen, die er zur Vertraulichkeit verpflichtet hat oder die einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

§ 5 Sicherheit der Verarbeitung / Technische und organisatorische Maßnahmen gemäß Art. 32 DS-GVO

(1) Der Auftragnehmer ergreift alle erforderlichen technischen und organisatorischen Maßnahmen gem. Artikel 32 DS-GVO. Diese werden in Anlage 3 spezifiziert.

(2) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Während der Dauer dieses Auftrags sind diese durch den Auftragnehmer fortlaufend an die Anforderungen dieses Auftrags anzupassen und dem technischen Fortschritt entsprechend weiterzuentwickeln. Das Sicherheitsniveau der hier und in Anlage 3 festgelegten technischen und organisatorischen Maßnahmen darf nicht unterschritten werden.

(3) Der Auftragnehmer verpflichtet sich, Änderungen der technischen und organisatorischen Maßnahmen, die einen wesentlichen Einfluss auf das gewährleistete Sicherheitsniveau haben, als Ergänzung der Anlage 3 schriftlich zu dokumentieren, was auch in einem elektronischen Format erfolgen kann, und dem Auftraggeber zur Kenntnis zu geben.

§ 6 Inanspruchnahme der Dienste weiterer Auftragsverarbeiter

(1) Der Auftragnehmer darf weitere Auftragsverarbeiter (im Folgenden: „Subunternehmer“) in Anspruch nehmen. Die zum Zeitpunkt des Vertragsschlusses in Anspruch genommenen Subunternehmer sind in **Anlage 4** zu diesem Vertrag aufgeführt. Der Auftragnehmer hat den Auftraggeber schriftlich, was auch in einem elektronischen Format erfolgen kann, über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmern zu informieren. Gegen derartige Änderungen kann der Auftragnehmer binnen 14 Tagen Einspruch erheben.

(2) Nimmt der Auftragnehmer die Dienste eines Subunternehmers in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, so werden diesem Subunternehmer im Wege eines Vertrags, der schriftlich abzufassen ist, was auch in einem elektronischen Format erfolgen kann, oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in diesem Vertrag festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DS-GVO erfolgt. Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Subunternehmers.

§ 7 Mitwirkungs-/ Unterstützungspflichten

Der Auftragnehmer unterstützt den Auftraggeber angesichts der Art der Verarbeitung mit geeigneten technischen organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DS-GVO genannten Rechte der betroffenen Person nachzukommen (Berücksichtigung von Betroffenenrechten hinsichtlich der Gewährleistung von Transparenz; Recht auf Auskunft; Berichtigungsrecht; Recht auf Löschung („Vergessenwerden"); Recht auf Einschränkung der Verarbeitung; Mitteilungsrecht bei Berichtigung und Löschung sowie Einschränkung der Verarbeitung; Recht auf Datenübertragbarkeit; Widerspruchsrecht; Rechte bei automatisierten Einzelfallentscheidungen).

§ 8 Haftung

Die Haftungs- und Schadensersatzvereinbarungen aus dem Hauptvertrag, soweit sie getroffen wurden, finden auf diesen Annex Anwendung.

§ 9 Unterstützung bei der Erfüllung von Auftraggeberpflichten

Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DS-GVO genannten Pflichten (Gewährleistung der Sicherheit der Verarbeitung; Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörden; Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person; Datenschutz-Folgenabschätzung; Vorherige Konsultation).

§ 10 Löschung und Rückgabe von Auftraggeber-Daten

Soweit gesetzliche oder anderweitige Aufbewahrungspflichten nicht entgegenstehen, wird der Auftragnehmer nach Beendigung des Auftrags auf Weisung des Auftraggebers die Auftraggeber-Daten dem Auftraggeber in einer für den Auftraggeber lesbaren und bearbeitbaren Form herausgeben oder die Auftraggeber-Daten löschen.

