

## Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

### 1. Gegenstand und Dauer des Vertrags

#### (1) Gegenstand

Der Auftragsverarbeiter erbringt für den Verantwortlichen Leistungen im Bereich des digitalen Fuhrpark- und Fahrzeugmanagements. Die Verarbeitung personenbezogener Daten erfolgt insbesondere zur Bereitstellung, zum Betrieb und zur Unterstützung folgender Produkt- und Leistungsbereiche:

#### a) SMR (Service, Maintenance & Repair) / Wartung und Verschleiß

- Planung, Steuerung und Dokumentation von Inspektionen, Wartungen und Verschleißmaßnahmen
- Abwicklung und Dokumentation von UVV-Prüfungen
- Abwicklung und Dokumentation von HU-/AU-Terminen
- Kommunikation und Statusmeldungen im Rahmen der Auftragsabwicklung

#### b) Leasingrückgaben / Rückgabeprozesse

- Organisation, Terminierung und Dokumentation von Leasingrückgaben
- Verarbeitung und Bereitstellung von leasingbezogenen Vertrags- und Rückgabedaten
- Kommunikation und Statusmeldungen im Rahmen des Rückgabeprozesses

#### (2) Dauer

Die Dauer dieses Vertrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

### 2. Konkretisierung des Vertragsinhalts

#### (1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter erfolgt ausschließlich zu folgenden Zwecken:

- Betrieb und Bereitstellung der vom Verantwortlichen beauftragten Module/Produkte (SMR, Leasingrückgaben, Schadenmanagement, Fleetmanagement)
- Organisation, Steuerung und Dokumentation der jeweiligen Prozesse (z. B. Inspektionen, UVV, HU, Rückgaben, Schadenbearbeitung)
- Kommunikation, Statusmeldungen und Support im Rahmen der Auftragsabwicklung
- Erstellung von Auswertungen/Reports für den Verantwortlichen im Rahmen der beauftragten Leistungen

## (2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- Personenstammdaten
  - ☑ Vor- und Nachname
  - ☑ Fahrer-ID / Personalnummer (sofern vorhanden)
- Kommunikationsdaten
  - ☑ Dienstliche E-Mail-Adresse
  - ☑ Dienstliche Telefonnummer
- Vertragsstammdaten
  - ☑ Leasingvertragsnummer, Status, Laufzeit
  - ☑ Zuordnung von Fahrzeugen zu Personen
  - ☑ Vertragsbezug (z.B. Dienstwagennutzer)
- Fahrzeugbezogene Daten mit Personenbezug
  - ☑ Kfz-Kennzeichen (wenn Fahrzeug einem Nutzer zugeordnet ist)
  - ☑ IN/VIN im Kontext dienstlicher Fahrzeugnutzung
  - ☑ Statusdaten (z.B. HU-/UVV-Fälligkeit im Zusammenhang mit Fahrer/Nutzer)
- Planungs- und Steuerungsdaten
  - ☑ Wartungstermine, UVV-/HU-Planung
  - ☑ Zuordnung von Fahrzeug- und Prozessdaten zu konkreten Personen
- Kunden-/Nutzerhistorie
  - ☑ Dokumentation bisheriger Werkstattaufträge, Rückgaben, Wartungshistorie
  - ☑ Historie bezogen auf Nutzer und genutztes Fahrzeug

## (3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Fahrer und Fahrzeugnutzer
- Leasingnehmer bzw. Vertragsnutzer
- Mitarbeitende des Kundenunternehmens (z. B. Fuhrparkverantwortliche, Ansprechpartner)

## 3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle erforderlichen technisch-organisatorische Maßnahmen gem. Art. 32 DS-GVO zum Schutz der personenbezogenen Daten und übergibt dem Auftraggeber die Dokumentation zur Prüfung [Anlage 1]. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Vertrags.

(2) Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(3) Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer zukünftig gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Über wesentliche Änderungen, die durch den Auftragnehmer zu dokumentieren sind, ist der Auftraggeber unverzüglich in Kenntnis zu setzen.

#### **4. Rechte von betroffenen Personen**

(1) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, 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.

