Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen

.....

.....

- Verantwortlicher - nachstehend Auftraggeber genannt -

und der

OnREX GmbH

04720 Döbeln OT Großsteinbach, Obersteinbach 52

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Gegenstand der Auftragsdatenverarbeitung sind ausschließlich die vom Auftraggeber auf der DYNAREX Plattform erfassten und verarbeiteten personenbezogenen Daten laut Auftrag/Bestellung DYNAREX vom ……..

Der Auftragnehmer verwendet personenbezogene Daten des Auftraggebers nicht für eigene Zwecke und ist insbesondere nicht berechtigt, sie an Dritte ohne Zustimmung des Auftraggebers weiterzugeben.

Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Benutzerinformationen und Sicherheitskopien, soweit sie zur Zugangssteuerung und Abrechnung sowie Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind

Daten /Datenkategorien

Der Auftragnehmer speichert im Auftrag des Auftragnehmers folgende personenbezogene Daten/Datenkategorien der Betroffenen:

- Adress- und Kommunikationsdaten
- Aktenzeichen (z. Bsp. bei Versicherung , Gericht)
- Fahrzeugdaten
- Versicherungsangaben
- Unfall- und Besichtigungsdaten

Kreis der von der Datenverarbeitung Betroffenen:

Der Auftragnehmer speichert im Auftrag des Auftraggebers die Daten vom Fahrzeughalter, Versicherungsnehmer, Anspruchsteller, Unfallgegner, Rechnungsempfänger, Mahnungsempfänger, Rechtsanwälten, Prozessbevollmächtigter, Besichtigungsanwesende, Sachverständige sowie Ansprechpartner von Firmen die am Schadensvorgang beteiligt sind, wie Versicherungen, Werkstätten, Abschleppfirmen, Gerichten, Drittdienstleistern oder Restwertaufkäufern.

(2) Dauer

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

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

DYNAREX ist eine Privat Cloud auf der der Auftraggeber Schadengutachten und weitere Fahrzeug- und personenbezogene Daten erfasst und verarbeitet, um KFZ-Sachverständigen-Dienstleistungen wie z.B. KFZ-Schaden- und –Wertgutachten, nachstehend Vorgang genannt, zu erbringen. Der Zugriff auf die DYNAREX- Plattform erfolgt eine gesonderte Benutzerberechtigung per Webbrowser bzw. Apps für mobile Endgeräte. Der Datenaustausch zwischen dem Endgerät des Auftraggebers und der DYNAREX-Plattform ist verschlüsselt.

Bei der Erfassung und Bearbeitung werden dabei vom Auftraggeber folgende Adress- und Kontaktinformationen der im Vorgang erforderlichen Beteiligten und deren Ansprechpartner gespeichert, verarbeitet und übertragen:

Soweit im Vorgang erforderlich der Vor- und Nachname, der Titel, die vollständige Adresse mit PLZ, Ort, Straße und Hausnummer ggf. PF-Nummer, Telefon-, Fax- und Mobilnummer für die private oder geschäftliche Kontaktaufnahme und die E-Mail-Adresse.

Zu den erfassten Beteiligten können die jeweiligen Bearbeitungsnummern (Aktenzeichen) gespeichert werden. z.B. zur Versicherung die Schadennummer, zum Gericht/Rechtsanwalt das Aktenzeichen, zum Leasinggeber die Leasingvertragsnummer oder zur Polizeidienststelle die Tagebuch-Nummer.

Gespeichert werden Fahrzeugdaten des Fahrzeughalters wie z.B. Fahrzeugidentifikationsnummer, Amtliches Kennzeichen, KBA-Schlüssel, EURO-Code DAT, Fahrzeug Hersteller-, Fabrikat- und Typ-Bezeichnung, Aufbauart, Anzahl Türen, Baujahr, Erstzulassung, Abmessung und Gewichte, Farbe und verwendete Lackart, Anzahl Vorbesitzer, Fahrzeugausstattung, Reifen und Profiltiefe, Allgemeiner Fahrzeugzustand und Kilometerlaufleistung

Gespeichert werden Versicherungsangaben des Fahrzeughalters wie z.B. Versicherungsadresse, Versicherungs-Scheinnummer, Versicherungs-Schaden-Nummer, Vertragsart / Deckung oder Selbstbehalt Kasko.

