PTV GROUP

the mind of movement

Auftragsverarbeitung

PTV Route Optimiser CL

PTV Planung Transport Verkehr AG, Hauptsitz / Headquarters: Karlsruhe,
Vorstand / Board of Directors: Christian U. Haas (CEO), Klaus Lechner, Dr. Peter Overmann
Vorsitzender des Aufsichtsrates / Chairman of the Board: Philipp von Hagen,
Handelsregister / Companies' Register (HRB-Nr): 109262, Ust-ID-Nr. DE 812 666 053,
Amtsgericht / District Court: Mannheim.

Inhalt

Begriffsbestimmungen 4

Gegenstand, Dauer und Konkretisierung des Auftrags..... 4

Technisch-organisatorische Schutzmaßnahmen des Auftragsverarbeiters..... 6

Weisungsbefugnis des Auftragsgebers 6

Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters 7

Einsatz von Subauftragnehmern..... 8

Kontrollrechte des Auftraggebers..... 9

Mitteilung bei Verstößen des Auftragsverarbeiters 9

Anfragen und Rechte Betroffener 10

Löschung und Rückgabe von personenbezogenen Daten 10

Haftung..... 11

Schlussbestimmungen 11

Anlage 1 - Allgemeine technische und organisatorische Maßnahmen 13

Anlage 2 - Weisungsberechtigte Personen 16

Anlage 3 - Genehmigte Subauftragnehmer 17

Kurztitel	Auftragsverarbeitung
Version der Vertragsvorlage:	1.1.0 vom 01.11.2019

Vereinbarung zwischen

Auftraggeber (Verantwortlicher):

Firma
Straße
PLZ Ort, Land

- Nachfolgend: Verantwortlicher oder Auftraggeber-

Ansprechpartner:

Vorname Name
Tel.: Telefon (Geschäftlich)
E-Mail: E-Mail (Geschäftlich)

und

Auftragnehmer (Auftragsverarbeiter):

PTV Planung Transport Verkehr AG
Haid-und-Neu-Straße 15
76131 Karlsruhe, Germany

- Nachfolgend: Auftragsverarbeiter -

Ansprechpartner:

[genesisWorld:UnterschriftName]
Tel.: +49 721 9651- [genesisWorld:Durchwahl]
E-Mail: [genesisWorld:EMail]

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der Auftragsverarbeitung gem. Art.28 Datenschutzgrundverordnung (DSGVO) ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragsverarbeiters oder durch den Auftragsverarbeiter Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

Begriffsbestimmungen

(1) Verantwortlicher ist gem. Art. 4 Abs. 7 DS-GVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(4) Besonders schutzbedürftige personenbezogene Daten sind personenbezogenen Daten gem. Art. 9 DS-GVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DS-GVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln sowie genetische Daten gem. Art. 4 Abs. 13 DS-GVO, biometrischen Daten gem. Art. 4 Abs. 14 DS-GVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DS-GVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(5) Verarbeitung ist gem. Art. 4 Abs. 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Gegenstand, Dauer und Konkretisierung des Auftrags

Gegenstand des Auftrags

Verarbeitung im Rahmen von PTV Software (hier: PTV Routeoptimiser CL)

Dauer des Auftrags

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Nutzungsvereinbarung.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.
Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.

Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten / -kategorien (Aufzählung / Beschreibung der Datenkategorien)

- ☒ Personenstammdaten
- ☒ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☒ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☐ ...

Kreis der Betroffenen

Der Kreis, der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst (Aufzählung / Beschreibung der betroffenen Personenkategorien):

- ☒ Kunden
- ☒ Interessenten
- ☒ Abonnenten
- ☒ Beschäftigte
- ☒ Lieferanten
- ☐ Handelsvertreter
- ☒ Ansprechpartner
- ☐ …

Technisch-organisatorische Schutzmaßnahmen des Auftragsverarbeiters

(1) Der Auftragsverarbeiter hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragsverarbeiter hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

Weisungsbefugnis des Auftragsgebers

(1) Der Auftragsverarbeiter darf Daten nur im Rahmen des zugrundeliegenden Vertrags und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragsverarbeiter durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Mündliche Weisungen bestätigt der Auftraggeber unverzüglich mindestens in Textform. Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt.

(3) Die weisungsberechtigten Personen ergeben sich aus Anlage 2. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

(4) Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen,

löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(5) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragsverarbeiter sicherzustellen.