(2) Soweit vom Leistungsumfang umfasst, sind die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung sowie Daten Portabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

#### **5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers**

(1) Der Auftragnehmer hat, zusätzlich zu der Einhaltung der Regelungen dieses Vertrags, eigene gesetzliche Pflichten gemäß der DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- a) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die berechtigterweise 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.
- b) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- c) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Vertrag 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.

- d) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeit- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten, einem anderen Anspruch oder einem Informationersuchen im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- e) 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.
- f) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrags.
- g) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Art. 33, 34 DS-GVO nachkommen kann. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt.
- h) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung.
- i) Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

(2) Dieser Vertrag entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DS-GVO.

## 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 Nebenleistungen, die der Auftragnehmer in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. 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 zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Der Auftraggeber stimmt der Beauftragung der in Anhang 2 bezeichneten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO mit dem Unterauftragnehmer zu.

Die vertragliche Vereinbarung wird dem Auftraggeber auf dessen Verlangen vorgelegt, wobei geschäftliche Klauseln ohne datenschutzrechtlichen Bezug hiervon ausgenommen sind.

Der Wechsel der gemäß Anhang 2 bestehenden Unterauftragnehmer sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer angemessenen Zeit, die 14 Tage nicht unterschreiten darf, vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung personenbezogener Daten und sodann regelmäßig durch den Auftragnehmer kontrolliert. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung. Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer ist nicht gestattet;

(6) Der Auftragnehmer kann zur Durchführung der Leistungen ein Netzwerk unabhängiger Partner Werkstätten einsetzen. Partner-Werkstätten sind keine Unterauftragnehmer im Sinne von Art. 28 DSGVO, sondern handeln als eigenständige Verantwortliche. Der Auftraggeber weist den Auftragnehmer hiermit an, die im Einzelfall zur Beauftragung und Durchführung der Werkstatteleistungen erforderlichen personenbezogenen Daten an die jeweils beauftragte Partner-Werkstatt zu übermitteln. Eine Auflistung der Partner-Werkstätten in Anlage/Anhang 2 erfolgt nicht. Änderungen im Werkstattnetz begründen keine Mitteilungs-, Zustimmungs- oder Widerspruchsrechte nach dieser AVV (insb. Ziff. 6) und erfordern keine Aktualisierung der AVV.

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

## **7. Internationale Datentransfers**

(1) Jede Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung des Auftraggebers und bedarf der Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DS-GVO.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

(2) Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DS-GVO verantwortlich.

## **8. Kontrollrechte des Auftraggebers**

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

(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.

(3) Der Nachweis der technisch-organisatorischen Maßnahmen zur Einhaltung der besonderen Anforderungen des Datenschutzes allgemein sowie solche, die den Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;

- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

## 9. Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Text-form). Die anfänglichen Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt.

(2) 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 so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

## 10. Löschung und Rückgabe von personenbezogenen Daten

(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 Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens aber mit Beendigung der Leistungsvereinbarung – 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. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Der Auftragsverarbeiter ist jedoch berechtigt, die im Rahmen der Auftragsverarbeitung verarbeiteten personenbezogenen Daten vor deren Löschung zu anonymisieren und die hieraus gewonnenen anonymen Daten zu eigenen Zwecken, insbesondere zur statistischen Auswertung sowie zur Verbesserung seiner Produkte und Dienstleistungen, zu verwenden. Ein Personenbezug ist nach der Anonymisierung ausgeschlossen.

## Anlage 1: Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

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

#### 1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Chipkarten / Transpondersysteme	<input checked="" type="checkbox"/> Schlüsselregelung / Liste
<input checked="" type="checkbox"/> Manuelles Schließsystem	<input checked="" type="checkbox"/> Empfang / Rezeption / Pförtner
<input checked="" type="checkbox"/> Einbruchshemmende Fenster und Türen	<input checked="" type="checkbox"/> Besucher in Begleitung durch Mitarbeiter
<input checked="" type="checkbox"/> Sicherheitsschlösser	<input checked="" type="checkbox"/> Sorgfalt bei Auswahl Reinigungsdienste
<input checked="" type="checkbox"/> Absicherung der Gebäudeschächte	

