Vertrag über Datenverarbeitung im Auftrag

Datum: 01.10.2018

Präambel

Der Kunde (nachfolgend: Verantwortlicher) beauftragt Audatex AUTOonline (nachfolgend: Auftragsverarbeiter) mit der Verarbeitung von Personendaten gemäß den nachfolgenden Bestimmungen.

Der Auftrag umfasst zwei unterschiedliche Prozesse, welche in den Ziffern 2 bis 5 jeweils mit a) und b) näher erläutert und unterschieden werden. Fehlt eine solche Unterscheidung, gelten die Regelungen für beide Prozesse gleichermaßen.

1. Dauer des Auftrags

a) Der Auftrag über die Datenverarbeitung ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von drei Monaten zum Quartalsende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

b) Ohne vorherige Kündigung gemäß vorstehender Ziffer 1. a) endet der Auftrag mit dem Ende der Laufzeit des Vertrages des Verantwortlichen mit dem Auftragsverarbeiter über die Nutzung der vereinbarten Plattform (z.B. AudaNet oder Restwertbörse).

c) Der Auftragsverarbeiter kann diesen Auftrag jederzeit ändern. Änderungen (bzw. ein neuer Auftragsverarbeitungsvertrag) werden vom Auftragsverarbeiter mindestens 14 Tagen vor dem vorgeschlagenen Zeitpunkt ihres Wirksamwerdens in Textform übermittelt. Die Zustimmung des Verantwortlichen gilt als erteilt, wenn er seine Ablehnung nicht vor dem vorgeschlagenen Zeitpunkt des Wirksamwerdens schriftlich angezeigt hat.

2. Umfang, Art und Zweck der Auftragsdatenverarbeitung

Die Verarbeitung und Nutzung der Daten findet derzeit ausschließlich im Gebiet der Bundesrepublik Deutschland, der Schweiz, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Eine Übermittlung von Daten in sonstige Staaten außerhalb des EU-/EWR-Raums ist nicht vorgesehen, aber grundsätzlich möglich, wenn das erforderliche EU-Datenschutzniveau aufrechterhalten wird.

Der Auftragsverarbeiter ist berechtigt, die Arbeitsergebnisse in anonymisierter Form für eigene Zwecke, einschließlich für statistische Auswertungen und die Verbesserung der Dienstleistungen, zu nutzen.

a) Der Verantwortliche übermittelt dem Auftragsverarbeiter zu jedem Prüfauftrag strukturierte Auftragsdaten und Binäranhänge. Die Beauftragung erfolgt, je nach Art der Beauftragung, elektronisch über eine abgesicherte VPN-Verbindung oder eine https-Verbindung mit einer Verschlüsselungstiefe von 128 Bit. Die strukturierten Auftragsdaten enthalten Ordnungsmerkmale des Verantwortlichen (z. B. die Schadennummer) und technische Fahrzeugdaten. Außerdem erhält der Auftragsverarbeiter mit jedem Auftrag als Binäranhang Fahrzeugfotos und ggf. vorliegende Fremdgutachten.

Vor Einstellung in die Restwertbörse werden die vom Verantwortlichen übermittelten Daten anonymisiert, das bedeutet, dass jeder herstellbare Personenbezug durch Schwärzung bzw. Nichtveröffentlichung (Löschung) unkenntlich gemacht wird (z. B. Schwärzung von Nummernschildern und Gesichtern, Nichtveröffentlichung von Gutachternamen etc.).

Sobald nicht mehr für die Erfüllung des Übermittlungszwecks erforderlich, spätestens aber vier Wochen nach Übermittlung, werden die personenbezogenen Daten durch den Auftragsverarbeiter automatisiert gelöscht.

Nach Ablauf der Gebotsfristen übermittelt der Auftragsverarbeiter dem Verantwortlichen die im Rahmen der Auktionen abgegebenen Gebote und zusätzlich die Namen, Adressen, sowie sonstige Kontaktdaten der jeweiligen Bieter, z. B. E-Mail-Adressen, Telefon- bzw. Faxnummern, um die Möglichkeit zum späteren Vertragsschluss zu eröffnen.

b) Der Verantwortliche kann über die Plattform AudaNet die gesamte Kommunikation mit den Beteiligten abwickeln, von der Auftragserteilung über die Rechnungsstellung bis zur Abrechnung.

Abhängig von den konkreten Beteiligten und den nachfolgend aufgeführten, vom Verantwortlichen teilweise optional buchbaren Komponenten, findet ein Umgang mit personenbezogenen Daten im folgenden Umfang statt:

i. AudaNet
AudaNet ist eine elektronische Kommunikationsplattform für den Informationsaustausch zwischen Werkstätten, Versicherungen, Sachverständigen und weiteren Dienstleistern. Alle Daten werden in der Regel nur noch einmal erfasst und liegen dann strukturiert und GDV-konform vor. Die Datenübermittlung zwischen Verantwortlichen, Versicherung, Werkstatt oder Sachverständigen und sonstigen Dienstleistern erfolgt elektronisch. AudaNet ist in der Regel die Kommunikationsschnittstelle der Werkstätten und Sachverständigen zu den Versicherern; es wird dabei sichergestellt, dass die Informationen bei dem gewünschten Empfänger in dem Format ankommen, wie dieser sie braucht, um sie direkt weiterverarbeiten zu können.

