Auftragsverarbeitungsvertrag
gemäß Art. 28 DSGVO (Datenschutz-Grundverordnung)

Mit dem Annehmen der PlanApp Nutzungsbedingungen schließt der Auftraggeber gem. § 4 Abs. 4 den nachfolgenden, von der PlanAPP GmbH verbindlich zur Annahme durch den Auftraggeber angebotenen Auftragsverarbeitungsvertrag zur Verarbeitung personenbezogener Daten mit der

PlanAPP GmbH
Imkerstr. 5
30916 Isernhagen

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

§ 1 Vertragsgegenstand

Gegenstand dieses Vertrages ist die Verarbeitung personenbezogener Daten (nachstehend „Daten" genannt) durch den Auftragnehmer für den Auftraggeber in dessen Auftrag und nach dessen Weisung. Die Beauftragung durch den Auftraggeber wird durch den zugrunde liegenden Hauptvertrag bestimmt. Die konkreten Verarbeitungstätigkeiten, insbesondere die Art der Daten, der Zweck der Datenverarbeitung und -nutzung, sowie der Kreis der Betroffenen sind in **Anlage 1** festgelegt.

§ 2 Verantwortlichkeit

(1) Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen, insbesondere für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der Betroffenen gem. Art. 12 bis 22 DSGVO allein verantwortlich.

(2) Der Auftraggeber und der Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich und vollständig, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

§ 3 Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten auf dokumentierte Weisung des Auftraggebers. Ausgenommen hiervon sind Sachverhalte, in denen dem Auftragnehmer eine Verarbeitung aus zwingenden rechtlichen Gründen auferlegt wird. Der Auftragnehmer unterrichtet soweit ihm möglich in derartigen Situationen den Auftraggeber vor Beginn der Verarbeitung über die entsprechenden rechtlichen Anforderungen.

(2) Die Weisungen werden anfänglich durch den Haupt- und Auftragsverarbeitungsvertrag festgelegt und können vom Auftraggeber danach in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden. Ein wesentlicher Zweck der Verarbeitung, den Vergleich von anonymisierten betriebswirtschaftlichen Daten (insb. Gewinn- und Verlustrechnung, betriebswirtschaftlichen Auswertungen, ggf. ergänzenden Bilanzdaten / Kennziffern) mit anderen Marktteilnehmern zu ermöglichen, kann nur erfolgen, indem diese relevanten Daten vom Auftragnehmer anonymisiert, ausgewertet, ggf. aggregiert und dem Auftraggeber sowie anderen zur Verfügung gestellt werden. Diese Weisung gilt als dokumentiert erteilt, sofern datenschutzrechtlich erforderlich.

(3) Auf anonymisierte Daten findet dieser Auftragsverarbeitungsvertrag keine Anwendung.

(4) 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 solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

§ 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutzfolgenabschätzungen und vorherigen Konsultationen der zuständigen Aufsichtsbehörde.

(2) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten Befugten zur Vertraulichkeit verpflichtet haben. Die Vertraulichkeits- / Verschwiegenheitspflicht besteht auch nach Beendigung des Vertrages fort.

(3) Der Auftragnehmer verpflichtet sich, den Auftraggeber angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Person zu unterstützen, ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen und Anfragen von Betroffenen unverzüglich an den Auftraggeber weiterzuleiten.

(4) Bestellung eines externen Datenschutzbeauftragten:
Thomas Althammer, c/o Althammer & Kill GmbH & Co. KG
Roscherstraße 7, 30161 Hannover, E-Mail kontakt-dsb@althammer-kill.de

(5) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

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

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

(8) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

§ 5 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung, zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO 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 DSGVO zu berücksichtigen. Die Festlegung des Schutzniveaus obliegt dem Auftraggeber und wird anhand der Kriterien in **Anlage 2** festgelegt.

(3) 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.

§ 6 Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebendienstleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/ Transportdienstleistungen, Architekten oder Planungsbüros, (IT-) 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 Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen.

(2) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung zum Einsatz neuer Unterauftragnehmer. Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind die in der **Anlage 1** aufgeführten Unternehmen als Unterauftragnehmer für den Auftragnehmer tätig. Für diese Unterauftragnehmer gilt die Zustimmung für das Tätigwerden als erteilt.

(3) Werden neue Unterauftragnehmer eingesetzt, so informiert der Auftragnehmer den Auftraggeber, wodurch dieser die Möglichkeit erhält, begründet Einspruch einzulegen.

(4) Die Verarbeitung von Daten des Auftraggebers außerhalb der EU/EWR darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(5) Der Auftragnehmer muss Unterauftragnehmer unter besonderer Berücksichtigung der Eignung hinsichtlich der Erfüllung der zwischen Auftraggeber und Auftragnehmer vereinbarten technischen und organisatorischen Maßnahmen gewissenhaft auswählen. Diesem werden im Wege eines Vertrags im Wesentlichen dieselben Pflichten auferlegt, die in dieser Vereinbarung zwischen dem Auftraggeber und dem Auftragnehmer festgelegt sind, insbesondere hinsichtlich der Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit. Hierbei müssen ferner hinreichend Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt.

