VERTRAG ÜBER DIE AUFTRAGSVERARBEITUNG (ART. 28 Abs. 3 DSGVO)

1. VERTRAGSGEGENSTAND UND AUFTRAGSINHALT

1.1 Der Gegenstand des Vertrags ergibt sich aus der zwischen den Parteien abgeschlossenen Vereinbarung über die Bereitstellung einer Software zum Zugriff über das Internet (SaaS) und / oder den Kauf eines Fahrzeugscanners zwischen der Instavalo GmbH, Gießerallee 23, 47877 Willich, Deutschland (nachfolgend **„Auftragnehmer“**) und dem Auftraggeber, auf die hier verwiesen wird (nachfolgend **„Hauptvertrag“**). Dieser Vertrag zur Auftragsverarbeitung (nachfolgend der **„Vertrag“**) findet Anwendung auf alle Tätigkeiten, die mit der Auftragsverarbeitung bei der Erbringung von Leistungen gemäß Hauptvertrag in Zusammenhang stehen und bei denen der Auftragnehmer mit personenbezogenen Daten, die dem Auftragnehmer vom Auftraggeber übermittelt oder offengelegt werden, in Berührung kommen kann.

1.2 Die Art der verarbeiteten Daten, die Kategorien betroffener Personen und die Art und der Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind im Detail in Annex 1 zu diesem Vertrag festgelegt.

1.3 Soweit in diesem Vertrag nicht ausdrücklich anders bestimmt, findet die Erbringung der vertraglich vereinbarten Datenverarbeitung ausschließlich in Deutschland, einem Mitgliedstaat der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den europäischen Wirtschaftsraum (EWR) statt. Jede Verlagerung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

2. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

2.1 Der Auftragnehmer hat die Sicherheit gemäß Art. 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. Die einzelnen Maßnahmen dokumentiert der Auftragnehmer in einem Maßnahmenkonzept in Annex 2.

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

2.3 Der Auftragnehmer 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.

3. BERICHTIGUNG, EINSCHRÄNKUNG UND LÖSCHUNG VON DATEN; BETROFFENENRECHTE

3.1 Der Auftragnehmer 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 Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

3.2 Der Auftragnehmer wird den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen darin unterstützen, die Rechte Betroffener auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft sicherzustellen. Für Unterstützungsleistungen, die nach dem Hauptvertrag nicht geschuldet sind, kann der Auftragnehmer eine Vergütung beanspruchen.

4. QUALITÄTSSICHERUNG UND SONSTIGE PFLICHTEN DES AUFTRAGNEHMERS

4.1 Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet worden sind. Der Auftragnehmer darf die Daten ausschließlich

entsprechend der Weisungen des Auftraggebers, einschließlich der in diesem Vertrag und im Hauptvertrag eingeräumten Befugnisse, verarbeiten, es sei denn, dass er gesetzlich zur Verarbeitung verpflichtet ist. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mindestens in Textform). Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

4.2 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32-36 DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören unter anderem:

4.2.1 die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden,

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

4.2.3 die Unterstützung des Auftraggebers bei dessen Datenschutz-Folgeabschätzung.

4.2.4 die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultation mit der Aufsichtsbehörde.

4.3 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung des Hauptvertrags enthalten oder auf ein Fehlverhalten des Auftraggebers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

5. UNTERAUFTRAGSVERHÄLTNISSE

5.1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu ge-

hören Nebenleistungen, die der Auftragnehmer zum Beispiel 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 Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Sicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

5.2 Der Auftragnehmer ist berechtigt, Unterauftragnehmer mit Sitz innerhalb der EU oder des EWR einzuschalten, sofern er mit dem Unterauftragnehmer eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 4 DS-GVO schließt.

5.3 Vorbehaltlich der in Ziffer 5.2 genannten Bedingung gestattet hiermit der Auftraggeber dem Auftragnehmer die Einschaltung der Annex 3 genannten Unternehmen als Subunternehmer.

5.4 Der Auftragnehmer informiert den Auftraggeber vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter. Der Auftraggeber kann dieser Änderung gegenüber dem Auftragnehmer innerhalb von 14 Tagen ab Eingang der Information beim Auftraggeber widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung zur Änderung als gegeben. Ein Widerspruch darf nicht ohne ein die Interessen des Auftragnehmers überwiegendes Interesse des Auftraggebers erfolgen.

6. KONTROLLRECHTE DES AUFTRAGGEBERS

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

6.2 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet

sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

6.3 Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

6.3.1 die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO,

6.3.2 die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO,

6.3.3 aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (zum Beispiel Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditorium, Qualitätsaudit),

6.3.4 eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (zum Beispiel nach BSI-Grundschutz oder ISO/IEC 27001).

6.4 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

7. LÖSCHUNG UND RÜCKGABE VON PERSONENBEZOGENEN DATEN

7.1 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 die Aufbewahrung von Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich ist.

7.2 Nach Abschluss der vertraglich vereinbarten Tätigkeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung des Hauptvertrags – hat der Auftragnehmer 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. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Die Pflichten des Auftragnehmers nach dieser Ziffer 7.2 gelten nicht, sofern nach dem Unionsrecht

oder dem Recht der Mitgliedstaaten der EU eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

7.3 Dokumentationen, die dem Nachweis der auftragsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

8. AUFTRAGSDAUER, KÜNDIGUNG

Die Laufzeit dieses Vertrages entspricht der Laufzeit des Hauptvertrags und schließt darüber hinaus den Zeitraum nach Ende des Hauptvertrags bis zur vollständigen Rückgabe oder Löschung der vom Auftraggeber im Zusammenhang mit der Durchführung des Hauptvertrages dem Auftragnehmer überlassenen Daten ein. Unberührt bleibt das Recht jeder Partei zur Kündigung aus wichtigem Grund.

9. SONSTIGES

9.1 Auf den Vertrag findet deutsches Recht unter Ausschluss der Regeln des internationalen Privatrechts, welche zur Anwendung eines anderen Rechts führen würden, Anwendung.

9.2 Ausschließlicher Gerichtsstand für sämtliche Streitigkeiten aus oder im Zusammenhang mit dem Vertrag ist der Sitz des Auftragnehmers. Der Auftragnehmer ist auch berechtigt, am Sitz des Kunden oder einem sonst zuständigen Gericht zu klagen.

9.3 Mündliche Nebenabreden sind nicht getroffen.

9.4 Sollten einzelne Bestimmungen des Vertrages ganz oder teilweise unwirksam sein oder werden, wird die Wirksamkeit der übrigen Bestimmungen hierdurch nicht berührt. Die Parteien verpflichten sich für diesen Fall, die ungültige Bestimmung durch eine wirksame Bestimmung zu ersetzen, die dem wirtschaftlichen Zweck der ungültigen Bestimmung möglichst nahekommt. Entsprechendes gilt für etwaige Lücken des Vertrages.

Anlagen:

Annex 1: Art und Zweck der Verarbeitung, Gegenstand der Verarbeitung, Art der Daten, Kreis der Betroffenen

Annex 2: Technische und organisatorische Maßnahmen

Annex 3: Unterauftragsverhältnisse

ANNEX 1 – ART UND ZWECK DER VERARBEITUNG, ART DER DATEN, KATEGORIEN DER BETROFFENEN

Betroffene Personen und Personengruppe	Insbesondere: • Nutzer des Services • Mitarbeiter des Kunden
Art der Daten oder Datenkategorien	• Kontaktdaten • Daten über die Nutzung der Software (Protokolldaten)
Empfänger	Auftragnehmer und Unterauftragnehmer
Art und Zweck der Verarbeitung	Bereitstellung einer Software zum Zugriff über das Internet (SaaS); Erbringung von IT-Dienstleistungen und sonstigen Dienstleistungen im Zusammenhang mit der bereitgestellten Software und / oder der Einrichtung und dem Betrieb eines Fahrzeugscanners, insbesondere Supportleistungen

ANNEX 2 - TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

Die folgenden technischen und organisatorischen Maßnahmen werden durch den Auftragnehmer umgesetzt:

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

a) Zutrittskontrolle/Gebäudeabsicherung

Maßnahmen, damit Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, verwehrt wird:

- ☐ Alarmanlage
- ☐ Videoüberwachung
- ☐ Automatisches Zutrittskontrollsystem, Ausweisleser (Magnet-/Chipkarte)
- ☐ Chipkarten / Transpondersysteme
- ☐ Lichtschranken / Bewegungsmelder
- ☐ Manuelles Schließsystem
- ☐ Sicherheitsschlösser
- ☐ Schlüsselregelung
- ☐ Besucher in Begleitung durch Mitarbeiter
- ☐ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Zeiterfassungssystem

b) Zugangskontrolle/Absicherung Systemzugang

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- ☐ Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk einschl. Passwort
- ☐ Autorisierungsprozess für Zugangsberechtigungen
- ☐ Begrenzung der befugten Benutzer

- ☐ Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall)
- ☐ Verwalten von Benutzerberechtigungen
- ☐ Erstellen von Benutzerprofilen
- ☐ Single Sign On der Hüsges One Applikationen
- ☐ Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)
- ☐ Firewall Sophos
- ☐ Einsatz von Intrusion-Detection-Systemen
- ☐ Einsatz von Anti-Viren-Software Server
- ☐ Einsatz von Anti-Viren-Software Clients
- ☐ Einsatz VPN-Technologie bei Remote-Zugriffen
- ☐ Verschlüsselung von Datenträgern in Notebooks, Laptops etc.

c) Zugriffskontrolle/Sicherstellung von Zugriffsberechtigungen

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und das personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- ☐ Einsatz von Berechtigungskonzepten
- ☐ Anzahl der Administratoren auf das „Notwendigste“ reduziert
- ☐ Verwalten der Rechte durch Systemadministrator
- ☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- ☐ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- ☐ Autorisierungsprozess für Berechtigungen
- ☐ Aktenshredder (mindestens Stufe 3, cross cut)
- ☐ Nicht-reversible Löschung von Datenträgern

d) Trennungskontrolle/Maßnahmen zur Zwecktrennung von Daten

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- ☐ Trennung von Produktiv- und Testumgebung
- ☐ Physikalische Trennung (Systeme/Datenbanken/Datenträger)
- ☐ Logische Mandantenfähigkeit relevanter Anwendungen
- ☐ Steuerung über Berechtigungskonzept
- ☐ Keine Produktivdaten in Testsystemen
- ☐ Festlegung von Datenbankrechten

e) Pseudonymisierung und Verschlüsselung

Maßnahmen zu Pseudonymisierung und Verschlüsselung (es ist Sorge zu tragen, dass eine Rückbeziehbarkeit von Daten auf (natürliche) Personen zumindest eingeschränkt ist):

- ☐ Alle Download-/Upload-Verbindungen via Internet sind gesichert durch SSL, SSH oder VPN
- ☐ Gesichertes WLAN

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

a) Weitergabekontrolle/Sicherheit beim Datentransfer

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbedingt gelesen, kopiert verändert oder entfernt werden können und dass überprüft sowie festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- ☐ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☐ Verschlüsselte Datenübermittlung (https, sftp etc.)
- ☐ Protokollierung der Zugriffe und Abrufe

b) Eingabekontrolle/Sicherheit beim Datentransfer

Maßnahmen, die gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind:

- ☐ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- ☐ Übersicht, mit welchen Applikationen/Programmen welche Daten eingegeben, geändert und gelöscht werden können
- ☐ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzeptes
- ☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☐ Klare Zuständigkeiten für Löschungen

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

a) Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- ☐ Backup & Recovery-Konzept
- ☐ Kontrolle des Sicherungsvorgangs
- ☐ Bedarfsgerechtes Einspielen von Sicherheits-Updates
- ☐ Getrennte Partitionen für Betriebssysteme und Daten
- ☐ Einsatz einer unterbrechungsfreien Stromversorgung (USV)
- ☐ Feuer- und Rauchmeldeanlagen
- ☐ Feuerlöscher Serverraum
- ☐ Klimatisierter Serverraum
- ☐ Schutzsteckdosenleisten Serverraum
- ☐ Spiegeln von Festplatten (Raid-System)
- ☐ Keine sanitären Anschlüsse im oder oberhalb des Serverraums

b) Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Maßnahmen, die gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können sowie Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden:

- ☐ Wiederherstellung nach Backup- und Recovery-Konzept
- ☐ Testen von Datenwiederherstellung
- ☐ Ausreichende Kapazität von IT-Systemen und Anlagen
- ☐ Resilienz und Fehler-Management

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

a) Datenschutz-Management

- ☐ Die Grundsätze zum Datenschutz sind einer unternehmensinternen Richtlinie festgelegt
- ☐ Es ist ein Datenschutzbeauftragter schriftlich bestellt
- ☐ Verpflichtung der Mitarbeiter auf das Datengeheimnis
- ☐ Verpflichtung der Mitarbeiter auf das Fernmeldegeheimnis
- ☐ Verpflichtung der Mitarbeiter auf das Sozialgeheimnis
- ☐ Der DSB ist bei der Datenschutzfolgenabschätzung eingebunden
- ☐ Der DSB ist im Organigramm eingebunden
- ☐ Schulung Datenschutz und Datensicherheit von Mitarbeitern
- ☐ Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird regelmäßig durchgeführt
- ☐ Die Organisation kommt den Informationspflichten nach Art. 13 und Art. 14 DS-GVO nach
- ☐ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
- ☐ Es werden Verzeichnisse von Verarbeitungstätigkeiten nach Art. 30 DS-GVO geführt
- ☐ Regelmäßige Datenschutzaudits des Datenschutzbeauftragten

b) Incident-Response-Management (Störungsfallmanagement)

- ☐ Erstellung eines Plans zum Umgang bei Störungen
- ☐ Einsatz von Firewall und regelmäßige Aktualisierung
- ☐ Einsatz von Spamfilter und regelmäßige Aktualisierung
- ☐ Einsatz von Virenscanner und regelmäßige Aktualisierung
- ☐ Intrusion Detection System (IDS)
- ☐ Intrusion Prevention System (IPS)
- ☐ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/Datenpannen (auch im Hinblick auf die Meldepflicht gegenüber Aufsichtsbehörde)
- ☐ Einbindung des Datenschutzbeauftragten in Sicherheitsvorfällen und Datenpannen

c) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO) - Privacy by design / Privacy by default

- ☐ Beachtung privacy by design (Datenschutz) durch Technikgestaltung
- ☐ Beachtung privacy by default durch datenschutzfreundliche Voreinstellungen
- ☐ Auswahl datenschutzfreundlicher Technologie bei der Beschaffung
- ☐ Es werden nicht mehr personenbezogene Daten erhoben als für den jeweiligen Zweck erforderlich sind
- ☐ Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen

d) Auftragskontrolle

Keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers

- ☐ Auswahl der Auftragsverarbeiter unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- ☐ Schriftlich dokumentierte Weisungen an den Auftragsverarbeiter
- ☐ Auftragsverarbeiter hat Datenschutzbeauftragten bestellt
- ☐ Wirksame Kontrollrechte gegenüber dem Auftragsverarbeiter vereinbart

- ☐ Vorherige Prüfung und Dokumentation der beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen
- ☐ Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf die Vertraulichkeit
- ☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☐ Laufende Überprüfung des Auftragsverarbeiters und seiner Tätigkeiten

ANNEX 3 – UNTERAUFTRAGSVERHÄLTNISSE

Name des Subunternehmens	Anschrift	Beschreibung der Leistungen
Webhoster.de AG	Zum Haunert 22 DE-59519 Möhnesee	Serverhosting
Sms.at mobile internet services gmbh	Klosterwiesgasse 101b/Ge01 AT-8010 Graz	SMS-Versand
ProfiMasking Bildbearbeitungsservice	Föhrenstrasse 33 DE-90530 Wendelstein	Bildaufbereitung
NOEMIX Germany GmbH	Mettlacher Straße 5 DE-81379 München	Softwarehosting
DAT – Deutsche Automobil Treuhand GmbH	Helmut-Hirth-Str. 1 DE-73760 Ostfildern	Fahrzeugdaten
LOX24 GmbH	Seestr. 109 DE-13353 Berlin	SMS-Versand