## 1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzererkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Login mit Benutzername + Passwort	<input checked="" type="checkbox"/> Verwalten von Benutzerberechtigungen durch qualifizierte Fachkräfte
<input checked="" type="checkbox"/> Login mit Zwei-Faktor-Authentifizierung	<input checked="" type="checkbox"/> Erstellen von Benutzerprofilen
<input checked="" type="checkbox"/> Anti-Virus-Software Clients	<input checked="" type="checkbox"/> Zentrale Passwortvergabe
<input checked="" type="checkbox"/> Firewall	<input checked="" type="checkbox"/> Richtlinie „Sicheres Passwort“
<input checked="" type="checkbox"/> Intrusion Detection Systeme	<input checked="" type="checkbox"/> Richtlinie „Löschen / Vernichten“
<input checked="" type="checkbox"/> Automatische Accountsperrung	<input checked="" type="checkbox"/> Richtlinie „Clean desk“
<input checked="" type="checkbox"/> Codierte Speicherung von Passwörtern	<input checked="" type="checkbox"/> Allg. Richtlinie Datenschutz und / oder Sicherheit
<input checked="" type="checkbox"/> Verschlüsselung Smartphones	<input checked="" type="checkbox"/> Richtlinie „Verschlüsselung“
<input checked="" type="checkbox"/> Gehäuseverriegelung	<input checked="" type="checkbox"/> Protokolle werden auf einem dezidierten Protokollserver gespeichert
<input checked="" type="checkbox"/> Automatische Desktopsperre	<input checked="" type="checkbox"/> Sicherheitsrichtlinien, Schulungen und statische Code-Analysen zur Beschränkung des Zugangs zum Source-Code
<input checked="" type="checkbox"/> Verschlüsselung von Notebooks / Tablet	<input checked="" type="checkbox"/> Sicherheitsrichtlinien, Schulungen und statische Code-Analysen zu Security by Design
<input checked="" type="checkbox"/> Eingehende Mails werden mit Anti-Malwareschutz überprüft	<input checked="" type="checkbox"/> Es werden keine personenbezogenen Daten oder Zugangsdaten in der Source-Code-Verwaltung abgelegt

### 1.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	<input checked="" type="checkbox"/> Einsatz Berechtigungskonzepte
<input checked="" type="checkbox"/> Externer Aktenvernichter (DIN 32757)	<input checked="" type="checkbox"/> Minimale Anzahl an Administratoren
<input checked="" type="checkbox"/> Verwendung des TLS2.1-Protokolls	<input checked="" type="checkbox"/> Regelmäßige Überprüfung der Rollen
	<input checked="" type="checkbox"/> Verwaltung Benutzerrechte durch Administratoren
	<input checked="" type="checkbox"/> Stärkere Richtlinien für Admin-Accounts
	<input checked="" type="checkbox"/> Rollenvergabe nach Position
	<input checked="" type="checkbox"/> Regelmäßige Überprüfung der Rollen

### 1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Trennung von Produktiv- und Testumgebung	<input checked="" type="checkbox"/> Steuerung über Berechtigungskonzept
<input checked="" type="checkbox"/> Physikalische Trennung (Systeme /Datenbanken / Datenträger)	<input checked="" type="checkbox"/> Festlegung von Datenbankrechten
<input checked="" type="checkbox"/> Trennung von Webservern durch eigene Server in Firewall-Struktur	<input checked="" type="checkbox"/> Datensätze sind mit Zweckattributen versehen
<input checked="" type="checkbox"/> Benutzung separater Cloud-Konten	

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

Die Verarbeitung personenbezogener Daten 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;

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (mögl. verschlüsselt)	

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

### 2.1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Email-Verschlüsselung	<input checked="" type="checkbox"/> Richtlinie für Datentransfers innerhalb der Organisation und mit anderen Parteien
<input checked="" type="checkbox"/> Einsatz von VPN	<input checked="" type="checkbox"/> Keine Versendung von Passwörtern über unsichere Transportwege
<input checked="" type="checkbox"/> Protokollierung der Zugriffe und Abrufe	
<input checked="" type="checkbox"/> Sichere Transportbehälter	
<input checked="" type="checkbox"/> Bereitstellung über verschlüsselte Verbindungen wie sftp, https	
<input checked="" type="checkbox"/> Nutzung von Signaturverfahren	
<input checked="" type="checkbox"/> Die Integrität von personenbezogenen Daten durch digitale Signaturen wird bei hohem Risiko sichergestellt	