ii. Werkstatt-Kommunikation
Bei der Werkstatt-Kommunikation können seitens der Versicherung Aufträge an eine Reparaturwerkstatt, die ebenfalls an AudaNet teilnimmt, in strukturierter Form versendet werden. Diese Daten können in das Managementsystem der Werkstatt eingelesen und dort weiter bearbeitet werden. Von der Werkstatt kann ein erstellter Kostenvoranschlag inkl. Bilder und beliebiger Anlagen dann über AudaNet an die Versicherung als Auftraggeber zurückgesendet werden. Auch die Reparaturkosten-Übernahmeerklärungen und die Reparaturfreigabe, die auf der Versicherungsseite entsprechend vorbelegt ist, kann über den gleichen elektronischen Weg an die Werkstatt gesendet werden. Der Prozess kann auch auf Werkstattseite mit der Schadenerfassung und der Erstellung eines Kostenvoranschlags beginnen. Eine Auftragserteilung durch den Versicherer kann ebenfalls elektronisch erfolgen.

iii. **Sachverständigen-Kommunikation**
In der Sachverständigen-Kommunikation können Versicherungen Aufträge an Sachverständige in strukturierter Form versenden. Dabei ist optional eine automatisierte Zuordnung der Aufträge an die Sachverständigen oder einen Sachverständigenpool nach Kriterien wie Postleitzahl und Qualifikation möglich. Der Sachverständige erhält optional eine automatische E-Mail-Benachrichtigung über die in seinen elektronischen Postkorb eingestellten Aufträge. Die Auftragsdaten können ins Managementsystem des Sachverständigen eingelesen werden und stehen dem Sachverständigen damit direkt zur Verfügung. Über den gleichen Weg kann der Sachverständige auch das fertig erstellte Gutachten inkl. Bilder und beliebiger Anlagen an die Versicherung zurücksenden.
Der Prozess kann auch auf Sachverständigenseite mit der Schadenerfassung und der Erstellung einer Kalkulation oder Fahrzeugbewertung beginnen.

iv. **Versicherer-Kommunikation**
Über AudaNet können Versicherungsunternehmen, Sachverständige, Werkstätten und weitere Dienstleister elektronisch miteinander kommunizieren und Daten austauschen. Darüber hinaus kann eine automatische Werkstatt- oder Sachverständigenbeauftragung – ggf. nach vorgegebenen Regeln –, ebenso wie eine Versendung von kompletten Kostenvoranschlägen und Gutachten, elektronischen Reparaturkosten-Übernahmeerklärungen, zentrale Datenspeicherung, Management Informationen etc. erfolgen.

v. **AudaPad Web**
AudaPad Web ist eine Internetlösung für die Schadenkalkulation. Über die Anbindung an die Kommunikationsplattform AudaNet können die Unterlagen direkt auf elektronischem Wege zwischen den Beteiligten versendet werden.

vi. **APWS**
APWS ist eine für Werkstätten optimierte Version von AudaPad Web, bietet dessen Funktionen, speichert zu einem einzelnen Vorgang aber die folgenden Daten nicht mehr nur lokal, sondern auch online auf den AudaNet-Servern ab: Fahrzeugdaten, Preisfaktoren der Werkstatt sowie Stammdaten, welche sich allesamt auf einen einzelnen Vorgang beziehen.

vii. **AudaNet RulesCheck**
Die Komponente RulesCheck ermöglicht die inhaltliche elektronische Prüfung einer strukturierten Kfz-Schadenkalkulation nach individuell durch den Verantwortlichen festgelegten Regeln. Hierbei werden die erfassten Schadendaten (Ersatzteile, Arbeitswerte und sonstige Positionen) sowie eine statistische Historie bei vergleichbaren Schäden (Plausibilität) einbezogen.

viii. **C@risma**
C@risma ist eine Managementlösung für den Karosserie- und Lackierfachbetrieb mit Anbindung an die Kommunikationsplattform AudaNet. Dabei können sämtliche Arbeitsprozesse und Ablaufpläne dargestellt und optimiert werden. Fahrzeugdaten, Preisfaktoren der Werkstatt sowie Stammdaten, die sich allesamt auf einen einzelnen Vorgang beziehen, werden dazu nicht nur lokal, sondern auch online auf AudaNet-Servern gespeichert. C@risma bietet u. a. folgende Funktionen: Schadenkalkulation und -erfassung, Kundendaten- und Dokumentenverwaltung, Mahnwesen, Personal- und Auftragszeiterfassung, Schnittstellen zur Finanzbuchhaltung sowie Customer Relationship Management. Diese Daten werden generell nur lokal gespeichert, sofern sie nicht fallbezogen verwendet werden.

