Auftragsbearbeitungsvertrag (ABV)

1. Gegenstand und Dauer des Vertrages

1.1. Dieser Auftragsbearbeitungsvertrag (nachfolgend "Vertrag" genannt) regelt die Rechte und Pflichten der Auto-i-DAT AG, Widmerstrasse 73h, 8038 Zürich (nachfolgend "Auftragsbearbeiter" genannt) sowie ihrer einzelnen Kundinnen und Kunden (nachfolgend einheitlich die einzelnen "Auftraggeber", gemeinsam die "Parteien" genannt) im Zusammenhang mit der datenschutzrechtlichen Auftragsbearbeitung nach Art. 9 des Datenschutzgesetzes (nachfolgend "DSG" genannt). Dieser Vertrag ist für alle Tätigkeiten anwendbar, bei denen der Auftragsbearbeiter ganz oder teilweise Personendaten (nachfolgend "Personendaten") im Auftrag und gemäss Weisungen des jeweiligen verantwortlichen Auftraggebers bearbeitet oder bearbeiten lässt.

1.2. Der Auftragsbearbeiter erbringt für den Auftraggeber [Online-, Hosting- und Supportdienstleistungen [im Rahmen der Nutzung von auto-i EXPERT Online, der e-Service Plattform, SilverDAT3 (inkl. FotoApp), autoValue sowie motoValue] gestützt auf ein [separates Vertragsverhältnis/ auf ihre Allgemeinen Geschäftsbedingungen] (nachfolgend "Hauptvertrag" genannt). Dieser Vertrag bildet eine Anlage und Bestandteil des Hauptvertrages, die dem Vertrag mit dem Auftraggeber zugrunde liegen und vom Auftraggeber akzeptiert wurden. Mit der Unterzeichnung des Hauptvertrages anerkennen die Parteien die Bedingungen dieses Auftragsbearbeitungsvertrages als für sie verbindlich.

1.3. Dieser Vertrag ermöglicht es den Parteien, ihren Verpflichtungen nach dem anwendbaren Datenschutzrecht nachzukommen, wenn der Auftragsbearbeiter für den Auftraggeber Personendaten bearbeitet. Sie konkretisiert die Verpflichtungen der Parteien zum Datenschutz, die sich aus dem im separaten Vertrag beschriebenen Auftragsbearbeitung ergeben. Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem separaten Vertragsverhältnis in Zusammenhang stehen und bei welcher die Auftragsbearbeiter und seine Beschäftigten oder durch die Auftragsbearbeiter Beauftragte mit Personendaten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

2. Geltungsbereich und Gegenstand

2.1. Der vorliegende Vertrag gilt für jede Form der Bearbeitung von Personendaten für den Auftraggeber durch den Auftragsbearbeiter.

2.2. Gegenstand und Dauer sowie Art und Zweck der Bearbeitung ergeben sich aus dem Hauptvertrag sowie aus Anlage 1, sofern sie nicht bereits im Hauptvertrag und in der zugehörigen Leistungsbeschreibung genügend konkretisiert sind.

2.3. Die Art der Personendaten sowie die Kategorien der betroffenen Personen sind in Anlage 1 spezifiziert, sofern sie nicht bereits im Hauptvertrag und in der zugehörigen Leistungsbeschreibung genügend konkretisiert sind.

3. Pflichten des Auftragsbearbeiters

3.1.1. Weisungsgemässe Bearbeitung

3.1.2. Der Auftragsbearbeiter verpflichtet sich, die Personendaten ausschliesslich für die Zwecke des Hauptvertrags einschliesslich dieses Vertrags sowie gemäss den dokumentierten Instruktionen/Weisungen des Auftraggebers zu verarbeiten. Dies gilt insbesondere auch bezüglich der Übermittlung der Daten ins Ausland, in ein Drittland (unsicheres Land). Wird der Auftragsbearbeiter durch das anwendbare Recht zu weiteren Bearbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Bearbeitung mit.

3.1.3. Der Auftraggeber kann jederzeit neue Instruktionen erlassen, ergänzen oder bestehende Instruktionen ändern. Dies umfasst auch Instruktionen im Hinblick auf die Berichtigung, Löschung und Sperrung der Personendaten. Die Weisungen des Auftraggebers an den Auftragsbearbeiter bezüglich Art, Zweck, Bearbeitung und Speicherung der Personendaten sind im Vertrag und in der Anlage 1 zu diesem Vertrag dargelegt. Etwaige zusätzliche Weisungen sind vom Auftraggeber schriftlich oder in einem dokumentierten elektronischen Format zu erteilen. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format durch den Auftraggeber zu bestätigen.

