Datenschutzvereinbarung nach Art. 28 DSGVO

über die Erbringung von IT-Dienstleistungen

zwischen

_____
_____
_____

- Verantwortlicher im Sinne der DSGVO, nachfolgend „Auftraggeber“ genannt -

und

LACOS Computerservice GmbH
Industriestraße 9
07937 Zeulenroda-Triebes

- Auftragsverarbeiter im Sinne der DSGVO, nachfolgend „Auftragnehmer“ genannt –

Präambel

Dieser Auftragsverarbeitungs-Vertrag („Vertrag“) enthält nach dem Willen der Parteien und insbesondere des Auftraggebers den Auftrag zur Auftragsverarbeitung und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung gemäß Art. 28 DSGVO. Er findet Anwendung auf alle Tätigkeiten, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Empfänger Zugang zu personenbezogenen Daten des Auftraggebers haben.

§ 1 Gegenstand, Art und Zweck der Verarbeitung

A. Art der Verarbeitung

Der Auftragnehmer stellt dem Auftraggeber eine Instanz der Web-Applikation LC:FLEETNAV-Web zum Flottenmanagement von Fahrzeug- und Landmaschinen zur Verfügung (SaaS) und leistet diesbzgl. Support.
(1) Bereitstellung, Pflege und Wartung LC:FLEETNAV-Web
(2) Support und Administration LC:FLEETNAV-Web

B. Gegenstand des Vertrags ist die Erbringung folgender Leistungen durch den Auftragnehmer bezüglich folgender Kategorien personenbezogener Daten und betroffener Personen:

Nr.	Gegenstand und Zweck der Verarbeitung	betroffene Personen	Kategorien personenbezogener Daten
1,2	Erheben, Erfassen, Organisation, Ordnen, Speicherung, Auslesen, Abfragen, Bereitstellung, Einschränken, Löschen oder Vernichtung personenbezogener Daten im Rahmen von Bereitstellung, Wartung, Pflege, Support und Administration LC:FLEETNAV-Web	Beschäftigte des Auftraggebers	• Unternehmensdaten: z.B. Betriebsname, Standort, Kontaktdaten zur Benachrichtigung • Fahrzeug- oder Maschineninformationen: z.B. Fabrikat, Modell bzw. Typ, Arbeitsbreite, hinterlegte Wartungsintervalldaten • GPS-basierte Arbeitszeitdaten: z.B. Park-, Transport-, Feld-, Standzeiten und ggf. zurückgelegte Strecke, kartierte Fahrspuren, Standortdaten je Fahrzeug oder Maschine • GPS-basierte Schlagdaten: z.B. hochgeladene Schläge des Kunden als GPS-Polygone, Schlagbezeichnung, Flächengröße, Mapping der Schläge in Karte, weitere zugewiesene Eigenschaften, festgelegte Geofencegebiete für bestimmte Fahrzeuge- oder Maschinen • Nutzerprofildaten: z.B. Benutzername, Name und Email-Adresse des angelegten Nutzers und zugewiesene Rolle sowie Passworthash

			• Telemetriegerätedaten: z.B. Seriennummer, eSIM-Nummer, zugeordneter Maschinentyp, Signalstärke und Statusdaten der Telemetrieeinheit, Konfiguration bzw. Modi LC:TRACKER

§ 2 Dauer des Vertrags:

(1) Dieser Vertrag beginnt mit der beiderseitigen Unterzeichnung und endet mit der Beendigung des Hauptvertrages, beziehungsweise der vollständigen Erbringung aller nach Maßgabe des Hauptvertrages zu erbringenden Leistungen des Auftragnehmers.

(2) Das Recht zur außerordentlichen Kündigung bleibt hiervon unberührt.

§ 3 Weisungsgebundenheit des Auftragnehmers

(1) Der Auftragnehmer verarbeitet die personenbezogenen Daten des Auftraggebers ausschließlich im Rahmen der vereinbarten Leistungserbringung und nur auf dokumentierter Weisung, auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Vom Vertragsgegenstand abweichende Weisungen wird der Auftraggeber oder dessen Bevollmächtigter, schriftlich per Brief, Fax oder E-Mail erteilen. Mündliche Weisungen bestätigt der Auftragnehmer unverzüglich (mind. Textform).

(3) Eine Berichtigung, Löschung oder eine Einschränkung der Verarbeitung ist dem Auftragnehmer nicht gestattet, es sei denn, es liegt eine entsprechende schriftliche Weisung des Auftraggebers vor. Der Auftragnehmer wird keine Auskunftsverlangen betroffener Personen bezüglich der vertragsgegenständlichen Verarbeitungen beantworten, sondern jedes Auskunftsverlangen unverzüglich an den Auftraggeber weiterleiten.

§ 4 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DSGVO zu beachten; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

i. Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DSGVO ausübt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

ii. Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO ist sicherzustellen. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

iii. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten im Anhang „technische und organisatorische Maßnahmen des Auftragnehmers (TOM)“].

iv. Ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 zu führen soweit gesetzlich gefordert ist.

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

vi. 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.

vii. 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.

viii. 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.

ix. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 6 dieses Vertrages.