ix. **AudaNet GlaserStory**
Die GlaserStory ist eine webbasierte Applikation zur kosten- und ablaufoptimierten Abwicklung von Glasschäden zwischen den Fachbetrieben und Versicherern. Die GlaserStory überprüft die Glasrechnungen schon während der Erstellung auf die von Versicherern und Fachbetrieben festgelegten Standards und leitet sie elektronisch an die entsprechende Versicherungsgesellschaft weiter. Der Versicherer erhält somit eine auf Herstellerbasis bearbeitete Glasschadenkalkulation, die den eigenen Standards bei der Regulierung entspricht. GlaserStory ermöglicht Versicherungen und Fachbetrieben den ständigen elektronischen Kontakt untereinander.

x. **AudaGlass**
Die Internet-Applikation AudaGlass ermöglicht es Sachverständigen und Versicherern, Glas-Rechnungen – basierend auf Herstellerdaten – auf Genauigkeit zu prüfen. Auch Werkstätten und Autoglaser können die Applikation AudaGlass zur Ermittlung grundlegender Rechnungsdaten und von Kostenvoranschlägen verwenden.

xi. **AudaFusionWeb**
Die Internet-Applikation AudaFusionWeb ist eine Bürokommunikationssoftware für Sachverständige mit Anbindung an die Kommunikationsplattform AudaNet. Es ermöglicht die Erstellung von Kfz-Gutachten inkl. Verwaltung von Kundenstammdaten, Fahrzeugidentifikation, Fahrzeugbewertung, Restwertermittlung, Schadenerfassung und -kalkulation, (halbautomatisierter) Gutachten- und Rechnungserstellung, Buchhaltungsfunktion (mit DATEV-Schnittstelle) und Anbindung an GDV. Alle Daten werden online auf den AudaNet-Servern gespeichert

xii. **Fernwartung**
Im Bedarfsfall greift der Auftragsverarbeiter auf Datenverarbeitungssysteme des Verantwortlichen zum Zweck der Fernwartung zu. Ein solcher Zugriff ist nur nach individueller und einzelfallbezogener Freischaltung durch den Verantwortlichen möglich und zulässig. Dem Verantwortlichen steht während des gesamten Zugriffs eine Aufsichtsmöglichkeit über die durchgeführten Wartungsarbeiten zur Verfügung.

3. Art der Daten

a) Die Auftragsdatenverarbeitung umfasst folgende Datenkategorien:

- Personenstammdaten
- Versicherungsvertragsdaten
- Abrechnungs- und Zahlungsdaten
- Schadendaten
- Fotos

Übersicht der vom Auftragsverarbeiter zu verwendenden Daten im Detail:

- <u>Verkäuferdaten:</u>

- ID, E-Mail-Adresse, Vor- und Nachname

- Aktenzeichen
- Standort des Kfz:
  - Länderkennzeichen, Postleitzahl
- Allgemeine und interne Bemerkungen
- Interne Kennzeichen:
  - Erfassungsart, Weiterleitungskennzeichen, Urheberrechtsschutz
- FIN (Fahrzeug-Identifikationsnummer)
- Daten aus Sachverständigengutachten:
  - Kontaktdaten von Sachverständigenfirma, besichtigenden Sachverständigen, Versicherungsnehmer, Anspruchsteller / Kfz-Halter, Rechtsanwälte, Reparaturfirma
  - Amtl. Kennzeichen von Halter und Unfallgegner
  - Besichtigungsdatum, -zeit und -ort
  - Gutachtennummer, -erstellungsdatum und -erstellungsort
  - Schadentag, -zeit und -ort
  - Reparatur-/Materialkosten, Wiederbeschaffungswert, Restwert
  - Unfallfotos
  - Technische Daten des Kfz (Modell, Baujahr, Hubraum etc.)
  - Schadensbeschreibung (betroffene Kfz-Teile, Hergang etc.)

b) Über AudaNet können die nachfolgend genannten Daten ausgetauscht werden. Welche Daten der Verantwortliche austauscht, legt dieser im Einzelfall fest:

- Adress- und Kontaktdaten:
  (in der Regel Name, Anschrift, Telefon- und Telefaxnummer, E-Mail-Adresse und ggf. weitere Kontaktdaten) von folgenden Personen:
  - Fahrer
  - Versicherungsnehmer
  - Fahrzeughalter
  - Unfallgegner
  - Werkstatt
  - Versicherung
  - Sachverständiger und weiteren involvierten Dienstleistern
  - Kontaktperson für „Besichtigung“ des KFZ
  - ggf. weiteren involvierten Personen
- von den Beteiligten vergebene Schaden-Nummern
  (z. B. des Vorgangs, des Vermittlers, des Unfallgegners etc.)
- Versicherungsdaten des Versicherungsnehmers und ggf. Unfallgegners
  (z. B. Versicherungsschein-Nummern sowie Vertragsart und Vertragstyp, Versicherungsvertragsdaten (z. B. Deckungssummen, Zeitraum des Versicherungsschutzes etc.)
- Daten zum Fahrzeug
  (z. B. amtl. Kennzeichen, Fahrzeug-Ident-Nummer, KBA-Schlüssel, Modellbezeichnung, Ausführung/Ausstattung, Erstzulassung, Fahrzeugwerte, Zustand, Laufleistung etc.)
- Unfalldaten
  (z. B. Datum und Uhrzeit, Ursache, Ort etc.)
- Schadensbeschreibung
  (z. B. polizeiliche Aufnahme/Dienststelle/Aktenzeichen etc.)
- Anstoßbereiche
  (z. B. Anstoßbereich, -richtung, -punkt; Reparaturdaten etc.)
- Besichtigungsdaten
  (z. B. Datum und Uhrzeit, Ort etc.)
- Preisfaktoren der Werkstatt
  (z. B. Lohn-/Lackpreise, sonstige Preisfaktoren etc.)
- Schadenpositionen
  (z. B. Kalkulationsdaten und -werte)
- Berechnungsergebnisse
  (z. B. Kalkulation/Kostenvoranschlag, Fahrzeugbewertung etc.)
- den ausgetauschten Daten beigefügte Anhänge
  (z. B. Bilder, PDF-Dateien etc.)