§ 11 Pflichtennachweis und Unterstützung bei Überprüfungen

Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten zur Verfügung. Er ermöglicht Überprüfungen – einschließlich Inspektionen –, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, und trägt zu ihrer Durchführung bei. Der Auftragnehmer kann die Einhaltung seiner Pflichten aus Art. 28 DS-GVO, insbesondere die Umsetzung der ergriffenen technischen und organisatorischen Maßnahmen auch durch Vorlage von Zertifikaten (IT-Sicherheits- oder Datenschutzaudits z.B. nach BSI-Grundschutz), Prüfberichten von unabhängigen Instanzen (z.B. Datenschutzbeauftragter, Datenschutz-/ Qualitätsauditoren, Wirtschaftsprüfer, Revision, IT-Abteilung) oder Auszügen hieraus nachweisen.

§ 12 Sonstiges, Allgemeines

(1) Die folgenden **Anlagen** sind wesentlicher Bestandteil dieses Vertrages:

- **Anlage 1:** Allgemeine Angaben zum Auftrag sowie zu Gegenstand, Art und Umfang der Datenverarbeitung.
- **Anlage 2:** Festlegung der Zwecke der Verarbeitung der Auftraggeber-Daten sowie der Art der Daten und des Kreises der betroffenen Personen
- **Anlage 3**: Beschreibung der technischen und organisatorischen Maßnahmen, die der Auftragsverarbeiter gemäß § 5 dieses Vertrages eingeführt hat
- **Anlage 4**: Angaben zu Subunternehmern des Auftragnehmers.

(2) Die Regelungen dieses Vertrags gehen abweichenden Regelungen in einem ggf. geschlossenen Hauptvertrag vor, soweit dieser Vertrag nicht ausdrücklich anderes bestimmt.

(3) Sollte eine Bestimmung dieses Vertrages unwirksam sein oder werden, oder eine an sich notwendige Regelung nicht enthalten sein, so wird dadurch die Wirksamkeit der übrigen Bestimmungen dieses Vertrages nicht berührt. Anstelle der unwirksamen Bestimmung oder zur Ausfüllung der Regelungslücke gilt eine rechtlich zulässige Regelung, die so weit wie möglich dem entspricht, was die Parteien gewollt haben oder nach Sinn und Zweck dieses Vertrages gewollt hätten, wenn sie die Regelungslücke erkannt hätten.

Anlage 1: Allgemeine Angaben zum Auftrag sowie zu Gegenstand, Art und Umfang der Datenverarbeitung