3.1.4. Ist der Auftragsbearbeiter der Ansicht, dass eine Instruktion des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstösst, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragsbearbeiter ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragsbearbeiter darf die Durchführung einer offensichtlich rechtswidrigen Instruktion ablehnen.

3.1.5. Der Auftragsbearbeiter darf Personendaten nicht für andere Zwecke bearbeiten als die, mit denen der Auftragsbearbeiter beauftragt wurde.

3.1.6. Das Recht vom Auftragsbearbeiter, vom Auftraggeber abgeleitete oder hergeleitete Daten in aggregierter oder anonymisierter Form, die keine Personendaten enthalten, zu speichern, zu bearbeiten und zu verwerten, bleibt unberührt.

3.2. Pflicht zur Verschwiegenheit

3.2.1. Der Auftragsbearbeiter verpflichtet sich und leistet Gewähr dafür, dass er alle mit der Datenbearbeitung betrauten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit in schriftlicher Form verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen, und dass die Verschwiegenheitsverpflichtung der mit der Datenbearbeitung betrauten Personen auch nach Beendigung ihrer Tätigkeit beim Auftragsbearbeiter bestehen bleibt. Der Auftragsbearbeiter haftet für ein etwaiges Zuwiderhandeln der mit der Datenbearbeitung betrauten Personen, wie für sein eigenes Verhalten.

3.2.2. Der Auftragsbearbeiter verpflichtet sich, ohne das schriftliche oder elektronisch dokumentierte Einverständnis des Auftraggebers Dritten gegenüber keine Personendaten, die im Rahmen des vorliegenden Vertrags bearbeitet werden, offenzulegen oder auf sonstige Weise verfügbar zu machen, es sei denn, dies ist nach dem anwendbaren Recht oder aufgrund eines Gerichtsentscheides so vorgesehen.

3.3. Schutzmassnahmen des Auftragsbearbeiters

3.3.1. Der Auftragsbearbeiter verpflichtet sich und leistet Gewähr dafür, dass er angemessene technische und organisatorische Massnahmen (nachfolgend "TOMs" bezeichnet) zur Gewährleistung der Sicherheit der Bearbeitung, insbesondere der Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit, gemäss Art. 7 und 8 DSG ergriffen hat und aufrechterhält, um eine unbefugte Bearbeitung, einen Verlust oder eine Beschädigung der Personendaten zu verhindern. Dies beinhalten insbesondere die Mindestvorkehrungen, welche in Anlage 2 beschrieben sind.

3.3.2. Die TOMs dürfen entsprechend dem technischen Fortschritt weiterentwickelt und durch adäquate Schutzmassnahmen ersetzt werden, sofern sie das Sicherheitsniveau der festgelegten Massnahmen nicht unterschreiten und wesentliche Änderungen dem Auftraggeber mitgeteilt werden.

3.3.3. Die im Rahmen des Vertrages überlassene Personendaten sowie allfällige Datenträger und sämtliche hiervon gefertigten Kopien verbleiben im Eigentum des Auftraggebers, sind durch die Auftragsbearbeiter sorgfältig zu verwahren, vor Zugang durch unberechtigte Dritte zu schützen und dürfen nur mit Zustimmung des Auftraggebers, und dann nur datenschutzgerecht, vernichtet werden. Kopien von Personendaten dürfen nur erstellt werden, wenn sie zur Erfüllung der Leistungshaupt- und Nebenpflichten der Auftragsbearbeiter gegenüber dem Auftraggeber erforderlich sind (z.B. Backups).

3.4. Unterstützungspflichten

Der Auftragsbearbeiter ist verpflichtet, den Auftraggeber auf Verlangen bei der Einhaltung der geltenden Datenschutzgesetze jederzeit und soweit möglich zu unterstützen.

3.4.1. Anträge und Rechte betroffener Personen

Der Auftragsbearbeiter verpflichtet sich, den Auftraggeber mit geeigneten TOMs zu unterstützen, damit der Auftraggeber seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Personen (insbesondere Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch sowie automatisierte Einzelentscheidung) innerhalb der gesetzlichen Fristen jederzeit nachkommen kann, und überlässt dem Auftraggeber alle dafür notwendigen und ihm zur Verfügung stehenden Informationen.