§ 5 Haftung

(1) Auftraggeber und Auftragnehmer haften für den Schaden, der durch eine nicht der DSGVO entsprechende Verarbeitung verursacht wird gemeinsam im Außenverhältnis gegenüber der jeweiligen betroffenen Person.

(2) Der Auftragnehmer haftet ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der

i. er den aus der DSGVO resultierenden und speziell für Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist oder
ii. er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers handelte oder
iii. er gegen die rechtmäßig erteilten Anweisungen des Auftraggebers gehandelt hat.

(3) Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff auf den Auftragnehmer vorbehalten.

(4) Im Innenverhältnis zwischen Auftraggeber und Auftragnehmer haftet der Auftragnehmer für den durch eine Verarbeitung verursachten Schaden jedoch nur, wenn er

i. seinen ihm speziell durch die DSGVO auferlegten Pflichten nicht nachgekommen ist oder
ii. unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers oder gegen diese Anweisungen gehandelt hat.

(5) Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

§ 6 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer im erforderlichen Umfang zu kontrollieren oder die Kontrollen durch im Einzelfall zu benennende Prüfer durchführen zu lassen.

(2) Der Auftragnehmer ist verpflichtet, diese Kontrollen zu dulden. Der Auftragnehmer wird auf Anfragen des Auftraggebers unverzüglich auf den konkreten Einzelfall bezogene Auskunft erteilen und bei Kontrollen die Einhaltungen dieses Vertrages auf Aufforderung durch geeignete Nachweise belegen.

(3) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(4) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist zu den jeweils üblichen Geschäftszeiten die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers bzw. Unterauftragnehmers vornehmen, in der die einzelne Auftragsverarbeitung durchgeführt wird. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang erfolgen.

§ 7 Informationspflichten

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, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

(1) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;

(2) die Verpflichtung, im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten des Auftraggebers oder anderen Verletzungen personenbezogener Daten dem Auftraggeber unverzüglich Meldung darüber zu erstatten;

(3) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen zur Verfügung zu stellen;

(4) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung;

(5) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

§ 8 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 Nebenleistungen, die der Auftragnehmer z.B. 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 Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragnehmer) ohne vorherige gesonderte Genehmigung des Auftraggebers beauftragen.

(3) Die Auslagerung auf Unterauftragnehmer oder der Wechsel bestehender Unterauftragnehmers sind zulässig, soweit:

i. der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
ii. der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
iii. eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

(4) Der Einspruch gegen die beabsichtigte Änderung ist innerhalb von 4 Wochen nach Zugang der Information über die Änderung gegenüber dem Auftragnehmer zu erheben. Im Fall des Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder - sofern die Erbringung der Leistung ohne die beabsichtigte Änderung dem Auftragnehmer nicht zumutbar ist - die von der Änderung betroffene Leistung gegenüber dem Auftraggeber innerhalb von 4 Wochen nach Zugang des Einspruchs kündigen.

(5) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zu:

Nr.	Name und Anschrift weiterer Auftragnehmer	Beschreibung der Teilleistungen	Ort der Leistungserbringung
-	-	-	-

(6) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(7) Der Auftraggeber ist berechtigt, beim Auftragnehmer Einsicht in dessen Verträge über die Auftragsverarbeitung zu nehmen und vom Auftragnehmer die Übersendung einer Kopie dieser Verträge zu verlangen.

(8) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden und diesbezüglich Vor-Ort-Kontrollen zu dulden sind.

(9) Eine Verlagerung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DSGVO erfüllt sind. Das angemessene Schutzniveau wird hergestellt durch Standardvertragsklauseln und bedarf der vorherigen Zustimmung des Auftraggebers. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

§ 9 Festlegung der technischen und organisatorischen Maßnahmen

(1) Der Auftragnehmer gewährleistet die Umsetzung der im Rahmen der ordnungsgemäßen Durchführung des Auftragsgegenstands erforderlichen Sicherheitsmaßnahmen. Er trifft geeignete technische und organisatorische Maßnahmen zum angemessenen Schutz der personenbezogenen Daten, die den Anforderungen der Datenschutz-Grundverordnung, insbesondere Art. 32 DSGVO, genügen. Hierzu wird der Auftragnehmer:

i. die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen,
ii. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, sicherstellen sowie
iii. die in der Anlage zu dieser Vereinbarung abgebildeten Maßnahmen treffen.

(2) Der Auftragnehmer unterhält ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(3) Die erforderlichen 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 und dem Auftraggeber mitzuteilen.

(4) Dem Auftraggeber sind die vom Auftragnehmer ergriffenen technischen und organisatorischen Maßnahmen bekannt. Der Auftraggeber trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

(5) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

Er trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Gefährdung für die Rechtsgüter der betroffenen Personen erforderliche technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(6) Der Auftragnehmer wird alle getroffenen technischen und organisatorischen Maßnahmen zu den in § 1 genannten Verarbeitungen im Anhang „technische und organisatorische Maßnahmen des Auftragnehmers“ zu diesem Vertrag wahrheitsgemäß angeben. Er wird die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse gewährleisten.