§ 7 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unter dem Aspekt ausgewählt, dass dieser hinreichende Garantien dafür bietet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder im Einzelfall durch zu benennende Prüfer durchführen zu lassen.

(1) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers 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.

(2) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- ☒ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- ☒ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- ☒ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter);
- ☒ eine geeignete Zertifizierung (z.B. gem. ISO 27001 oder ISO27701).

§ 8 Kopien, Vertragsbeendigung und Löschung von Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt und sind untersagt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung und IT-Sicherheit erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglichen Arbeiten – oder früher nach Aufforderung durch den Auftraggeber – hat der Auftragnehmer alle im Rahmen des Auftrags in seinen Besitz gelangte Unterlagen oder Datenträger sowie Daten dem Auftraggeber auszuhändigen oder auf Anweisung des Auftraggebers datenschutzkonform zu löschen bzw. zu vernichten, sofern keine gesetzliche Pflicht zur Aufbewahrung besteht.

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

(4) Sofern zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten entstehen, bedarf es einer vorherigen Vereinbarung (mindestens Textform) über die Kostentragung.

§ 9 Zurückbehaltungsrecht

Die Einrede des Zurückbehaltungsrechts, gleich aus welchem Rechtsgrund, an den vertragsgegenständlichen Daten sowie an evtl. vorhandenen Datenträgern wird ausgeschlossen.

§ 10 Laufzeit und Kündigung

(1) Dieser AVV kommt automatisch mit der Antragsannahme des Hauptvertrags durch den Auftraggeber verbindlich zustande, er ist ohne separate Unterschrift gültig.

(2) Die unten aufgeführten Anlagen sind zwingender Vertragsbestandteil.

(3) Die Laufzeit richtet sich nach dem zugrundliegenden Hauptvertrag. Er kann nicht separat gekündigt werden. Soweit nach Beendigung dieses Vertrages noch Verarbeitungen notwendig sein sollten, beispielsweise Übermittlungen an den Auftraggeber, so gilt die Laufzeit automatisch bis zur vollständigen Beendigung aller Verarbeitungsvorgänge. Kündigungen bedürfen zu ihrer Wirksamkeit der Schriftform.

(4) Nebenabreden bestehen nicht. Solche müssen grundsätzlich in Schriftform separat vereinbart werden.

(5) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

- Anlage 1: Zweck, Art der Daten und Betroffenen, Dienstleister
- Anlage 2: Technische und organisatorische Maßnahmen

Anlage 1: Zweck, Art der Daten und Betroffenen, Dienstleister

Art und Zweck der Verarbeitung:	
Zur Verfügungstellung der Webapp www.planapp.de als spezialisierte Software für Autohaus-Controlling, Planung und Benchmarking auf Basis eines Hauptvertrags, geregelt in Nutzungs- und Teilnahmebedingungen sowie Leistungsbeschreibungen.	
Art der Daten	**Kategorien der Betroffenen**
Kontakt- und Stammdaten, Zugangsdaten Sofern als personenbezogen geltend: buchhaltungsrelevante Daten	Auftraggeber (sofern Betroffener i.S.d. DSGVO), Mitarbeitende, Ansprechpartner, Kunden und Lieferanten des Auftraggebers, sofern relevant.

Nr.	**Name des Unterauftragnehmers**	**Ort der Leistungserbringung**	**Art der Dienstleistung**
1	EDV Systemhaus GmbH & Co. KG, 31303 Burgdorf	Deutschland / Großbritannien	Unterstützung IT; Bereitstellung dbc-Cloud Lösung
2	AKRA GmbH, 20095 Hamburg	Deutschland	Programmierung und Entwicklung

Anlage 2: Technische und organisatorische Maßnahmen

PlanAPP wird gehostet bei der DATEV eG, betreut von der EDV.de Systemhaus GmbH & Co. KG. Die DATEV eG ist zertifiziert nach DIN EN ISO / IEC 27001:2017 und DIN EN ISO /IEC 27701:2019. Nähere Informationen zu den technischen und organisatorischen Schutzmaßnahmen der DATEV: https://apps.datev.de/help-center/documents/1000562.

1. Vertraulichkeit gem. Art. 32 Abs. 1 DSGVO

Zutrittskontrolle

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Einbruchmeldeanlage	☒ Schlüsselregelung / -liste / -verwaltung
☒ Biometrische Zugangssperren	☒ Empfang / Rezeption / Pförtner
☒ Chipkarten / Transpondersysteme	☒ Besucherbuch / Protokoll der Besucher
☒ Manuelles Schließsystem	☒ Besucherausweise
☒ Sicherheitsschlösser	☒ Besucher nur in ständiger Begleitung
☒ Türen mit Knauf an Außenseite	☒ Sorgfalt bei Auswahl Reinigungsdienste
☒ Klingelanlage	☒ Zoneneinteilung der Gebäude
☒ gesicherter Serverraum	☒ Besucherbereich
☒ Zugangsregelung zu sensiblen Räumen	☒ Interner Bereich
	☒ Zutrittsberechtigungskonzept

Zugangskontrolle

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Login mit Benutzername + Passwort	☒ Benutzerberechtigungskonzept
☒ Anti-Viren-Software Server	☒ Verwalten von Benutzerprofilen (Regelung)
☒ Anti-Virus-Software Clients	☒ Richtlinie „Sicheres Passwort“
☒ Firewall-System	
☒ Intrusion Detection Systeme	
☒ BIOS Schutz (separates Passwort)	
☒ Protokollierung von An-, Abmeldungen	
☒ Server-Racks verschließbar	
☒ Netzwerktrennung Produktivsystem, Test-systeme, (Maschinensteuerung)	

Zugriffskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Aktenschredder (mind. Stufe 3, cross cut)	☒ Berechtigungskonzept-, (Roll Based) ☒ Rollen-, ☒ Funktionsbasiert
☒ Physische Löschung / Vernichtung von Datenträgern	☒ Zugriffskonzept (bedarfsgerecht) ☒ Verzeichnisse ☒ Anwendungsprogramme
	☒ Checkliste für Mitarbeiteraustritt
	☒ Minimale Anzahl an Administratoren

Trennungskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Trennung von Produktiv- und Test-umgebung	☒ Steuerung über Berechtigungskonzept
☒ Logische Trennung (Systeme / Datenbanken / Datenträger)	☒ Festlegung von Datenbankrechten
☒ Mandantenfähigkeit relevanter Anwendungen	

Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Technische Maßnahmen	Organisatorische Maßnahmen
	☒ Wo immer es möglich und wirtschaftlich oder rechtlich sinnvoll bzw. geboten ist, werden Daten/ Auswertungen pseudonymisiert oder anonymisiert

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

Weitergabekontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
☒ E-Mail-Verschlüsselung	☒ Weitergabe in anonymisierter oder pseudonymisierter Form
☒ Einsatz von VPN	☒ Sorgfalt bei Auswahl von Transportpersonal und Fahrzeugen
☒ Missbrauchsschutz von USB-Schnittstellen durch Sperrung der USB-Ports für Datenträger	
☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	

Eingabekontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
	☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Feuer- und Rauchmeldeanlagen	☒ Backup & Recovery-Konzept
☒ Feuerlöscher Serverraum (CO_2 Löscher)	☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☒ Serverraumüberwachung Temperatur und Feuchtigkeit	☒ Keine sanitären Anschlüsse im oder oberhalb des Serverraums
☒ Serverraum klimatisiert	
☒ Einsatz virtueller Server	
☒ Server-Cluster für virtuelle Umgebung	
☒ RAID System / Festplattenspiegelung	
☒ Netzwerk-Storage im Einsatz (SAN)	
☒ Einsatz/Nutzen von Cloud-Systemen in externen Rechenzentren	
☒ Datensicherung	

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

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Ersatz-Festplatten für Server, SAN-Systeme	☒ Es werden Ersatzsysteme (Hardware) vorgehalten
☒ Jederzeit eine „aktuelle“ Datensicherung (Tag/Woche/Monat)	☒ Restorekonzept inkl. wichtiger Telefonnummern die im Bedarfsfall benötigt werden (Notfallkontakt)
	☒ Regelmäßige Kontrollen und Trainings zur System- und Datenwiederherstellung

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

Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Intranet etc.)	☒ Externer Datenschutzbeauftragter Thomas Althammer, Althammer & Kill GmbH & Co.KG, Roscherstr. 7, 30162 Hannover, Kontakt-dsb@althammer-kill.de
	☒ Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
	☒ Regelmäßige Sensibilisierung der Mitarbeiter (mindestens 1x jährlich)
	☒ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach

Incident-Response-Management

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von Firewall und regelmäßige Aktualisierung	☒ Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde- 72 h)
☒ Einsatz von Spamfilter und regelmäßige Aktualisierung	☒ Einbindung von DSB in Datenpannen
☒ Einsatz von Virenscanner und regelmäßige Aktualisierung	☒ Dokumentation Datenpannen
☒ regelmäßige Sensibilisierung der Mitarbeiter in Datenschutz bzw. Datensicherheit	☒ Prozess und Verantwortlichkeiten zur Nachbearbeitung von Datenpannen

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Es werden nicht mehr personen-bezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	☒ Software und Hardware ist von Grund auf so konzipiert und entwickelt, dass relevante Datenschutzmaßnahmen von Anfang an berücksichtigt werden
☒ Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maß-nahmen	☒ Einhaltung der Datenschutzgrundsätze ☒ Datenminimierung, ☒ Garantien zur sicheren Verarbeitung
☒ Benutzerfreundliche Einstellmöglich-keiten zum Schutz ihrer Privatsphäre (Cookie- und Tracking-Einsatz)	

Auftragskontrolle (Outsourcing an Dritte)

Technische Maßnahmen	Organisatorische Maßnahmen
	☒ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (in Bezug auf Datenschutz und Datensicherheit)
	☒ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung
	☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis /Fernmeldegeheimnis
	☒ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
	☒ Regelung zum Einsatz weiterer Subunternehmer
	☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
	☒ geeignete Garantien bei Auftragsverarbeitung in einem Drittland