Sofern die Komponente „AudaFusionWeb“ genutzt wird, können außerdem folgende Daten auf den AudaNet-Servern gespeichert werden:

- Buchhaltungsdaten
  (z. B. Debitor- und Kreditorstammdaten, Rechnungsdaten [Rechnungshöhe, -nummer, -datum] etc.)

- Kontodaten
  (Kontoinhaber, IBAN, BIC, Währung etc.; von Sachverständigen und Auftraggebern)
- Mitarbeiterdaten
  (Adress- und Kontaktdaten, eingescannte Unterschrift [als Stempel zur Verifizierung eines Prozesses])
- Zugangs-/Logindaten zu externen Onlineschnittstellen
  (z. B. Restwertbörsen, Prüfdienstleistern, DATEV, SSH)

4. Kreis der Betroffenen

a) Der Kreis der Betroffenen umfasst folgende Personenkategorien:

- Versicherungsnehmer
- Geschädigte und versicherte Personen des Verantwortlichen
- Kunden
- Sachverständige / Gutachter

b) Der Kreis der Betroffenen umfasst folgende Personenkategorien:

- Reparaturwerkstätten
- Versicherer und Sachverständige, soweit diese an AudaNet teilnehmen
- Fahrzeughalter, Versicherte, involvierte Dienstleister und weitere an der Schadensabwicklung Beteiligte.

Wer diese Beteiligten sind, hängt vom konkreten Schadensfall ab; betroffen sind regelmäßig Fahrer, Sachverständige, Rechtsanwälte der Beteiligten, sowie etwa hinzugezogene Beamten einer bestimmten Polizeiniederlassung.

5. Technisch-organisatorische Datenschutz- und Datensicherheits-Maßnahmen

Der Auftragsverarbeiter hat die Umsetzung der technischen und organisatorischen Maßnahmen in Anhang 1 dokumentiert. Die dokumentierten Maßnahmen sind Grundlage des Auftrags. Soweit eine Prüfung oder ein Audit des Verantwortlichen einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

Insgesamt handelt es sich bei den zu treffenden Maßnahmen um nicht auftragsspezifische Maßnahmen hinsichtlich der Kontrolle von Organisation, Zutritt, Zugang, Zugriffen, Weitergaben, Aufträgen und Verfügbarkeit sowie der Kontrolle des Trennungsgebots.

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.

6. Berichtigung, Sperrung und Löschung von Daten

Der Auftragsverarbeiter hat nur nach Weisung des Verantwortlichen die Berichtigung, Sperrung oder Löschung der verarbeiteten personenbezogenen Daten vorzunehmen. Anfragen Betroffener bezüglich dieser Maßnahmen sind unverzüglich an den Verantwortlichen zur direkten Beantwortung weiterzuleiten.

Vom Auftragsverarbeiter in anonymisierter Form gespeicherte Daten (vgl. Ziffer 4) bleiben von den Pflichten dieser Ziffer unberührt.

7. Kontrollen und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags folgende Pflichten:

(1) Der Auftragsverarbeiter hat einen betrieblichen Datenschutzbeauftragten bestellt. Dessen Kontaktdaten werden dem Verantwortlichen zum Zweck der direkten Kontaktaufnahme mitgeteilt:

Sascha Kremer
#LOGIN Datenschutzberatung
Rommerskirchener Straße 21, 50259 Pulheim
+49 (0)2238 1401762
audatex-dsb@login.fm.

Ein Wechsel des Datenschutzbeauftragten ist dem Verantwortlichen unverzüglich mitzuteilen.

(2) Der Auftragsverarbeiter setzt für die auftragsgemäße Verarbeitung personenbezogener Daten nur Personal ein, das auf das Datengeheimnis nach EU-DSGVO verpflichtet wurde. Er sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den Bestimmungen des Datenschutzes vertraut macht.

(3) Der Auftragsverarbeiter gewährleistet im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die von der EU-DSGVO vorgeschriebenen und die darüber hinaus vereinbarten technischen und organisatorischen Sicherheitsmaßnahmen und deren Nachweisbarkeit gegenüber dem Verantwortlichen. Hierzu kann der Auftragsverarbeiter auch aktuelle Testate, Berichte unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision) oder eine geeignete Zertifizierung vorlegen. Der Auftragsverarbeiter beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Er bestätigt, dass ihm die einschlägigen Datenschutzvorschriften bekannt sind. Der Auftragsverarbeiter sichert zu, dass er die Einhaltung der datenschutzrechtlichen Vorschriften überwacht.