(6) Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragsverarbeiter darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt.
Als Datenschutzbeauftragter ist beim Auftragsverarbeiter
Herr Thomas Heimhalt,
DATENSCHUTZ *perfect* GbR, Karlsruhe, Deutschland
datenschutz@ptvgroup.com
bestellt.
Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

b) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragsverarbeiter setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

d) Der Auftraggeber und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragsverarbeiter ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.

g) Der Auftragsverarbeiter kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

Einsatz von Subauftragnehmern

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragsverarbeiter z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragsverarbeiter darf Subauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) Der Auftraggeber stimmt der Beauftragung der in Anlage 3 aufgeführten Subauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO;

b) Die Auslagerung auf weitere Subauftragnehmer oder der Wechsel des bestehenden Subauftragnehmers sind zulässig, soweit:
   - der Auftragsverarbeiter eine solche Auslagerung auf Subauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und

- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragsverarbeiter schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Subauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Subauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragsverarbeiter die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Subauftragnehmer ist nicht gestattet;

Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragsverarbeiter Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragsverarbeiter stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DS-GVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragsverarbeiter einen Vergütungsanspruch geltend machen.

Mitteilung bei Verstößen des Auftragsverarbeiters

(1) Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen

Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden;

c) die Verpflichtung ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DS-GVO enthält, zu führen. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen;

d) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;

e) die Unterstützung des Auftraggebers für dessen Verfahrensverzeichnis und Datenschutz-Folgenabschätzung;

f) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Sollten die Daten des Auftraggebers beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragsverarbeiter wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DS-GVO liegen.

(3) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragsverarbeiters zurückzuführen sind, kann der Auftragsverarbeiter eine Vergütung beanspruchen.

Anfragen und Rechte Betroffener

(1) Der Auftragsverarbeiter unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DS-GVO.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragsverarbeiter geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der 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 erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Haftung

(1) Auftraggeber und Auftragsverarbeiter haften gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragsverarbeiter i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Karlsruhe.

Anlagen:

Anlage 1 – Technische und organisatorische Maßnahmen des Auftragsverarbeiters

Anlage 2 – Weisungsberechtigte Personen

Anlage 3 – Genehmigte Subauftragnehmer

Karlsruhe, den _____	Ort, den _____
PTV Planung Transport Verkehr AG	Firma
_____	_____
Vorname, Nachname (in Druckschrift) Funktion	Vorname, Nachname Funktion
Karlsruhe, den _____	Ort, den _____
PTV Planung Transport Verkehr AG	Firma
_____	_____
Vorname, Nachname (in Druckschrift) Funktion	Vorname, Nachname Funktion

Anlage 1 - Allgemeine technische und organisatorische Maßnahmen

Zur Sicherung der Anforderungen an die Sicherheit der Datenverarbeitung werden gem. Art. 32 DS-GVO technische und organisatorische Maßnahmen ergriffen.

Dabei sollen solche Maßnahmen getroffen werden, die nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.

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

Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen

Auszug aus den bei PTV Planung Transport Verkehr AG getroffenen Maßnahmen:

- Wachdienst mit Verbindung zur Polizei
- Videoüberwachung des nicht-öffentlichen Bereichs (außen) und teilweise innen
- Gebäude-Zugang mit Chip-Key
- Besetzter Empfang während der Öffnungszeiten
- Schließsystem für sensible Aufgabenbereiche / Räume
- Zugang in den Serverräumen nur für Berechtigte, besonderes Schließsystem

Zugangskontrolle

Keine unbefugte Systembenutzung

Auszug aus den bei PTV Planung Transport Verkehr AG getroffenen Maßnahmen:

- User-ID-Abfrage mit Passwort
- Passwortkonvention vorhanden, ausgestaltet nach aktuellen Empfehlungen
- Zeitliche Begrenzung der Passwortgültigkeit
- Passwortgenerationen
- Verschlüsselung der Notebook-Festplatten

Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen

Auszug aus den bei PTV Planung Transport Verkehr AG getroffenen Maßnahmen:

- Berechtigungs- und Administrationskonzept vorhanden
- Benutzerrollen- / Gruppenkonzept
- Zugriffsprüfung per Protokoll
- Vorgabe der Verwendung von Pausenschaltung (Bildschirmschoner)
- Passwortgeschützter Bildschirmschoner, zeitgesteuerte Aktivierung

Trennungskontrolle:

Getrennte Verarbeitung von Daten, die unterschiedlichen Zwecken dienen

Auszug aus den bei PTV Planung Transport Verkehr AG getroffenen Maßnahmen:

- Verarbeitung der Unternehmensdaten getrennt von den jeweiligen Kundendaten

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

Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport

Auszug aus den bei PTV Planung Transport Verkehr AG getroffenen Maßnahmen:

- VPN-Verwendung
- Verschlüsselung der Notebook-Festplatten

Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Systeme eingegeben, verändert oder entfernt worden sind

Auszug aus den bei PTV Planung Transport Verkehr AG getroffenen Maßnahmen:

- Protokollierung aller Eingaben im zentralen CRM und den sonstigen relevanten Programmen

3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b, c EU-DSGVO)

Verfügbarkeitskontrolle, Rasche Wiederherstellbarkeit

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust

Auszug aus den bei PTV Planung Transport Verkehr AG getroffenen Maßnahmen:

- Tägliche bis jährliche Sicherung, Zusatzsicherungen und getestete Rücksicherungen
- RAID-Festplattenspeicher
- Getestetes Notfallkonzept
- Virenscanner und mehrstufige Firewalls
- Serverraum-Klimatisierung, USV, CO2-Feuerlöscher, Brandmelder
- Regelmäßige Software-Updates
- Aufbewahrung der Sicherungen in speziell geeigneten Datentresoren.

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

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

- Unsere Mitarbeiter werden auf die Einhaltung des Datenschutzes verpflichtet.

Datenschutz-Management

Gemeinsam mit dem externen Datenschutzbeauftragten wird ein Datenschutzmanagementsystem (DSMS) geführt, in dem alle Maßnahmen, Verfahren, Tätigkeiten etc. abgebildet werden. Das DSMS beinhaltet die wichtigsten datenschutzrechtlichen Vorgaben und eine umfassende Struktur zur Abbildung der Datenschutzmaßnahmen. Das DSMS wird laufend gepflegt und aktualisiert.

Incident-Response-Management

Ein organisatorischer und technischer Prozess zum Umgang mit Sicherheitsvorfällen (incidents) ist definiert und implementiert. Hierüber wird auch eine einheitliche Reaktion sowie ein prozessualisierter Umgang mit erkannten und vermuteten Sicherheitsvorfällen/Störungen sichergestellt. Ebenfalls erfolgt im Rahmen dessen eine einheitliche Nachbereitung und Kontrolle im Sinne eines kontinuierlichen Verbesserungsprozesses.

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 EU-DSGVO)

Grundsätzlich werden nur Daten erhoben und verarbeitet, die für die Geschäftszwecke zweckmäßig und erforderlich sind. Verfahren der automatisierten Datenerfassung und -verarbeitung sind so gestaltet, dass nur die erforderlichen Daten erhoben werden.

Anlage 2 - Weisungsberechtigte Personen

Weisungsberechtigte Personen des Auftraggebers sind:

.....

(Vorname, Name, Organisationseinheit, Telefon)

Weisungsempfänger beim Auftragsverarbeiter sind:

.....

(Vorname, Name, Organisationseinheit, Telefon)
Sowie Support PTV Routeoptimiser

Für Weisung zu nutzende Kommunikationskanäle sind:

.....

(genaue postalische Adresse/ E-Mail/ Telefonnummer)

Anlage 3 - Genehmigte Subauftragnehmer

Die nachfolgenden Unternehmen sind genehmigte Subauftragnehmer im Sinne des Abschnitts 6 Abs.2 lit.b:

Firma Subauftragnehmer*	Anschrift/Land	Leistung
Microsoft Ireland Operations Ltd	Carmenhall Road, Sandyford, Dublin 18, Irland	Betrieb des Dienstes in der Cloud
PTV UK Holding Ltd.	No 5 Centre Court, Vine Lane, Halesowen, West Midlands, England, B63 3EB	Software Entwicklung
PTV Distribution Planning Software Ltd.	No 5 Centre Court, Vine Lane, Halesowen, West Midlands, England, B63 3EB	Support-Leistungen

*: Unternehmen mit Namen, Rechtsform, Kontaktdaten, Anschrift