1.1	Beschreibung der konkreten Datenverarbeitung (Gegenstand, Art und Umfang)	Telefónica Germany stellt dem Kunden den Service „Smart Mobility“ zur Verfügung. Dies umfasst die Bereitstellung von Telematik-Hardware und einer cloudbasierten Software (Cloud Plattform) für die Verwaltung der Telematik Daten des Kunden, für die Telefónica Germany den Dienstleister GEOTAB INC. einsetzt. Mittels der Cloud Plattform der Dienstleister werden mittels der Telematik-Hardware Fahrzeuge des Fuhrparks vernetzt und eine digitale Fuhrparkverwaltung der Endkunden ermöglicht. Hierbei nutzt ein oder mehrere registrierter Anwender (zum Beispiel Administrator, Fuhrparkleiter und Fahrer) des Endkunden die Plattform für die effiziente Administration und Steuerung des vernetzten und digitalisierten Fuhrparks des Unternehmens (beispielweise intelligente Routenplanung, Kraftstoffverbrauchsmanagement, Auslesen der Motordaten/Fehlern zur optimierten Fuhrparkwartung, sowie Fahrzeugortung und Streckenverfolgung mittels GPS.) Um die Verwaltung der Telematik-Hardware durch die Cloud Plattform zu ermöglichen, werden unter anderem folgende Daten im System gespeichert: - Seriennummer der Telematik-Hardware - VIN (Vehicle Identifcation Number, Fahrzeugidentifkationsnummer) des Fahrzeugs (nach Verfügbarkeit) - Optional Motordaten des Fahrzeugs (je nach M2M-Leistung (Service Plan)) - Optional Kennzeichen des Fahrzeugs (Nur durch den Nutzer in der Plattform hinterlegbar) - Optional Daten des Fahrers (Nur durch den Nutzer in der Plattform hinterlegbar) - Daten des Cloud Plattform Nutzers (Vorname, Nachname, Email) - Nutzer ist in der Regel ein Mitarbeiter des Kunden - Administratordaten (Vorname, Nachname und Email) – Administrator ist in der Regel ein Mitarbeiter des Kunden (gemäß Auftragsformular der Auftraggeber) - Der Auftraggeber kann in der Cloudplattform (mygeotab) dem Auftragnehmer Telefónica Germany GmbH & Co. OHG einen so genannten „Reseller Zugriff“ gewähren (Administratorrechte, z.B. für das initiale Einrichten der Plattform für den Auftraggeber, sowie bei Supportanfragen des Auftraggebers) Der Subdienstleister (Geotab INC.) als Betreiber der Plattform hat mit der Rolle des Super Administrator Zugriff auf die gelisteten personenbezogenen Daten, nehmen aber keine Veränderungen an den personenbezogenen Daten durch, es sei denn auf Anweisung eines weisungsberechtigten Mitarbeiters von Telefónica Germany oder des Auftraggebers. Die Plattform wird als Cloud Service dem Auftraggeber zur Verfügung gestellt.
1.2	E-Mail-Adresse zur Meldung von Datenschutzvorfällen (§ 2 Abs. 7)	Email: datenschutz@telefonica.com
1.3	Betriebsstätte des Auftragnehmers	Anschrift: Telefónica Germany GmbH & Co. OHG Georg-Brauchle-Ring 50 80992 München

1.4	Weisungsbefugte Personen/ Abteilungen gegenüber dem Auftragnehmer	Fachbereich: M2M Service E-Mail-Adresse: service@m2m.telefonica.de
	Weisungsempfänger auf Seiten des Auftragnehmers	Fachbereich: M2M Service E-Mail-Adresse: service@m2m.telefonica.de
1.5	Hauptvertrag (Purchase Order-/ Vertragsbezeichnung):	Auftragsformular inkl. weiterer Anlagen, sowie ggf. individueller Rahmenvertrag
1.6	Beginn der Verarbeitung	Nach Unterschrift des Auftragsformulares seitens des Auftraggebers und Bestätigung des Auftrags durch Telefónica Germany GmbH & Co. OHG als Auftragnehmer.
1.7	Geplante Dauer des Auftrags	Maßgeblich ist die gewählte Vertragslaufzeit sowie die einschlägigen Kündigungsfristen

Anlage 2: Festlegung von Zweck der Verarbeitung der Auftraggeber-Daten sowie der Art der Daten und des Kreis der betroffenen Personen