(4) Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde informieren, soweit diese die im Auftrag verarbeiteten Daten betreffen.

(5) Soweit die Daten in Privatwohnungen oder im Rahmen der Telearbeit verarbeitet werden, ist der Zutritt zur Wohnung vorher mit dem Auftragsverarbeiter abzustimmen. Der Auftragsverarbeiter sichert das Einverständnis der Bewohner zu.

(6) Der Auftragsverarbeiter verpflichtet sich über den Bestand und den Inhalt dieses Vertrags striktes Stillschweigen zu bewahren. Diese Verpflichtung besteht auch nach Vertragsende.

(7) Der Auftragsverarbeiter wird geeignete technische und organisatorische Maßnahmen treffen, um den Verantwortlichen nach Möglichkeit bei seiner Verpflichtung zur Beantwortung von Anfragen betroffener Personen zu unterstützen, dies betrifft insbesondere Anfragen betroffener Personen in Bezug auf:

- Auskunft (Art. 15 EU-DSGVO)
- Berichtigung (Art. 16 EU-DSGVO)
- Löschung (Art. 17 EU-DSGVO)
- Einschränkung der Verarbeitung (Art. 18 EU-DSGVO)
- Datenportabilität (Art. 20 EU-DSGVO) sowie
- Widerspruch (Art. 21 EU-DSGVO)

(8) Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen wird der Auftragsverarbeiter den Verantwortlichen bei der Sicherheit der Verarbeitung, der gesetzlich erforderlichen Meldung von Verstößen an die Aufsichtsbehörde sowie der gesetzlich erforderlichen Benachrichtigung der betroffenen Person bezüglich einer Verletzung des Schutzes personenbezogener Daten unterstützen.

8. Unterauftragsverhältnisse, Telearbeit

(1) Aufträge an Unterauftragnehmer dürfen nur nach vorheriger Genehmigung in Textform durch den Verantwortlichen vergeben werden. Der Auftragsverarbeiter gewährleistet bei Vergabe von Unteraufträgen die Einhaltung der Vorschriften des EU-DSGVO bezüglich der Auftragsdatenverarbeitung. Er hat die Einhaltung dieser Regelungen durch den Unterauftragnehmer regelmäßig zu überprüfen.

Zurzeit sind die folgenden Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Verantwortliche einverstanden:

- Die Audatex (Schweiz) GmbH, Elias-Canetti-Strasse 2, 8050 Zürich, Schweiz, stellt als Service Provider die technische Infrastruktur (physikalische Server) zur Verfügung, in welcher die Daten verarbeitet werden. Diese technische Infrastruktur steht bei zwei Drittanbietern, welche Serverstellplatz mit Klimatisierung und Stromversorgung jeweils in einem Rechenzentrum zur Verfügung stellen; an der Datenverarbeitung sind die Drittanbieter nicht beteiligt.

(2) Der Auftragsverarbeiter hat die vertraglichen Vereinbarungen mit Unterauftragnehmern so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen dem Verantwortlichen und Auftragsverarbeiter entsprechen und dem Verantwortlichen Kontroll- und Überprüfungsrechte beim Unterauftragnehmer eingeräumt werden.

(3) Der Auftragsverarbeiter gewährleistet eine Protokollierung der Systemleistungen, insbesondere wenn Dritte auf das System des Auftragsverarbeiters zugegriffen haben (Fernwartung).

(4) Mitarbeiter des Auftragsverarbeiters verarbeiten in Privatwohnungen personenbezogene Daten im Rahmen der Telearbeit bis auf Widerruf. Der Verantwortliche erlaubt die Verarbeitung von diesen Daten nur unter Gewährleistung der nötigen Datenschutz- und Datensicherheitsmaßnahmen. Soweit Daten des Verantwortlichen in einer Privatwohnung verarbeitet werden, ist der Zugang zur Wohnung zu Zwecken der Auftragskontrolle vorher mit dem Verantwortlichen abzustimmen. Der Auftragsverarbeiter versichert, dass alle Bewohner dieser Privatwohnung mit dieser Regelung einverstanden sind.

(5) Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z. B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

9. Kontrollrechte des Verantwortlichen

(1) Der Auftragsverarbeiter berechtigt den Verantwortlichen jederzeit nach vorheriger Absprache die Einhaltung der Vorschriften über den Datenschutz und die vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

10. Mitzuteilende Verstöße durch den Auftragsverarbeiter

(1) Der Auftragsverarbeiter unterrichtet den Verantwortlichen umgehend bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Verletzungen von Datenschutzbestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen.

(2) Insbesondere bei Verdacht auf eine Verletzung des Schutzes personenbezogener Daten gem. Art. 33, 34 EU-DSGVO (meldepflichtige Datenpanne) ist der Verantwortliche unverzüglich zu benachrichtigen. Soweit den Verantwortlichen Pflichten nach Art. 33, 34 EU-DSGVO treffen, hat der Auftragsverarbeiter ihn hierbei zu unterstützen.