Wird ein entsprechender Antrag an den Auftragsbearbeiter gerichtet, hat der Auftragsbearbeiter den Antrag unverzüglich an den Auftraggeber weiterzuleiten. Der Auftragsbearbeiter muss die Beantwortung solcher Anträge dem Auftraggeber überlassen, es sei denn, er ist gesetzlich dazu verpflichtet. In jedem Fall vereinbaren die Parteien, die Beantwortung solcher Anträge gegenseitig abzusprechen.

3.4.2. Weitere Informations- und Unterstützungspflicht

Der Auftragsbearbeiter verpflichtet sich, den Auftraggeber unter Berücksichtigung der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 7, 8, 22–24 DSG genannten Pflichten zu unterstützen (Datensicherheitsmassnahmen, Meldungen von Verletzungen der Datensicherheit an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung der Datensicherheit betroffenen Personen, Datenschutz-Folgenabschätzung und vorherige Konsultation).

Der Auftragsbearbeiter verpflichtet sich, den Auftraggeber unverzüglich zu benachrichtigen im Falle:

- einer etwaigen tatsächlichen oder mutmasslichen Verletzung der Datensicherheit unter Angabe sämtlicher dem Auftragsbearbeiter zur Verfügung stehenden Informationen betreffend die Art der Verletzung, deren Folgen und die ergriffenen oder vorgesehenen Schutzmassnahmen;
- des Vorliegens etwaiger Anträge auf Zugang sowie des tatsächlich erfolgten Zugangs zu Personendaten durch Behörden, sofern diese Benachrichtigung nicht per Gesetz aus wichtigen Gründen des öffentlichen Interesses verboten ist.

3.5. Rückgabe oder Löschungspflicht bei Vertragsbeendigung

3.5.1. Der Auftragsbearbeiter verpflichtet sich, nach Beendigung des Hauptvertrags einschliesslich dieses Vertrags oder auf Verlangen des Auftraggebers sämtliche Personendaten, vorbehaltlich gesetzlicher Aufbewahrungspflichten, an den Auftraggeber nach seiner Wahl zurückzugeben oder zu löschen.

3.6. Kontrollrechte des Auftraggebers

3.6.1. Der Auftragsbearbeiter verpflichtet sich, dem Auftraggeber sämtliche Informationen zur Verfügung zu stellen, die erforderlich sind, um die Einhaltung dieses Vertrags durch den Auftragsbearbeiter nachzuweisen und Überprüfungen, einschliesslich Inspektionen, durch den Auftraggeber selbst, einen vom Auftraggeber beauftragten Prüfer oder durch die Aufsichtsbehörde zu ermöglichen und aktiv zu unterstützen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zum Auftragsbearbeiter stehen, hat der Auftragsbearbeiter gegen die Beauftragung dieses Prüfers ein Widerspruchsrecht.

3.6.2. Kontrollen beim Auftragsbearbeiter haben innerhalb der Geschäftszeiten gemäss den Betriebsrichtlinien des Auftragsbearbeiters zu erfolgen, sind von dem Auftraggeber mit einer angemessenen Frist (mindestens dreissig Tage, ausser in Notfällen) anzumelden und durch den Auftragsbearbeiter zu unterstützen.

3.6.3. Um eine Kontrolle durchzuführen, sendet der Auftraggeber einen detaillierten Audit-/Kontroll-Plan mindestens zwei Wochen vor dem geplanten Prüfungstermin an den Auftragsbearbeiter und gibt darin den Umfang, die Dauer der Überprüfung sowie das Startdatum der Prüfung bekannt. Der Auftragsbearbeiter überprüft den Audit-/Kontroll-Plan und übermittelt an den Auftraggeber hierzu alle wesentlichen Bedenken und Fragen, wie beispielsweise Anfragen zu Informationen, die die Sicherheit, Privatsphäre oder Beschäftigungspolitik vom Auftragsbearbeiter beeinträchtigen können. In jedem Fall arbeitet der Auftragsbearbeiter mit dem Auftraggeber kooperativ zusammen, um einen abschliessenden Audit-/Kontroll-Plan zu vereinbaren.