### 2.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

<b>Technische Maßnahmen</b>	<b>Organisatorische Maßnahmen</b>
<input checked="" type="checkbox"/> Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	<input checked="" type="checkbox"/> Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
<input checked="" type="checkbox"/> Manuelle oder automatisierte Kontrolle der Protokolle	<input checked="" type="checkbox"/> Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
<input checked="" type="checkbox"/> IOCs (Indicators of Compromise, meist URL und IP-Hashes) werden protokolliert, blockiert und regelmäßig aktualisiert	<input checked="" type="checkbox"/> Klare Zuständigkeiten für Löschungen
<input checked="" type="checkbox"/> Es wird eine automatische Ausführung von heruntergeladenen Programmen verhindert.	

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

#### 3.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlage, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidssysteme, Plattenspiegelungen etc.

Hinweis: Der Betrieb von Serverinfrastruktur ist an Cloudanbieter ausgelagert, die die u.g. technischen Maßnahmen umgesetzt haben.

<b>Technische Maßnahmen</b>	<b>Organisatorische Maßnahmen</b>
<input checked="" type="checkbox"/> Feuer- und Rauchmeldeanlagen	<input checked="" type="checkbox"/> Backup & Recovery-Konzept (ausformuliert)
<input checked="" type="checkbox"/> Sprinkleranlage Serverraum	<input checked="" type="checkbox"/> Kontrolle des Sicherungsvorgangs
<input checked="" type="checkbox"/> Serverraumüberwachung Temperatur und Feuchtigkeit	<input checked="" type="checkbox"/> Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
<input checked="" type="checkbox"/> Serverraum klimatisiert	<input checked="" type="checkbox"/> Backups werden auf geeigneten Backupmedien, nach der 3-2-1 Regel durchgeführt
<input checked="" type="checkbox"/> USV	<input checked="" type="checkbox"/> Keine sanitären Anschlüsse im oder oberhalb des Serverraums
<input checked="" type="checkbox"/> Schutzsteckdosenleisten Serverraum	<input checked="" type="checkbox"/> Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)

<input checked="" type="checkbox"/> Sowohl symmetrische als auch asymmetrische Verschlüsselung nach Stand der Technik mit AES-256 bzw. mit CBC/GCM Modus	<input checked="" type="checkbox"/> Regelmäßige Wartung der Feuer- und Rauchmeldeanlagen durch Fachfirmen
<input checked="" type="checkbox"/> Keine Fenster zum Serverraum	<input checked="" type="checkbox"/> Effektive Schlüsselverwaltung
	<input checked="" type="checkbox"/> Sicherstellung, dass keine kryptographischen Verfahren mit bekannten Schwachstellen oder zu kurzer Schlüssellänge mehr verwendet werden
	<input checked="" type="checkbox"/> Regelmäßige Durchführung von System- und Sicherheitstests, wie z. B. Code-Scan und Penetrationstests unter Berücksichtigung ausreichender Testzyklen
	<input checked="" type="checkbox"/> Fortlaufender Plan zur Überwachung, Bewertung und Anwendung von Updates oder Konfigurationsänderungen für die gesamte Lebenszeit einer Softwareanwendung

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

##### 4.1. Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Software-Lösungen für Datenschutz-Management im Einsatz	<input checked="" type="checkbox"/> Externer Datenschutzbeauftragter: Projekt 29 GmbH & Co. KG anfragen@projekt29.de
<input checked="" type="checkbox"/> Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet ...)	<input checked="" type="checkbox"/> Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet
<input checked="" type="checkbox"/> Ohne vorherige technische Schutzmaßnahmen können keine Daten in Drittländer übertragen werden	<input checked="" type="checkbox"/> Jährliche Sensibilisierung der Mitarbeiter durch Schulungen
<input checked="" type="checkbox"/> Anderweitiges dokumentiertes Sicherheits-Konzept	<input checked="" type="checkbox"/> Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
<input checked="" type="checkbox"/> Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	<input checked="" type="checkbox"/> Sichere Nutzung von Home-Office
	<input checked="" type="checkbox"/> Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
	<input checked="" type="checkbox"/> Regelmäßige Audits

	<input checked="" type="checkbox"/> Meldeverpflichtungen nach Art. 33 und 34 wurden identifiziert
	<input checked="" type="checkbox"/> Mitarbeiter sind geschult Cyberangriffe zu erkennen

#### 4.2. Incident-Response-Management

*Unterstützung bei der Reaktion auf Sicherheitsverletzungen*

<b>Technische Maßnahmen</b>	<b>Organisatorische Maßnahmen</b>
<input checked="" type="checkbox"/> Einsatz von Firewall und regelmäßige Aktualisierung	<input checked="" type="checkbox"/> Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
<input checked="" type="checkbox"/> Einsatz von Spamfilter und regelmäßige Aktualisierung	<input checked="" type="checkbox"/> Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
<input checked="" type="checkbox"/> Einsatz von Virens Scanner und regelmäßige Aktualisierung	<input checked="" type="checkbox"/> Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
<input checked="" type="checkbox"/> Intrusion Detection System (IDS)	<input checked="" type="checkbox"/> Formaler Prozeß und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen
<input checked="" type="checkbox"/> Intrusion Prevention System (IPS)	<input checked="" type="checkbox"/> Ablaufplan bei Schadcode Befall
<input checked="" type="checkbox"/> zentrale Erfassung von Schadcode Alarmmeldungen	<input checked="" type="checkbox"/> Notfallplan zur Business Continuity
<input checked="" type="checkbox"/> Durchführung von Security Reporting	

#### 4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

*Privacy by design / Privacy by default*

<b>Technische Maßnahmen</b>	<b>Organisatorische Maßnahmen</b>
<input checked="" type="checkbox"/> Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	
<input checked="" type="checkbox"/> Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen	

#### 4.4. Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/>	<input checked="" type="checkbox"/> Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
<input type="checkbox"/>	<input checked="" type="checkbox"/> Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
<input type="checkbox"/>	<input checked="" type="checkbox"/> Schriftliche Weisungen an den Auftragnehmer
<input type="checkbox"/>	<input checked="" type="checkbox"/> Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
<input type="checkbox"/>	<input checked="" type="checkbox"/> Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
<input type="checkbox"/>	<input checked="" type="checkbox"/> Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
<input type="checkbox"/>	<input checked="" type="checkbox"/> Regelung zum Einsatz weiterer Subunternehmer
<input type="checkbox"/>	<input checked="" type="checkbox"/> Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
<input type="checkbox"/>	<input checked="" type="checkbox"/> Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

**Anlage 2: Übersicht der Unterauftragnehmer (Subunternehmer) RONYA**

Lfd. Nr.	Unternehmensbezeichnung inkl. Geschäftsanschrift	Handelsregister-Nummer / Umsatzsteuer-Identifikationsnummer	Sofern abweichend von der Geschäftsanschrift: Standort der Dienstleistungserbringung	Sofern abweichend von der Geschäftsanschrift: Standort der Datenspeicherung	Weiterverlagte Aktivitäten und Prozesse	Datum der Verlagerung	Datum der Genehmigung / Freigabe
# 1	Schwacke GmbH Westendstraße 28, 60325 Frankfurt	HRB 114451 USt-IdNr DE114 147 620	-	-	Abfrage der Servicepläne und Teileinformationen	01.08.2023	
# 2	Zectos Software Private Limited First Floor, 3460, Block 9 Sector 45D, Chandigarh 160047, India	GST 04AABCZ7 107K1Z9	-	Microsoft Corp. Frankfurt am Main	Schwesterfirma für Softwareentwicklung und IT Support	19.12.2021	
# 3	HaynesPro B.V., Teil der InfoPro Digital Automotive Gruppe Stationsstraat 79-F 3811 MH in Amersfoort Niederlande	Eingetragen in Amersfoort 31047540 NL805700821B01			Abfrage der Servicepläne, Reparturdaten und Öl-Spezifikationen	01.12.2025	