11. Weisungsbefugnis des Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten des Verantwortlichen ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Verantwortlichen. Dies gilt nicht, soweit das Recht der Europäischen Union oder deutsches Recht den Auftragsverarbeiter zur weitergehenden Verarbeitung verpflichten. In diesem Fall wird der Auftragsverarbeiter den Verantwortlichen über eine solche weitergehende Verarbeitungspflicht informieren, außer wenn dem Auftragsverarbeiter eine solche Information auf Grund wichtigen öffentlichen Interesses kraft Gesetzes nicht gestattet ist.

(2) Der Verantwortliche behält sich zu jeder Zeit das uneingeschränkte Verfügungsrecht über die dem Auftragsverarbeiter zur Erfüllung des Auftrags zur Verfügung gestellten personenbezogenen Daten vor. Der Auftragsverarbeiter unterwirft sich hinsichtlich der Verarbeitung und Nutzung dieser Daten den Weisungen des Verantwortlichen.

(3) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche oder andere zwingende gesetzliche Vorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch die zuständige Person beim Verantwortlichen bestätigt oder geändert wird.

(4) Sollte Eigentum des Verantwortlichen beim Auftragsverarbeiter durch Maßnahmen Dritter, etwa durch Pfändung, durch ein Konkurs- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, hat der Auftragsverarbeiter den Verantwortlichen unverzüglich und vor Eintritt dieser Maßnahmen zu verständigen.

12. Löschung von Daten und Rückgabe von Datenträgern

(1) Der Auftragsverarbeiter verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen als die vereinbarten Zwecke und bewahrt sie nicht länger auf, als es der Verantwortliche bestimmt hat. Kopien oder Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt. Der Auftragsverarbeiter erwirbt keinerlei Rechte an den ihm zur Verfügung gestellten Daten.

(2) Anfallendes Test- und Ausschussmaterial wird vom Auftragsverarbeiter unter Verschluss gehalten, bis es entweder vom Auftragsverarbeiter datenschutzgerecht vernichtet oder dem Verantwortlichen übergeben wird. Nicht mehr benötigte Unterlagen mit personenbezogenen Daten dürfen erst nach vorheriger Zustimmung durch den Verantwortlichen datenschutzgerecht vernichtet werden.

(3) Nach Abschluss der vertraglichen Arbeiten des jeweiligen Einzelvertrags und auf schriftliches Verlangen des Verantwortlichen hat der Auftragsverarbeiter sämtliche in Zusammenhang mit dem jeweiligen Einzelvertrag in seinen Besitz gelangten Unterlagen und physisch erstellte Verarbeitungsergebnisse dem Verantwortlichen auszuhändigen. Die Datenträger des Auftragsverarbeiters sind danach physisch zu löschen.

(4) Die Verpflichtung auf das Datengeheimnis und zur Einhaltung der Vertraulichkeit bleibt auch nach Beendigung des Auftrages bestehen.

13. Pflichten des Verantwortlichen

(1) Der Verantwortliche ist verantwortlich für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen.

(2) Der Verantwortliche ist für die Sicherheit aller Unterlagen auf dem Transportweg zum Auftragsverarbeiter verantwortlich.

(3) Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei Prüfung der Auftragsergebnisse festgestellt hat.

(4) Der Verantwortliche ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen des Auftragsverarbeiters vertraulich zu behandeln.

(5) Der Verantwortliche ist verpflichtet seine Weisungen an den Auftragsverarbeiter zu dokumentieren.

14. Schlussbestimmungen

Sollte einer der oben genannten Vertragsbestandteile unwirksam sein, so bleibt die Wirksamkeit des Vertrages im Übrigen unberührt. Die unwirksame Bestimmung ist unverzüglich durch eine Neuregelung zu ersetzen, die in ihrer Auswirkung der gewollten Bestimmung möglichst nahekommt.

Anhang 1: Technische und organisatorische Maßnahmen

IT-Infrastrukturbeschreibung

Der Auftragnehmer nutzt über die Audatex (Schweiz) GmbH, Elias-Canetti-Strasse 2, CH-8050 Zürich-Oerlikon, je ein Primär- und Sekundärrechenzentrum in der Schweiz (an unterschiedlichen Standorten in Zürich). Die Audatex (Schweiz) GmbH sowie beide Rechenzentren sind bzgl. IT-Sicherheit ISO-27001-zertifiziert. Gleiches gilt für Server und Administration bzgl. der Kommunikationsplattform „AudaNet“. Der Unternehmenshauptsitz befindet sich in Berlin, mit einer Geschäftsstelle in Neuss und kleineren Softwareentwicklungsstätten in Döbeln und Bruchsal. Für alle Arbeitsstätten gilt: Produktiv- und Testdaten werden allein in den Rechenzentren gespeichert und diese Daten nur über eine gesicherte VPN-Verbindung lediglich am Bildschirm dargestellt. Bandbackups werden über die Audatex Schweiz GmbH verschlüsselt erstellt und dort separat verschlüsselt gelagert. Der Auftragnehmer setzt über die Audatex (Schweiz) GmbH neben Microsoft-Windows-Server- auch Linux-basierte Clientbetriebssysteme ein. Als Datenbanksysteme kommen Oracle- und Microsoft-SQL-Server-Datenbanken zum Einsatz.

A) Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

A1) <u>Zutrittskontrolle</u> (kein unbefugter Zutritt zu DV-Anlagen)

<u>Primär- und Sekundärrechenzentrum Zürich:</u>

Serververwaltung über Audatex (Schweiz) GmbH in separaten zutrittskontrollierten Cages. Zutrittskontrolle u. a. durch folgende Maßnahmen:

- Regelung für Zutrittsberechtigung und Genehmigung. Monatliche Prüfungen durch Audatex (Schweiz) GmbH; jährliche Prüfung durch Revisionsgesellschaft.
- Pförtner
- Vereinzelungsschleuse mit Kartenleser und Fingerabdrucksensor
- Videoüberwachung
- Elektronische Zutrittskontrolle durch Badges
- Ausweiskontrolle
- Besucherzutritt zu Cage nur in Begleitung und nur nach vorheriger Anmeldung
- Nochmalige Kontrolle der Zutrittsberechtigung im ausschließlich dem Unternehmen zugewiesenen Bereich
- Ausgebildetes Sicherheitspersonal
- Sicherheitszaun als Abgrenzung zu Nachbargrundstücken
- Gesondert gesicherter und zutrittsbeschränkter Raum innerhalb der Büroräume der Audatex (Schweiz) GmbH für Datenträger, welche personenbezogene Daten enthalten können (z. B. Sicherungsbänder)

<u>Büro Berlin:</u>

- Pförtner
- Empfangsdame

- Geregelte Badge- und Schlüsselverwaltung
- Videoüberwachung des Haupteingangs
- Datenträger, die personenbezogene Daten enthalten können, werden in einem gesondert gesicherten Raum innerhalb der Büroräume gelagert.

Büro Neuss:
- Empfangsdame
- Geregelte Schlüsselverwaltung
- Separate Sicherheitszone für den Bandbackupraum. Besucher dieses Raumes haben nur Zutritt in Begleitung.
- Datenträger, die personenbezogene Daten enthalten können (z. B. Sicherungsbänder), werden in einem gesondert gesicherten Raum innerhalb der Büroräume gelagert. Es gibt gesonderte Zutrittsberechtigungen.

Softwareentwicklungsstätte Döbeln:
- Geregelte Schlüsselverwaltung

Softwareentwicklungsstätte Bruchsal:
- Geregelte Schlüsselverwaltung

A2) Zugangskontrolle (Keine unbefugte Systembenutzung)
- Schutz aller DV-Systeme durch Zugriffsberechtigungsverfahren
- Eindeutige Benutzerkennung jedes Mitarbeiters
- Gemäß Passwortrichtlinie erzwungene Passworte
  - Gemäß üblicher Sicherheitsstandards bzgl. Länge, Aufbau und Historie
  - Regelmäßige obligatorische Passwortänderung
- Automatische Sperrung inaktiver Bildschirme durch automatische Bildschirmschoner; Reaktivierung durch Kennwort
- Firewall-Systeme zum Netzwerkschutz gegen unberechtigte Zugriffe
- Einsatz stets aktualisierter Virenschutzsoftware auf mehreren Ebenen
- (Arbeitsplatz, Mailsystem, Proxy)
- Bzgl. Datenbankzugriffen auf Systemlevel: Zusätzlich zu Benutzernamen und Passwort wird Sicherheitstoken benötigt (persönlicher Code und Geheimzahl, erzeugt von einem als Hardwarekomponente ausgegebenen Security-Token)

A3) Zugriffskontrolle (Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems)
- Beschränkung von Benutzerrechten gemäß „Need to know"-Prinzip
- Gewährung von Userrechten immer durch andere, autorisierte Person
- Rollen-/Funktionsbasierter Zugriff auf DV-Systeme
- Protokollierter Zugriff auf Systeme
- Protokollierte Änderung an Zugriffsrechten
- Einsatz stets aktualisierter Virenschutzsoftware auf mehreren Ebenen eingesetzt (Arbeitsplatz, Mailsystem, Proxy).
- Standardmäßig verschlüsselte Laptops und Notebooks per Bitlocker
- Möglichkeit zur Fernlöschung von Mobiltelefonen
- Segmentierung und sichere Netzwerkübergänge durch Firewall-Systeme
- Regelmäßige PEN-Tests zum Entdecken und Beseitigen von Schwachstellen
- Aktueller System-Patchlevel (u. a. durch Einsatz von Microsoft WSUS)

A4) Trennungskontrolle (Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden)
- Mandantenfähige Systeme
- Getrennte Umgebungen für Entwicklung, Test und Produktion
- Keine Tests mit Originaldaten
- Sandboxing

A5) Pseudonymisierung (Art. 32 Abs. 1 lit. A und Art. 25 Abs. 1 DS-GVO)
- Nach Möglichkeit Nutzung von IDs statt Klardaten
- Berücksichtigung von Pseudonymisierung bei Softwareneu- und -weiterentwicklung

B) Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

B1) Weitergabekontrolle (Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport)
- Produktive Daten nur im RZ und am für Backuplagerung vorgesehen Ort
- Transport produktiver Daten, etwa zur Backupsite, wird mittels spezieller Sicherheitsfirma ausgeführt und vom Sicherheitspersonal begleitet
- Elektronische Übermittlung personenbezogener Daten erfolgt entweder verschlüsselt oder über sichere Datenleitungen, mit einer Verschlüsselungstiefe von mind. 128 Bit.
- USB-Port-Verschlüsselung
- E-Mail-Übermittlung standardmäßig per TLS 1.2 (AES 256 Bit Verschlüsselung), sofern Gegenstelle dies unterstützt
- Physischer Transport von Datenträgern nur durch eigene Boten
- Datenträger-Entsorgung durch zertifizierte Dienstleister, in verschlossenen Behältnissen, unter Beaufsichtigung von Sicherheitspersonal

B2) Eingabekontrolle (Feststellung, ob / von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt wurden)
- Eingabe sämtlicher Daten grundsätzlich nur durch den Auftraggeber bzw. von diesem benannten Nutzern
- Automatisierte Verarbeitung ohne manuelle Zwischenschritte
- Grundsätzlich keine Veränderung der Daten ohne Autorisierung des Auftraggebers
- Protokollierung physischer Zugriffe des Unternehmens. Bei technischen Problemen Möglichkeit zur Einsichtnahme auf Kundendaten durch einzelne autorisierte Mitarbeiter des Unternehmens

C) Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

C1) Verfügbarkeitskontrolle (Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen)
- Durchführung und Kontrolle von Backups und Restores gemäß strenger SOX- und ISO-27001-Richtlinien
- Doppelt ausgelegte Rechenzentren mit Spiegelung der Festplatten
- Redundante Systeme
- Backup-Verfahren mit regelmäßig an gesicherten Orten ausgelagerten Datenträgern
- Unterbrechungsfreie Stromversorgung, Klimaanlage, Brandmeldeanlage
- Rechenzentren in der Schweiz haben zusätzlich netzunabhängige Stromversorgung sowie eine automatische Löschanlage
- Redundante Internetverbindungen
- Meldewege und Notfallpläne
- Virenschutz auf vielen Ebenen (Arbeitsplatz, Proxy, Mailsystem. Server)
- Firewall
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

D) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

D1) Datenschutz-Management (Unternehmensorganisation ist so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird)
- Bestellung eines Datenschutzbeauftragten (s. o.)
- Verpflichtung aller Mitarbeiter auf Einhaltung des Datenschutzes
- Regelmäßige Schulungen aller Mitarbeiter bzgl. IT-Sicherheit und Datenschutz
- Einbindung von „Privacy by Design" bereits in die Konzeptphase der Softwareentwicklung

D2) Incident-Response-Management (Prozessmanagement bzgl. Vorfällen / Störungen zu Datenschutz und IT-Sicherheit)
- Dokumentierte Richtlinien und Prozesse zu:
  - Datenschutzverstößen („Data Breach") gem. Art. 33 GDPR
  - Störungen bzgl. IT-Sicherheit („Security Breach")
  - Wahrnehmung von Betroffenenrechten (Recht auf Vergessenwerden; Änderung, Löschung, Widerspruch bzw. Recht auf Übertragung von personenbezogenen Daten)
  - Anfragen von Betroffenen

D3) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
- Optional abschaltbare Cookies auf Webseiten des Unternehmens (sofern Webseitennutzung ohne Cookies technisch möglich)
- Frühzeitige Berücksichtigung datenschutzfreundlicher Voreinstellungen bei neu- und weiterentwickelter Software

D4) Auftragskontrolle (Keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers)
- Eindeutige Vertragsgestaltung
- Strenge Auswahl des Dienstleisters
- Verarbeitung personenbezogener Daten ausschließlich gemäß Weisung des Dienstleisters

Mit dem Inhalt dieser Vereinbarung erklärt sich einverstanden:

Audatex AUTOonline GmbH

Berlin, _____

_____	_____
Oliver Blüher	ppa. Erik Jahn
Area Managing Director GSA	Leiter Sales & Customer Support

Mit dem Inhalt dieser Vereinbarung erklärt sich einverstanden:

_____
Ort, Datum

_____	_____
Stempel (Auftraggeber)	Unterschrift (Auftraggeber)
	_____
	Name bitte auch in Druckbuchstaben

Bitte senden Sie diese Seite unterschrieben im Original zurück an:

Inhalt: Auftragsverarbeitungsvertrag

Audatex AUTOonline GmbH
- Sales Backoffice -
Lorenzweg 5
12099 Berlin

Mit dem Inhalt dieser Vereinbarung erklärt sich einverstanden:

Audatex AUTOonline GmbH

Berlin, _____

_____
Oliver Blüher
Area Managing Director GSA

_____
ppa. Erik Jahn
Leiter Sales & Customer Support

Mit dem Inhalt dieser Vereinbarung erklärt sich einverstanden:

_____
Ort, Datum

_____
Stempel (Auftraggeber)

_____
Unterschrift (Auftraggeber)

Audatex ID:_____

_____
Name bitte auch in Druckbuchstaben