3.6.4. Die Kontrollen sind auf den erforderlichen Rahmen beschränkt und müssen auf Betriebs- und Geschäftsgeheimnisse des Auftragsbearbeiters sowie den Schutz von Personendaten Dritter (z.B. anderer Kunden oder Mitarbeiter des Auftragsbearbeiters) Rücksicht nehmen. Der Auftragsbearbeiter darf die Inspektion von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der vom Auftragsbearbeiter getroffenen technischen und organisatorischen Maßnahmen sowie der Geschäfts- und Betriebsgeheimnisse vom Auftragsbearbeiter abhängig machen

3.6.5. Der Auftraggeber darf eine Überprüfung pro Kalenderjahr durchführen. Weitere Überprüfungen erfolgen nur gegen Kostenerstattung und nach vorheriger Abstimmung mit dem Auftragsbearbeiter.

3.6.6. Nach Wahl des Auftragsbearbeiters kann der Nachweis der Einhaltung der Pflichten nach diesem Vertrag anstatt einer Überprüfung durch den Auftraggeber gemäss den vorstehenden Bestimmungen auch durch Vorlage geeigneter Nachweise erbracht werden. Geeignete Nachweise können insbesondere ein genehmigtes Zertifizierungsverfahren im Sinne von Art. 13 DSG sein. Auch die Vorlage von Testaten oder Berichten unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Rechtsabteilung, IT-Sicherheitsbeauftragter, Datenschutzbeauftragter), ein schlüssiges Datensicherheitskonzept oder eine geeignete Zertifizierung durch ein IT-Sicherheits- und Datenschutzaudit werden als geeignete Nachweise anerkannt, wenn sie innerhalb der letzten zwölf Monate vor der Prüfanfrage des Auftraggebers erstellt wurden und der Auftragsbearbeiter oder die Unterauftragsbearbeiter schriftlich bestätigen, dass seit Erteilung keine wesentlichen Änderungen an den zu prüfenden Kontrollen und Systemen vorgenommen wurden.

4. Ort der Durchführung der Datenbearbeitung

4.1. Die Datenbearbeitungen werden in der Schweiz und Deutschland durchgeführt.

4.2. Der Auftragsbearbeiter verpflichtet sich, keine Personendaten, auch nicht teilweise, ohne vorgängige schriftliche oder elektronisch dokumentierte Zustimmung des Auftraggebers an ein Drittland zu übermitteln.

4.3. Werden die Datenbearbeitungstätigkeiten, wenn auch nur teilweise, auch ausserhalb des Europäischen Wirtschaftsraums (EWR) durchgeführt, stellt der Auftragsbearbeiter vorgängig ein angemessenes Datenschutzniveau u.a. mittels der nachfolgend aufgeführten geeigneten Garantien sicher:

- Angemessenheitsbeschluss der Europäischen Kommission sowie des Eidgenössischen Datenschutzbeauftragten (EDÖB) bzw. des Bundesrates;
- Standarddatenschutzklauseln der EU-Kommission mit den Anpassungen zum Schweizer Recht;
- eine vom DSG vorgesehene Ausnahme für bestimmte Fälle sowie für Einzelfälle;
- andere durch das DSG vorgesehen Garantien, die eine angemessenes Datenschutzniveau vorsehen.

5. Einsatz von Unterauftragsbearbeitern

5.1. Der Auftragsbearbeiter ist nicht berechtigt, einen Unterauftragsbearbeiter heranzuziehen, ohne vorgängig die schriftliche oder elektronisch dokumentierte Zustimmung des Auftraggebers einzuholen.

5.2. Der Auftragsbearbeiter hat den Unterauftragsbearbeiter sorgfältig auszuwählen, auf dessen Zuverlässigkeit zu prüfen und diese, als auch dessen Einhaltung der vertraglichen und gesetzlichen Vorgaben zu überwachen.

5.3. Der Auftragsbearbeiter ist befugt, die im Anhang 3 aufgeführten Unternehmen als Unterauftragsbearbeiter heranzuziehen.

5.4. Beabsichtigte Änderungen des Unterauftragsbearbeiters sind dem Auftraggeber rechtzeitig schriftlich oder in elektronisch dokumentierter Form bekannt zu geben, sodass er diese gegebenenfalls untersagen kann. Der Auftragsbearbeiter schliesst die erforderlichen Vereinbarungen zur Vertraulichkeit und zum Datenschutz mit dem Unterauftragsbearbeiter ab, welche mindestens so streng wie die Bestimmungen dieses Vertrags sein müssen. Dabei hat der Auftragsbearbeiter insbesondere sicherzustellen, dass der Unterauftragsbearbeiter dieselben Verpflichtungen eingeht und insbesondere auch die technischen und organisatorischen Massnahmen trifft, die dem Auftragsbearbeiter aufgrund dieses Vertrags obliegen.