§ 10 Nebenverpflichtung

(1) Der Auftragnehmer sichert dem Auftraggeber die unmittelbare ordnungsgemäße Vernichtung nicht benötigten Datenmaterials zu (Probeausdrucke, überzählige Listen, etc.).

(2) Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Vorgaben verarbeitet werden müssen.

(3) Der Auftragnehmer wird vor Vertragsschluss dem Auftraggeber einen Ansprechpartner benennen.

§ 11 Verpflichtung über das Vertragsende hinaus

(1) Nach Abschluss der vertraglich vereinbarten Arbeiten 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, sofern nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

(2) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen 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.

(3) Die Vertragsparteien sind verpflichtet, auch über das Ende des Vertragsverhältnisses hinaus Stillschweigen über die im Zusammenhang mit dem Auftrag bekannt gewordenen Daten zu wahren und diese nicht ohne schriftliche Zustimmung zu verwerten.

§ 12 Sonstiges, Allgemeines

(1) Änderungen und Ergänzungen dieses Vertrages und aller seiner Bestandteile einschließlich etwaiger Zusicherungen des Auftragnehmers bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf das Formerfordernis.

(2) Sollten sich einzelne Bestimmungen dieses Vertrags ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrags im Ganzen hiervon unberührt.

(3) An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

(4) Für sämtliche Rechtsstreitigkeiten zwischen den Parteien obliegt die Wahl des Gerichtsstands dem Auftragnehmer.

_____, den _____ Zeulenroda-Triebes, den _____

_____ _____

Auftraggeber *Auftragnehmer*
_____ LACOS Computerservice GmbH

Anhang

Technische und organisatorische Maßnahmen des Auftragnehmers (TOM)

1. Vertraulichkeit

>> Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen des Auftragnehmers:

- Manuelles Schließsystem
- Personenkontrolle beim Empfang
- Einbruchmeldeanlage
- Videoüberwachung Geschäftsstelle Außenbereich
- Sorgfältige Auswahl von Reinigungspersonal

>> Zugangskontrolle

Keine unbefugte Benutzung der Systeme des Auftragnehmers:

- Erstellen von Benutzerprofilen gemäß zugewiesener Aufgaben
- Zuordnung von Benutzerrechten
- Authentifikation mit Benutzername / Passwort
- Verwendung von Passwörtern bezüglich Länge und Komplexität entsprechend IT-Sicherheitsrichtlinien
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Verschlüsselung von Datenträgern in Laptops
- Einsatz einer Hardware-Firewall
- Bildschirmsperre mit Passwortaktivierung

>> Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb der Systeme des Auftragnehmers:

- differenzierte Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen
- Verwaltung der Rechte durch die Geschäftsleitung
- Reduzierung der Administratorenrollen und deren Nutzung auf das „Notwendigste“
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf kritische Unternehmensanwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten, soweit technisch möglich
- ordnungsgemäße Vernichtung von Datenträgern
- Protokollierung der Vernichtung

>> Trennungskontrolle
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden in Systemen des Auftragnehmers:

- die Daten des Auftraggebers werden, soweit es technisch möglich ist, getrennt von den Daten anderer Kunde des Auftragnehmers gehalten

>> Pseudonymisierung
Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

- nicht im Aufgabenbereich des Auftragnehmers

2. Integrität

>> Weitergabekontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport aus Systemen des Auftragnehmers heraus:

- Authentifizierung erfolgt verschlüsselt
- grundsätzlich erfolgt Transportsicherung von Datenträgern soweit geboten
- Verschlüsselung entsprechend dem Stand der Technik

>> Eingabekontrolle
Feststellung, ob und von wem personenbezogene Daten in Systemen eingegeben, verändert oder entfernt worden sind:

- Protokollierung der Aktivitäten

3. Verfügbarkeit und Belastbarkeit

>> Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust von Daten in Systemen des Auftragnehmers:

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Backup- & Recoverykonzept
- Testen von Datenwiederherstellung
- Notfallplan
- Datensicherung an einem externen Standort
- Serverräume nicht unterhalb von Räumen mit sanitären Anlagen

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der TOM

>> Datenschutz-Management

- Regelmäßige Überprüfung der Wirksamkeit der technischen und organisatorischen Schutzmaßnahmen
- Regelmäßige Datenschutzschulung Beschäftigte
- Datenschutzleitlinie und Arbeitsanweisung Wahrung Betroffenenrechte informiert Beschäftigte über DSGVO-Anforderungen

>> Incident-Response-Management;

- Arbeitsanweisung zur Erkennung und Meldung von Sicherheitsvorfällen / Datenschutzverletzungen (auch im Hinblick auf Melde- und Benachrichtigungspflicht)
- Dokumentation von Sicherheitsvorfällen / Datenschutzverletzungen
- Dummynutzerkonto zur Alarmierung bei Mißbrauch nach einem breach

>> Auftragskontrolle

- Keine Auftragsverarbeitung ohne entsprechende Weisung des Auftraggebers
- eindeutige und Art.28 DSGVO konforme Vertragsgestaltung
- formalisiertes Auftragsmanagement (Ticketsystem)
- strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht