Beauftragung zur Datenverarbeitung im Auftrag (Auftragsdatenverarbeitung)

zwischen

API – Automotive Process Institute GmbH
Wittenberger Straße 15
04129 Leipzig

- im Folgenden "**API**" -

und

dem **Vertragspartner**

- im Folgenden "**Kunde**" -

1. Vorbemerkungen

API stellt dem Kunden im Rahmen eines Nutzungsverhältnisses ein API Digitalannahme-System bestehend aus verschiedenen Produkten zur Verfügung. Auf den gesonderten Nutzungsvertrag, dessen rechtlicher Bestand Grundlage dieser Vereinbarung ist, wird verwiesen. Die zum Zwecke der individuellen Kundenbetreuung erforderlichen Daten zur Nutzung der API Digitalannahme-Systeme werden vom Kunden erhoben und durch das Personal des Kunden in computergestützter Form erfasst. Die erfassten Daten werden durch API für den Kunden in dessen Auftrag verarbeitet. Der Kunde hat API im Rahmen seiner Sorgfaltspflichten nach dem Bundesdaten-schutzgesetz (BDSG) als Dienstleister zur Auftragsdaten-verarbeitung i.S.d. § 11 BDSG ausgewählt und beauftragt. Sofern in diesem Vertrag die Begrifflichkeiten „Datenverarbeitung“ oder „Verarbeitung von Daten“ verwandt werden, wird darunter allgemein und lediglich die Verwendung von personenbezogenen Daten verstanden. Eine Verwendung personenbezogener Daten umfasst insbesondere die Speicherung, Veränderung, Übermittlung, Sperrung, Löschung sowie das Anonymisieren, Pseudonymisieren, Verschlüsseln oder die sonstige Nutzung von Daten (§ 3 Abs. 4 BDSG). Innerhalb dieser Vereinbarung ist als „Endkunde“ der Kunde des Auftraggebers zu verstehen.

2. Gegenstand des Auftrags

2.1 Der Auftrag des Kunden zur Datenverarbeitung durch API umfasst die Verarbeitung von Endkundendaten, wenn und soweit diese zur Erbringung der Dienstleistungen laut den Leistungsbestandteilen des zugrunde liegenden Nutzungsvertrages erforderlich sind, insbesondere die Verarbeitung von:

- Personenstammdaten
- Kommunikationsdaten
- Fahrzeugdaten
- Vertragsabrechnungs- und Zahlungsdaten
- die Kundenhistorie
- Planungs- sowie Steuerungsdaten

2.2 Die verarbeiteten Daten können im Auftrag des Kunden mit Daten von Dritten ergänzt bzw. mit Dritten ausgetauscht werden, um alle angebotenen Dienstleistungen laut dem Leistungsverzeichnis des zugrunde liegenden Nutzungsvertrages zu ermöglichen.

2.3 Die vom Kunden erhobenen Daten werden ebenfalls zum Zwecke der Abrechnung gegenüber dem Kunden und des erneuten Abrufs der Daten durch den Kunden im Falle einer wiederholten Nutzung (Übermittlung) gespeichert.

2.4 Der Kunde kann die erhobenen Daten für Informationszwecke gegenüber den Endkunden für Services oder Aufträge im Rahmen der Kundenbetreuung unter Verwendung der verarbeiteten Daten jederzeit im Rahmen der Vertragslaufzeit abrufen.

2.5 Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Darüberhinausgehende Verlagerungen bedürfen der schriftlichen Zustimmung des Kunden.

3. Rechte und Pflichten des Kunden

3.1 Der Kunde ist verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG für die Verarbeitung von Daten im Auftrag durch API. Die Beurteilung der Zulässigkeit der Datenverarbeitung erfolgt allein durch den Kunden. API steht das Recht zu, den Kunden auf ihrer Meinung nach rechtlich unzulässige Datenverarbeitungen hinzuweisen. Die Regelungen des § 3 Abs. 6 dieses Vertrages bleiben unberührt.

3.2 Der Kunde ist als verantwortliche Stelle für die Wahrung der Rechte der Endkunden verantwortlich. Diese Rechte sind gegenüber dem Kunden wahrzunehmen. API wird den Kunden unverzüglich darüber informieren, wenn Endkunden ihre Rechte direkt gegenüber API geltend machen.

3.3 Der Kunde hat sich zu Beginn der Datenverarbeitung von der Einhaltung der bei API getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit überzeugt

und wird dies auch künftig in regelmäßigen Abständen tun und in geeigneter Weise dokumentieren.

3.4 Sofern erforderlich und nicht in dieser Vereinbarung bereits abschließend geschehen, ist der Kunde berechtigt, ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber API zu erteilen. Etwaiger Mehraufwand für ergänzend erteilte Weisungen ist über § 8 hinaus gesondert zu vergüten. Weisungen haben schriftlich zu erfolgen. Im Falle der Erteilung ergänzender Weisungen wird API den Kunden unverzüglich darüber informieren, wenn eine vom Kunden erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen des Datenschutzes verstößt. In diesem Fall ist API berechtigt, die Durchführung der betreffenden Weisung(en) bis zur Klärung der Angelegenheit auszusetzen.

3.5 Der Kunde kann weisungsberechtigte Personen benennen. Für den Fall, dass sich die weisungsberechtigten Personen beim Kunden ändern, wird der Kunde dies API schriftlich mitteilen.

3.6 Der Kunde informiert API unverzüglich, sollte er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch API feststellen.

3.7 Für den Fall, dass eine Informationspflicht gegenüber Dritten nach § 42a BDSG besteht, ist der Kunde für die Erfüllung der Pflichten aus § 42a BDSG verantwortlich.

4. ALLGEMEINE PFLICHTEN VON API

4.1 API wird personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Kunden gemäß § 2 Abs. 4 erteilten ergänzenden Weisungen verarbeiten. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach diesem Vertrag und/oder ergänzenden Weisungen des Kunden gemäß § 2 Abs. 4. Eine hiervon abweichende Verarbeitung von Daten ist API untersagt, es sei denn, dass der Kunde dieser schriftlich zugestimmt hat.

4.2 Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien dürfen erst nach vorheriger Zustimmung durch den Kunden datenschutzgerecht vernichtet werden.

4.3 API bestätigt, dass sie einen betrieblichen Datenschutzbeauftragten i.S.d. § 4f BDSG bestellt hat und wird diesen gegenüber dem Kunden auf Anforderung benennen.

4.4 API sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung sämtlicher vereinbarter Maßnahmen zu. Sie sichert insbesondere zu, dass die verarbeiteten Daten der Anlage von sonstigen Datenbeständen aus anderen Anlagen getrennt werden.

4.5 API wird ihr Unternehmen und ihre Betriebsabläufe so gestalten, dass die Daten, die sie im Auftrag des Kunden verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. API wird Änderungen bei der Vorgehensweise der beauftragten Datenverarbeitung, die für die Sicherheit der Daten erheblich sind, vorab mit dem Kunden abstimmen.

4.6 API wird dem Kunden jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die gemäß § 2 Abs. 4 erteilten Weisungen des Kunden unverzüglich mitteilen.

4.7 API wird die Daten, die sie im Auftrag für den Kunden verarbeitet, für die jeweilige Anlage kennzeichnen. Sofern die Daten für verschiedene Zwecke verarbeitet werden, wird API die Daten mit dem jeweiligen Zweck kennzeichnen.

4.8 An einer etwaigen Erstellung von Verfahrensverzeichnissen durch den Kunden hat API mitzuwirken. Sie hat dem Kunden die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

4.9 API kann empfangsberechtige Personen für Weisungen des Kunden benennen. Für den Fall, dass sich die berechtigten Personen bei API ändern, wird sie dies dem Kunden mitteilen.

5. KONTROLLBEFUGNISSE

5.1 Der Kunde hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der vertraglichen bzw. weisungsbedingten Regelungen durch API jederzeit im erforderlichen Umfang zu kontrollieren. API wird dem Kunden auf Anforderung insoweit entsprechende Auskunft erteilen, soweit dies zur Wahrung seiner Rechte im Sinne des Satz 1 erforderlich ist.

5.2 Der Kunde kann durch einen von Beruf wegen zur Verschwiegenheit verpflichteten Angehörigen der rechts- und steuerberatenden Berufe die Einsichtnahme in die von API für ihn verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen. Dieser kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte von API zu den jeweils üblichen Geschäftszeiten vornehmen. Der Kunde wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, sofern die Betriebsabläufe von API durch die Kontrollen gestört werden. Entstehende Mehrkosten sind durch den Kunden zu tragen.

5.3 API ist verpflichtet, im Falle von Maßnahmen der zuständigen Aufsichtsbehörden nach § 38 BDSG, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Kunden zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Kunde ist über entsprechende geplante Maßnahmen von API zu informieren.

6. DATENGEHEIMNIS, GEHEIMHALTUNGSPFLICHTEN

6.1 API ist bei der Verarbeitung von Daten für den Kunden zur Wahrung des Datengeheimnisses nach § 5 BDSG verpflichtet. API verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie den Kunden treffen. Der Kunde wird API entsprechend informieren.

6.2 API sichert zu, dass ihr die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und sie mit

der Anwendung dieser vertraut ist. API sichert ferner zu, dass sie die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und diese auf das Datengeheimnis i.S.d. § 5 BDSG verpflichtet werden.

6.3 Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

7. WAHRUNG VON ENDKUNDENRECHTEN

Der Kunde ist für die Wahrung der Rechte der Endkunden allein verantwortlich. Soweit eine Mitwirkung von API für die Wahrung von Rechten der Endkunden - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Kunden erforderlich ist, wird API die jeweils erforderlichen Maßnahmen nach Weisung des Kunden gemäß § 2 Abs. 4 treffen. Ein diesbezüglich entstehender Mehraufwand bei API ist API über § 8 hinaus gesondert zu vergüten.

8. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN ZUR DATENSICHERHEIT

8.1 API verpflichtet sich gegenüber dem Kunden zur Einhaltung der technischen und organisatorischen Maßnahmen gemäß § 9 BDSG, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind.

8.2 Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen lautet wie folgt:

(a) Zutrittskontrolle zu Datenverarbeitungsanlagen:
- Schutz durch Alarmsysteme
- Absicherung von Gebäudeschächten
- Transponder-Schließsysteme
- Schlüsselregelung
- Sicherheitsschlösser
- Videoüberwachung der Zugänge

(b) Zugangskontrolle
- Zuordnung von Benutzerrechten
- Authentifikation mit Benutzername / Passwort
- Einsatz von VPN-Technologie
- Schlüsselregelung
- Sicherheitsschlösser
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall

(c) Zugriffskontrolle
- Dokumentiertes Berechtigungskonzept
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das "Notwendigste" reduziert
- Passwortrichtlinien inkl. Passwortlänge, Passwortwechsel
- Sichere Aufbewahrung von Datenträgern
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- Einsatz von Aktenvernichtern bzw. Dienstleistern

(d) Weitergabekontrolle
- Einrichtung von Standleitungen bzw. VPN-Tunneln
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- Einsatz von verschlüsselten Kommunikationsmitteln

(e) Eingabekontrolle
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

(f) Auftragskontrolle
- Auswahl von Dritten durch den Auftragnehmer unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- Schriftliche Weisungen an den Auftragnehmer (Vereinbarung zur Auftragsdatenverarbeitung)
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§5 BDSG)
- Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer

(g) Verfügbarkeitskontrolle
- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperaturen und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen an einen beauftragten Sicherheitsdienstleister
- Dokumentiertes Backup- & Recoverykonzept
- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

(h) Serverräume nicht unter wasserführenden Anlagen
Trennungsgebot
- Logische Kunden- und Anlagentrennung (softwareseitig)
- Dokumentiertes Berechtigungskonzept
- Dokumentierte Datenbankrechte
- Trennung von Produktiv- und Testsystem

8.3 Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen sind schriftlich zu vereinbaren. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können von API ohne Abstimmung mit dem Kunden umgesetzt werden. Der Kunde kann jederzeit eine aktuelle Fassung der von API getroffenen technischen und organisatorischen Maßnahmen anfordern.

9. DAUER, BEENDIGUNG

9.1 Der Vertrag beginnt am Tage der Überlassung der Produkte gemäß dem Nutzungsvertrag zwischen Kunden und API und endet mit Beendigung dieses Vertrages, er ist insoweit abhängig vom rechtlichen Bestand des zugrundeliegenden Nutzungsverhältnisses. Das Nutzungsverhältnis ist hingegen unabhängig vom Bestand dieser Vereinbarung.

9.2 Nach Beendigung des Vertrages hat API sämtliche in ihren Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dieser Vereinbarung stehen, dem Kunden auszuhändigen oder datenschutzgerecht zu vernichten. Dies betrifft auch etwaige Datensicherungen bei API. Die Löschung ist in geeigneter Weise zu dokumentieren. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch API entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

10. SONSTIGES

10.1 Sollte das Eigentum des Kunden bei API durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat API den Kunden unverzüglich zu informieren. API wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

10.2 Alle Änderungen und Ergänzungen dieses Vertrages bedürfen zu ihrer Wirksamkeit der Schriftform. Das gilt auch für eine Änderung dieser Schriftformklausel selbst.

10.3 Sollte eine Bestimmung dieses Vertrages unwirksam oder undurchführbar sein oder werden, so wird die Wirksamkeit der übrigen Bestimmungen hierdurch nicht berührt. Die Parteien werden in diesem Fall die unwirksame oder undurchführbare Bestimmung durch eine wirksame und durchführbare Regelung ersetzen, durch die der mit der unwirksamen oder undurchführbaren Bestimmung beabsichtigte wirtschaftliche Zweck so weit wie möglich erreicht wird. Entsprechendes gilt im Fall von Lücken dieses Vertrages. Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

10.4 Gerichtsstand für sämtliche Streitigkeiten aus diesem Vertrag ist, soweit dies gesetzlich zulässig vereinbart werden kann, Leipzig. Daneben ist API berechtigt, den Kunden auch an seinem Sitz zu verklagen.

10.5 Sämtliche sich aus diesem Vertrag ergebenden Rechte und Pflichten bestimmen sich ausschließlich nach dem Recht der Bundesrepublik Deutschland.