5.5. Der Auftragsbearbeiter haftet gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Unterauftragsbearbeiters wie für sein eigenes Verhalten.

6. Ausserordentliches Kündigungsrecht

6.1. Jede Partei kann den Vertrag ausserordentlich und bei schwerwiegendem Verstoss jederzeit mit einer Frist von 30 Tagen ab schriftlicher Benachrichtigung über den wesentlichen Verstoss der anderen Partei kündigen, es sei denn, der Verstoss wird innerhalb dieser dreissig Tage geheilt. Ein schwerwiegender Verstoss des Auftragsbearbeiters liegt bspw. bei einer Verletzung der Datenschutzvorschriften, der Bestimmungen dieses Vertrages, der Weisungen des Auftraggebers oder wenn die Kontrollrechte des Auftraggebers vertragswidrig verweigert werden.

7. Vergütung

7.1. Der Auftragsbearbeiter hat Anspruch auf eine angemessene Vergütung für alle Arbeiten und alle Kosten, die aufgrund von Verarbeitungsanweisungen des Auftraggebers entstehen, wenn diese die Merkmale und das Sicherheitsniveau auf der Grundlage der Dienste übersteigen, die der Auftragsbearbeiter seinen Kunden normalerweise zur Verfügung stellt, z.B. wenn an den Auftragsbearbeiter Systemen oder Leistungen spezifische Anpassungen oder Entwicklungen aufgrund von Spezialwünschen des Auftraggebers vorgenommen werden müssen.

7.2. Der Auftragsbearbeiter hat keinen Anspruch auf eine Vergütung von Kosten, die auf der Einhaltung von Anforderungen beruhen, die im DSG festgelegt sind.

8. Bezug zu bestehenden Verträgen

8.1. Die Anlagen zu diesem Vertrag bilden einen integrierenden Bestandteil des vorliegenden Vertrags.

8.2. Steht eine in diesem Vertrag enthaltene Bestimmung im Widerspruch zum Hauptvertrag, gilt die im vorliegenden Vertrag enthaltene Bestimmung als massgeblich, soweit die im Hauptvertrag vorgesehene Bestimmung nicht auf zwingendes Recht beruht, welche weiter geht, als die Bestimmung im vorliegenden Vertrag.

8.3. Die Bestimmungen des vorliegenden Vertrags haben auch nach Beendigung des Hauptvertrags weiterhin Bestand, solange der Auftragsbearbeiter im Besitz von Personendaten des Auftraggebers ist.

9. Haftung

9.1. Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenbearbeitung oder Nutzung im Rahmen der Auftragsbearbeitung erleidet, haften im Innenverhältnis der Auftragsbearbeiter und der Auftraggeber entsprechend ihrem jeweiligen Verursachungs- und Verschuldensanteil. Die Vertragsparteien stellen sich jeweils von der Haftung frei, wenn eine der Vertragsparteien nachweist, dass sie für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, nicht verantwortlich ist.

9.2. Im Übrigen bestimmt sich die Haftung nach dem Gesetz.

10. Schlussbestimmungen

10.1. Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform bzw. der elektronischen Form. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

10.2. Sollten einzelne Bestimmungen dieses Vertrags ganz oder teilweise ungültig sein oder werden, so wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. Die Parteien vereinbaren, die unwirksame Bestimmung durch eine wirksame Bestimmung zu ersetzen, welche dem wirtschaftlichen Sinn und Zweck der unwirksamen Bestimmung am nächsten kommt.

10.3. Dieser Vertrag untersteht Schweizer Recht unter Ausschluss des Internationalen Privatrechts (IPRG). Ausschliesslicher Gerichtsstand für Streitigkeiten aus diesem Vertrag oder im Zusammenhang mit der Auslegung und Anwendung des vorliegenden Vertrags ist der Sitz des Auftragsbearbeiters.

ANLAGEN

Anlage 1: Auftragsspezifizierung
Anlage 2: Technische und organisatorische Massnahmen – Mindestvorkehrungen
Anlage 3: Zugelassene Unterauftragsbearbeiter

Anlage 1: Auftragsspezifizierung

1. Auftragsspezifizierung

1.1. Gegenstand, Art und Zweck der Bearbeitung

Gegenstand, Art und Zweck dieses Auftrags sind im Hauptvertrages geregelt. Sie beinhalten im Wesentlichen die Nutzung von auto-i EXPERT Online, des e-Service4, SilverDAT 3 (inkl. FotoApp), autoValue, motoValue sowie greycardScanner oder in Kombination.

1.2. Dauer der Bearbeitung

Die Dauer der Bearbeitung richtet sich nach dem Hauptvertrag.

1.3. Art der Personendaten

Zur Erfüllung der Aufgaben werden folgende Personendaten bearbeitet:

- **Identifikationsdaten**: Hierzu gehören persönliche Informationen, die eine Person eindeutig identifizieren, wie Name, Geburtsdatum, Geschlecht, Staatsangehörigkeit, Ausweisnummern, Sozialversicherungsnummer, FZ-Kennzeichen, Fotos, usw.
- **Kontaktinformationen**: Diese Kategorie umfasst Daten, die es ermöglichen, mit der betreffenden Person in Kontakt zu treten, wie Adresse, Telefonnummer, E-Mail-Adresse, Notfallkontaktinformationen usw.
- **Finanzdaten**: Hierzu gehören Informationen im Zusammenhang mit Finanzen und Zahlungen, Steueridentifikationsnummern usw.
- Die Liste ist nicht abschliessend

1.4. Kategorien der betroffenen Personen

Die Datenbearbeitung bezieht sich auf folgende Kategorien betroffener Personen:

Kunden, Interessenten, Lieferanten, Ansprechpartner, Beschäftigte usw..

Anlage 2: Technische und organisatorische Massnahmen – Mindestvorkehrungen

Im Folgenden werden die auf Art. 7 und 8 DSG und Art. 3 der neuen Verordnung zum neuen Datenschutzgesetz basierenden technischen und organisatorischen Massnahmen beschrieben, die konkret vom Auftragsbearbeiter im Zusammenhang mit der Bearbeitung der Personendaten und der Erfüllung seiner Verpflichtungen gemäss dem Hauptvertrag einschliesslich diesem Vertrag als Mindestvorkehrungen zu ergreifen sind, um ein dem Risiko angemessenes Schutzniveau hinsichtlich des Datenschutzes und der Datensicherheit der überlassenen Daten zu gewährleisten.

1. Vertraulichkeit

a. Zutrittskontrolle: Anforderung: Schutz vor unbefugtem Zutritt zu Daten-Bearbeitungsanlagen

Der Auftragsbearbeiter gewährleistet die Zutrittskontrolle zu seinen Räumlichkeiten durch geeignete Massnahmen.

Beschreibung der konkreten Massnahmen: Schlüssel, Magnet- oder Chipkarten, elektrische Türöffner, Portier und Alarmanlagen

b. Zugangskontrolle: Anforderung: Schutz vor unbefugter Systembenutzung

Der Auftragsbearbeiter gewährleistet die elektronische Zugangskontrolle durch geeignete Massnahmen.

Mögliche Massnahmen: z.B. Kennwörter, Passwörter (einschliesslich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern.

Beschreibung der konkreten Massnahmen: Kennwörter, Passwörter (einschliesslich entsprechender Policy), Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern.

c. Zugriffskontrolle: Anforderung: kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems

Der Auftragsbearbeiter gewährleistet die Zugriffskontrolle durch geeignete Massnahmen.

Beschreibung der konkreten Massnahmen: z.B. Standard-Berechtigungsprofile auf «Need-to-know-Basis», Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten.

d. Pseudonymisierung

Sofern für die jeweilige Datenbearbeitung möglich, werden die primären Identifikationsmerkmale der Personendaten in der jeweiligen Datenanwendung entfernt und gesondert aufbewahrt.

Beschreibung der konkreten Massnahmen: Automatisierte Pseudonymisierung der Personendaten nach 6 Monaten.

e. Fähigkeit der Systeme und Dienste

Der Auftragsbearbeiter gewährleistet die Fähigkeit der Systeme und Dienste, wonach alle Funktionen des Systems und Dienste zur Verfügung stehen und auftretende Fehlfunktionen gemeldet und behoben werden.