2.1	**Zweck der** Tätigkeit des Auftragnehmers	**Zwecke bezüglich Mitarbeitern** ☒ Pflege und Verwaltung von Mitarbeiterdaten **Zwecke bezüglich IT-Leistungen** ☒ Verwaltung von Zugangs-/ Zugriffsrechten auf Informations- und Kommunikationstechnik und Unternehmensnetzwerk ☒ Software-/ Systementwicklung und Testing ☒ Software-/ Systembetrieb ☒ Wartung/ Support (maintenance) **5. Sonstige Zwecke** ☒ Sonstiges*:* „Smart Mobility“ dient der Vernetzung und Digitalisierung des Fuhrparks zur Fuhrparkverwaltung. Zum Zwecke der Fuhrparkverwaltung werden auch Daten der Nutzer des Portals sowie optional der Fahrer der Fahrzeuge verarbeitet. Zum Zwecke der Fehlererkennung und Entstörung der Geräte werden Gerätedaten der Geotab Telematik-Hardware verwaltet. Weiter werden Daten zum Zwecke der Streckenverfolgung und GPS-Ortung verarbeitet. Zur Erbringung der „Smart Mobility“ Leistungen werden weitere Fahrzeugdaten verarbeitet.
2.2	**Datenkate-gorien,** die durch den Auftragnehmer verarbeitet werden	**Daten bezüglich Mitarbeitern** ☒ Berufliche Kontaktdaten von Mitarbeitern, Zeitarbeitern, Praktikanten, Auszubildenden (berufliche Telefonnummer/ E-Mailadresse, Abteilungszugehörigkeit) ☒ Nutzerkennungen (z.B. Login-Daten, Benutzername und Passwort) **3. Sonstige Datenarten** ☒ Sonstiges*: bitte konkret angeben*: Seriennummer der Telematik-Hardware, VIN (Vehicle Identifcation Number, Fahrzeugidentifkationsnummer) des Fahrzeugs (nach Verfügbarkeit), optional Motordaten des Fahrzeugs (je nach M2M-Leistung (Service Plan)) Daten zu Mitarbeitern des Geschäftskunden, insbesondere Bestandsdaten des Cloud Plattform Nutzers (Vorname, Nachname, E-Mail) sowie Bestandsdaten des Administrators (Mitarbeiter des Geschäftskunden; Vorname, Nachname, E-Mail), Kennzeichen des Fahrzeuges (optional nur durch den Nutzer hinterlegbar), Daten zum Fahrer (optional nur durch den Nutzer hinterlegbar), Standortdaten des Fahrzeuges zur GPS-Ortung, Streckenverfolgung sowie weitere Fahrzeugdaten zur intelligenten Routenplanung, Kraftstoffverbrauchsmanagement, Auslesen der Motordaten/Fehlern zur optimierten Fuhrparkwartung
2.3	Folgende Daten von **betroffenen Personen** werden durch den Auftrag-nehmer verarbeitet	☒ Beschäftigte (z.B. Mitarbeiter/Innen, Praktikanten, Auszubildende) ☒ Sonstiges*: bitte konkret angeben*: Geschäftskunden des Smart Mobility Dienstes
2.4	Folgende Vorgaben für die **Datenlöschung** werden berücksichtigt	Die Auftraggeber-Daten (insbesondere Bestands-/ Verkehrs-/ Inhalts- und Mitarbeiterdaten) sind zu löschen, wenn sie für die Durchführung des Auftrags nicht mehr erforderlich sind, es sei denn es liegt eine abweichende Weisung des Auftraggebers vor. Die Löschung von Verkehrsdaten hat entsprechend den rechtlichen Anforderungen aus dem “Leitfaden des BfDI und der BNetzA für eine datenschutzgerechte Speicherung von Verkehrsdaten” zu erfolgen.

Anlage 3: Beschreibung der technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO

	Anforderung	GEOTAB INC.
3.1	**Ergebnis der Risikobewertung** Die Bewertung des jeweiligen Risikos erfolgt anhand der Maßstäbe der DSGVO. (Für Telefónica ist dafür eine Schutzbedarfsanalyse mit dem Bereich Corporate Security durchzuführen, bevor die Anlage ab Ziffer 2 ausgefüllt wird.)	Die Vertragspartei hat die datenschutzrechtlichen Risiken für die in ihrem Aufgabenbereich durchgeführte Datenverarbeitung wie folgt definiert: **Risiko bzgl. Vertraulichkeit:** Daten dürfen lediglich von autorisierten Benutzern gelesen bzw. modifiziert werden. Dies gilt sowohl beim Zugriff auf gespeicherte Daten wie auch während der Datenübertragung. ☐ hoch ☒ normal ☐ ausgeschlossen **Risiko bzgl. Integrität:** Daten dürfen nicht unbemerkt und unautorisiert verändert werden. Alle etwaigen Änderungen müssen nachvollziehbar sein (Daten- & Systemintegrität). ☒ hoch ☐ normal ☐ ausgeschlossen **Risiko bzgl. Verfügbarkeit:** Der Zugriff auf die Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet werden; Verhinderung von Systemausfällen. ☐ hoch ☒ normal ☐ ausgeschlossen **Risiko bzgl. Belastbarkeit:** Toleranz und Ausgleichsfähigkeit eines Systems gegen Störungen/Angriffe von innen und außen (Widerstandsfähigkeit, Ausfallsicherheit). ☐ hoch ☒ normal ☐ ausgeschlossen

3.2	Liegt ein **Sicherheitskonzept** gemäß Art. 32 DSGVO vor?	☒ Ja (*bitte Sicherheitskonzept als weitere Anlage diesem Vertrag beifügen*) Beachtung von internationalen Standards: ☒ Zertifizierung nach ISO 27001 Weitere Maßnahmen ☒ Durchgeführte Sicherheitsmaßnahmen sind immer auf dem Stand der Technik gehalten
3.3	Sind Maßnahmen zur **Pseudonymisierung** personenbezogener Daten ergriffen worden?	☒ Nein, weil *(bitte begründen)*: Es liegt in der Verantwortung des Kunden der das Portal nutzt, die Daten von Nutzern zu pseudonymisieren.

		Die MyGeotab-Lösung benötigt keine personenbezogenen Daten.
3.4	Sind Maßnahmen zur räumlichen **Zutrittskontrolle** ergriffen worden, die es Unbefugten verwehren, sich den Systemen, Datenverarbeitungsanlagen oder Verfahren physisch zu nähern, mit denen personenbezogene Daten verarbeitet werden?	☒ Ja Maßnahmen: ☒ Zutrittskontrollsystem, z.B. Ausweisleser (Magnet-/Chipkarten) ☒ Werkschutz/ Pförtner
3.5	Sind Maßnahmen zur **Zugangskontrolle** ergriffen worden, die verhindern, dass ein Zugang durch Unbefugte auf Datenverarbeitungssysteme verhindert wird?	☒ Ja Maßnahmen: ☒ Benutzer haben einen eindeutigen persönlichen Bezeichner ☒ Getrennte Benutzerkennungen für priviligierte Berechtigungen ☒ Benutzerkennungen werden, wenn die Benutzer das Unternehmen verlassen haben, gelöscht oder deaktiviert ☒ Passwörter werden grundsätzlich nicht im Klartext gespeichert oder unverschlüsselt übertragen ☒ Sichere Passwortverfahren ☒ Sichere Erzeugung und Übermittlung von Initial- und Reset-Passwörtern ☒ Single-Sign-On für die wesentlichen IT-Systeme ☒ Zwei-Faktor-Authentifizierung ☒ Automatische Sperrung der Clients nach Zeitablauf ohne Useraktivität (bspw. passwortgeschützter Bildschirmschoner) ☒ Dokumentation administrativer Passwörter in gesicherten Passwortsafes ☒ sichere Verwaltung und Verwendung von digitalem Schlüsselmaterial (z.Bsp.: digitale Zertifikate, Token, etc.) ☒ Regelmäßige Softwareaktualisierung / Patching (Patchmanagement) ☒ Regelmäßige Schwachstellenscans ☒ Netzwerksegmentierung ☒ Firewall, IDS/IPS
3.6	Sind Maßnahmen zur **Zugriffskontrolle** ergriffen worden, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht	☒ Ja Maßnahmen: ☒ Inventarisierung der für den Auftrag relevanten Unternehmenswerte ☒ Angemessene Berechtigungskonzepte ☒ Verantwortlichkeiten ☒ Aufgabenbezogene Profile und Rollen ☒ Benutzermanagementprozess inkl. Genehmigungsverfahren ☒ Regelmäßige Prüfung der Aktualität von Zugriffsrechten (Rezertifizierung) ☒ Sonstiges: *bitte im Einzelnen aufführen*: Audit-Logs sind in der MyGeotab Applikation verfügbar

	unbefugt gelesen, kopiert, verändert oder entfernt werden können?	
3.7	Sind Maßnahmen zur **Weitergabekontrolle** ergriffen worden, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist?	☒ Ja Maßnahmen: ☒ SSL-/TLS-Verschlüsselung ☒ Verwaltung kryptographischer Schlüssel ☒ Diebstahlschutz für mobile Geräte ☒ Regelungen zur Datenträgervernichtung, etc.
3.8	Sind Maßnahmen zur **Eingabekontrolle** ergriffen worden, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind?	☒ Ja Maßnahmen: ☒ Berechtigungskonzepte vorhanden, inkl.: ☒ Funktionale Verantwortlichkeiten ☒ Need-to-know Prinzip (allgemein) ☒ Angemessene Funktionstrennung ☒ Sonstiges*: bitte im Einzelnen aufführen*: Audit-Logs
3.9	Sind Maßnahmen zur **Auftragskontrolle** ergriffen worden, die sicherstellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können?	☒ Ja Maßnahmen: ☒ Schulungen aller zugriffsberechtigten Mitarbeiter ☒ Regelmäßig stattfindende Nachschulungen ☒ Betriebshandbücher für den sicheren Betrieb ☒ Regelmäßige Datenschutzaudits des betrieblichen Datenschutzbeauftragten ☒ Prüfungsplanung für interne und externe Audits ☒ Nutzung eines risikoorientierten Auditansatzes ☒ Monitoring & Reporting über neu Identifizierte Risiken / Schwachstellen

		☒ IT Change Management Prozess ☒ Trennung von Entwicklungs- und Produktivsystemen inkl. geregeltem Transportprozess (production take over) ☒ Durchführung von Funktions- und Benutzerakzeptanztests ☒ Genehmigungs- und Freigabeverfahren ☒ Regeln für die sichere Entwicklung von Software und Systemen sind festgelegt und werden angewandt ☒ Zugriff auf Source-Code / Customizing geschützt (need-to-know Prinzip) ☒ Sonstiges*: bitte im Einzelnen aufführen*: Geotab End User Agreement, das vor der Nutzung durch den Kunden akzeptiert werden muss
3.10	Sind Maßnahmen zur **Verfügbarkeitskontrolle** ergriffen worden, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind bzw. zügig wiederhergestellt werden können?	☒ Ja Maßnahmen: ☒ Business Continuity Strategie und Management, ☒ Service Level Agreements (SLAs) mit Dienstleistern ☒ Backup Verfahren ☒ Sichere Aufbewahrung für Backups (z.B. Safe, getrennter Brandabschnitt) ☒ Viren-/Schadcodeschutz ☒ Redundante Komponenten (z.B. Spiegeln von Festplatten) ☒ Redundante Versorgung (z.B. Internet, Telefon, Strom) ☒ Geeignete Archivierungsräumlichkeiten ☒ Schutz der relevanten Infrastruktur gegen Defekte durch äußere Einflüsse ☒ Pläne für Ausfall / Notfall / Wiederanlauf etc. (einzelner Komponenten) ☒ Sonstiges*: bitte im Einzelnen aufführen*: Die Business Continuity und Data Recovery Pläne von Geotab sind öffentlich verfügbar
3.11	Sind Maßnahmen zur Einhaltung des **Trennungsgebots** ergriffen worden, die gewährleisten, dass Daten, die zu unterschiedlichen Zwecken erhoben werden, getrennt verarbeitet (z.B. gelöscht) werden können.	☒ Ja Maßnahmen: ☒ Getrennte Systeme ☒ Getrennte Datenbanken
3.12	Sind Maßnahmen und Verantwortlichkeiten für den **Umgang mit Informations-sicherheitsvorfällen und Krisensituationen** definiert worden?	☒ Ja Maßnahmen: ☒ Managementprozess für Security Incidents ☒ Managementprozess für datenschutzrelevante Incidents ☒ Definition der Sicherheitsanforderungen in Krisensituation / im Notfall ☒ Übergreifender Notfallplan inkl. regelmäßiger Aktualisierung ☒ Regelmäßige Durchführung und Dokumentation von Notfalltests

3.13	Sind Maßnahmen für **Logging** in den relevanten Bereichen ergriffen worden?	☒ Ja Maßnahmen: ☒ Nutzung von Sicherheits-/Protokollierungssoftware ☒ Die Log-Systeme beziehen sich auf eine einzige Zeitquelle ☒ Verarbeitung der Daten in Übereinstimmung mit geltenden gesetzlichen Bestimmungen für die Informationssicherheit ☒ Logs sind gegen unberechtigten Zugriff geschützt (Vertraulichkeit) ☒ Logs sind vor unberechtigter Veränderung geschützt (Integrität) ☒ Logs sind vor Verlust geschützt (Verfügbarkeit) **Weitergabekontrolle** ☒ Logging der Datenweitergabe und regelmäßige Überprüfung der Logfiles **Verfügbarkeitskontrolle** ☒ Logging der Verfügbarkeit ☒ Regelmäßige Überwachung der Systeme und Logfiles **Zutrittskontrolle** ☒ Logging der Zutritte ☒ Regelmäßiges Monitoring von Zutritten ☒ Auswertung der Logs zur weiteren Verwendung **Zugangskontrolle** ☒ Logging der Zugänge ☒ Regelmäßiges Monitoring von Zugängen: *bitte spezifizieren, welche Parameter regelmäßig überwacht werden:* _____ ☒ Auswertung der Logs zur weiteren Verwendung
3.14	Ist Mitarbeitern erlaubt aus dem **Homeoffice** zu arbeiten? Sind Maßnahmen zur Arbeit im Homeoffice bzw. für Telearbeit ergriffen worden?	☒ Ja ☒ Homeoffice Richtlinie / Richtlinie mobiles Arbeiten ☒ Privatnutzung geschäftlicher Ausstattung erlaubt ☒ Endgerät ist nach dem Stand der Technik geschützt ☒ Verschlüsselung der Remoteverbindung

Anlage 4: Angaben zu Subunternehmern des Auftragnehmers

Zur Erfüllung des Vertrages/Hauptvertrages werden bzw. wurden Subunternehmer mit der Erbringung eines Teils der Dienstleistung beauftragt:

Angabe des Subunternehmers/ Konzernunternehmen	**Ort der Speicherung/ des bestimmungsgemäßen Zugriffs auf Auftraggeber-Daten** *[falls abweichend von Anschrift des Subunternehmers]*	**Erfolgt eine Datenverarbeitung oder ein Zugang zu Auftraggeber-Daten aus Drittstaaten (außerhalb der EU/ EWR)?** *[z.B. durch Beauftragung von weiteren Dienstleistern durch den beauftragten Subunternehmer]*	**Gegenstand der Unterbeauftragung und verarbeitete Kategorien von Auftraggeber-Daten**	**Abgeschlossener ADV-Vertrag / EU-Standardvertrag** **Der zwischen Auftragnehmer und Subunternehmer abgeschlossene ADV-Vertrag nach Art. 28 DS-GVO/ EU Model Clauses ist vor dem Abschluss dieses Vertrags auf Anforderung vorzulegen.**
Name/ Firma: GEOTAB INC. Anschrift: 2440 Winston Park Drive Oakville, Ontario L6H 7V2, Canada Datenschutzbeauftragter mit Kontaktdaten: Geotab Inc. Attn: Chief Privacy Officer 2440 Winston Park Dr. Oakville, Ontario, Canada L6H 7V2 legal@geotab.com	Anschrift: St. Ghislain, Belgium (europe-west1)	☐Ja, *[bitte spezifizieren, welcher Dienstleister, Anschrift/ Ort des möglichen Datenzugangs, Art der Tätigkeit und Datenarten]* ☒Nein, ein Zugang zu Auftraggeber-Daten ist ausgeschlossen	Betrieb der Telematik Cloud Plattform	☒Ja, liegt vor ☐Nein