Beschreibung der konkreten Massnahmen: Monitoring der externen Server und Systeme durch Unterauftragsverarbeiter im Auftragsverhältnis. Dasselbe gilt für die internen gehosteten Server und Systeme.

2. Integrität

a. Weitergabekontrolle: Anforderung: kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport

Der Auftragsbearbeiter gewährleistet die Weitergabekontrolle durch geeignete Massnahmen.

Beschreibung der konkreten Massnahmen: z.B. Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur.

b. Eingabekontrolle: Anforderung: Feststellung, ob und von wem Personendaten in Daten-Bearbeitungssysteme eingegeben, verändert oder entfernt worden sind

Der Auftragsbearbeiter gewährleistet die Eingabekontrolle durch geeignete Massnahmen.

Beschreibung der konkreten Massnahmen: Protokollierung, wer, wann, welche Daten eingeben oder ändern darf, Protokollierung von Datenänderungen, Dokumentenmanagement.

3. Verfügbarkeit und Belastbarkeit

a. Verfügbarkeitskontrolle: Anforderung: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust

Der Auftragsbearbeiter gewährleistet die Verfügbarkeit sowie die rasche Wiederherstellbarkeit und das Löschen nach Gebrauch der Daten durch geeignete Massnahmen.

Beschreibung der konkreten Massnahmen: z.B. Back-up-Strategie zwecks Datensicherung und Wiederherstellung (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne; Security-Checks auf Infrastruktur- und Applikationsebene, mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern, Löschungsfristen sowohl für Daten selbst als auch Metadaten wie Logfiles u.Ä.

b. Trennungskontrolle: Anforderung: es muss gewährleistet sein, dass Daten, die für verschiedene Zwecke erhoben wurden, getrennt verarbeitet werden können

Der Auftragsbearbeiter gewährleistet die getrennte Bearbeitung von Daten durch geeignete Massnahmen. Insbesondere müssen zu unterschiedlichen Zwecken erhobene Personendaten getrennt verarbeitet werden.

4. Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

a. Anforderung: regelmässige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Bearbeitung

Der Auftragsbearbeiter gewährleistet die Implementierung eines Verfahrens zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Bearbeitung.

Beschreibung der konkreten Massnahmen: Datenschutzmanagement, einschliesslich regelmässiger Mitarbeiterschulungen; Incident-Response-Management; datenschutzfreundliche Voreinstellungen (Privacy by Design & Privacy by Default), unverzügliche Behebung von entdeckten Mängeln.

b. Auftragskontrolle: Anforderung: keine Auftragsbearbeitung im Sinne von Art. 9 DSG ohne entsprechende Weisung des Auftraggebers

Der Auftragsbearbeiter gewährleistet die Überprüfung der Unterauftragsbearbeiter durch geeignete Massnahmen.

Beschreibung der konkreten Massnahmen: z.B. formalisiertes Auftragsmanagement, strenge Auswahl des Unterauftragsbearbeiters (ISO-Zertifizierung, ISMS), eindeutige schriftliche Vertragsgestaltung mit dem Unterauftragsbearbeiter, Überprüfung der Einhaltung dieser Verträge durch die Unterauftragsbearbeiter, Vorabüberzeugungspflicht, Nachkontrollen.

Anlage 3: Zugelassene Unterauftragsbearbeiter

EveryWare AG
Zurlindenstrasse 52 A
CH-8003 Zürich
Tel.: +41 44 466 60 00
E-Mail: info@everyware.ch

care4IT.ch GmbH
Grubenstrasse 56
CH-8045 Zürich
Tel.: +41 43 388 20 20
E-Mail: info@care4it.ch

Deutsche Automobil Treuhand GmbH
Hellmuth-Hirth-Str. 1
D-73760 Ostfildern
Tel.: +49 711 4503-130
E-Mail: zentrale@dat.de

Logicalis Architects of Change
Siemensstrasse 10
63263 Neu-Isenburg
Tel.: +49 6102 7786 – 0
E-Mail: info@logicalis.de

Anlage 4: Änderungsmanagement

Version	Datum	Autor	Inhalt der Änderungen
1.2024	08.05.24	PAH	Erstellung
2.2024	19.06.24	PAH	1.2. Produktergänzungen um: autoValue, motoValue
			Anlage 1, 1.3.: um Fotos