Im Zusammenhang mit der Erstellung des Gutachtens werden weitere Daten verarbeitet und gespeichert wie z.B. Schadentag, Schadenbeschreibung, Anstoßbereiche, Besichtigungstermin, Uhrzeit, Ort und Beteiligte, Besichtigungszustand, Unfallskizzen, Digitale Fotos, Schadenpositionen, Berechnungsergebnisse (Reparaturkosten, Fahrzeugwert, Restwert, Marktwert, Merkantile Wertminderung), Berechnungsergebnis im Format PDF (z.B. Gutachten, Bewertung, Kostenvoranschlag Gerichtsgutachten)

Arbeitsergebnisse in Form von PDF-Dokumenten werden ausschließlich vom Auftraggeber an Beteiligte eines Vorganges wie folgt übermittelt:

- per Freigabe-Link auf die DYNAREX Plattform über SMS bzw. E-Mail und Passwort-Authentifizierung.
- Per Ausdruck auf Papier auf lokal installierte Drucksysteme.
- Per elektronische Datenübermittlung via GDV-Schadennetz bzw. mit ihr verbundener Schadennetze in einem Datenformat, dass vom berechtigten Empfänger in die eigene Datenverarbeitungsanlage importiert und verarbeitet werden kann.

Eingebundene Services von Drittdienstleistern

Für die Ermittlung von Berechnungsergebnisse werden auf der DYNAREX-Plattform Drittdienstleister eingebunden. Drittdienstleister sind Anbieter von kostenpflichtigen Diensten für die Ermittlung von

Schadenkalkulationen, Bewertungen, Restwertgeboten und Marktwertübersichten usw.

Die Weitergabe von Auftragsdaten an Drittdienstleister wird grundsätzlich erst nach Bestellung des Auftraggebers und mit dessen Zugangsdaten durchgeführt. Die Datenübertragung zum Drittdienstleister erfolgt verschlüsselt und ausschließlich nach dessen Schnittstellenvorgaben.

OnREX haftet nicht für Schäden, die durch unsachgemäße Auftragsdatenverarbeitung beim Drittdienstleister verursacht werden. Die Auftragsdatenverarbeitung beim Drittdienstleister ist vertraglich ausschließlich zwischen Auftraggeber und Drittdienstleister zu regeln.

Benutzerinformation

Benutzerinformationen werden ausschließlich für den Betrieb der DYNAREX Plattform verwendet, insbesondere zu Registrierung, für die Programmfunktionen von DYNAREX wie zum Beispiel der Zuordnung von Berechtigungen, für Workflows, zur Dokumentation, Abrechnung und zur Kommunikation mit dem Auftragnehmer.

- Folgende Daten werden gespeichert.

Erfasste Informationen	**Verwendung**
E-Mail Adresse	• Zur Kontoerstellung • Verifizierung der Registrierung • Schutz vor unberechtigtem Anmelden, Spam und Betrug • Zurücksetzen des Kennwortes • Zur Kontaktaufnahme für Informationen zum DYNAREX Betrieb
Name und Adresse des Unternehmens / Mandant	• Für die Zuordnung der erworbenen Lizenz • Bei Bedarf zur Anzeige in Ergebnisdokumenten • Für die Berechnung der Leistungen
Name und Adresse des Unternehmens / Büro	• Bei Bedarf zur Anzeige in Ergebnisdokumenten • Zur Steuerung der Nummernkreise von Aktenzeichen im Programm • Für die Zuordnung von Usern zum Büro • Für bürobezogene Programmeinstellung
Berufliche Kontaktdaten	• Für die Anzeige in der Userverwaltung des Mandanten • Für die Zuordnung von Programm-Berechtigungen durch den Admin des Mandanten • Bei Bedarf zur Anzeige in Ergebnisdokumenten z.B. Gutachten • Zur Protokollierung bzw. / Freigabe von Aktivitäten im Programm für den Mandanten • Für die Interaktion mit anderen Usern des Mandanten
Qualifikation, wenn erfasst	• Für die Dokumentation auf Gutachten bzw. sonstigen Dokumenten

Das geografische Gebiet, indem der Dienst nutzen und die Sprache	• Zur Hilfe des Mandanten um die Nutzung des Kontos nachzuverfolgen. Über Kontoeinstellungen können Sie den Verlauf der zuletzt verwendeten IP nachverfolgen. • Um die Interaktion mit dem Programm zu verbessern. • Zur Einhaltung landesbezogener rechtlicher Beschränkungen
Zahlungsinformationen	• Für die Bearbeitung und zur Weitergabe an eine externe Zahlungsverarbeitung wie z.B. PayPal

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) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind, Personenstammdaten, Kommunikationsdaten (z.B. Telefon, E-Mail), Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse), Kundenhistorie, Vertragsabrechnungs- und Zahlungsdaten, Planungs- und Steuerungsdaten und Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

(3) Kategorien betroffener Personen
Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen Kunden, Interessenten, Abonnenten, Beschäftigte, Lieferanten, Handelsvertreter und Ansprechpartner

3. Technisch-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. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 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 [Einzelheiten in Anlage 1].
(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. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(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.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.

Als Datenschutzbeauftragter ist beim Auftragnehmer bestellt:

Rüdiger Ortolf
Altenburger Straße 9
04275 Leipzig

Tel.: 0341-3500 2460
e-mail: r.ortolf@t-online.de
www.datenschutz-ortolf.de

b) Die Wahrung der Vertraulichkeit gemäß Artt. 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 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.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

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

e) 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.

f) 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.

g) 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.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

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 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 Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.
Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma Unterauftragnehmer	Anschrift/Land	Leistung
ACS Solutions GmbH	Maximilianallee 2 04129 Leipzig	Betrieb Serverfarm im RZ envia Tel datacenter, Leipziger Straße 116b, 04425 Taucha

der Wechsel des bestehenden Unterauftragnehmers ist zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit 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 DS-GVO 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.
(4) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

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

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) 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

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

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

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

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

10. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützten. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten

technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

11. 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 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.
(3) 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.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift Auftraggeber	Unterschrift Auftragnehmer

Anlage – Technisch-organisatorische Maßnahmen

Technische und organisatorische Maßnahmen zum Datenschutz und zur IT-Sicherheit werden je nach sachlicher und fachlicher Zuordnung am Standort des Auftragsverarbeiters oder am Standort des Rechenzentrums envia Tel datacenter Leipziger Straße 116b, 04425 Taucha umgesetzt.

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

Zutrittskontrolle wird gewährleistet durch:

- Alarmanlage
- Türsicherung durch Chip-Karten/Transpondersystem
- Videoüberwachung der Zugänge
- Bewegungsmelder
- Personenkontrolle durch Wachdienst am Objekteingang
- Protokollierung der Besucher
- Sorgfältige Auswahl des Reinigungs- und des Wachpersonals
- Tragepflicht von Berechtigungsausweisen
- Verschluss der Serverschränke

Zugangskontrolle wird gewährleistet durch:

- Passwortvergabe nach Passwortrichtlinie
- Authentifikation mit Benutzername und Kennwort
- Zuordnung von Benutzerrechten
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie
- Einsatz von Intrusion-Detection-Systemen
- Einsatz von Anti-Viren-Software
- Einsatz von Software-Firewall
- Verschlüsselung von mobilen Datenträgern.

Zugriffskontrolle wird gewährleistet durch:

- Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)
- Verwalten der Rechte durch Systemadministrator
- Reduzierung der User mit Administratorenrechten auf des notwendige Minimum
- Passwortrichtlinie
- Sichere Aufbewahrung von Datenträgern
- Vernichtung von Datenträgern nach DIN 66399
- Protokollierung der Vernichtung
- Regelmäßige Auswertung und Kontrolle bestehender Berechtigungen
- Zeitnahe Aktualisierung bzw. Löschung der Berechtigungen

Trennungskontrolle wird gewährleistet durch:

- Physikalisch getrennte Speicherung

- Interne Mandantenfähigkeit der Software
- Funktionstrennung (Produktion/Test)

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

Weitergabekontrolle wird gewährleistet durch:

- Verschlüsselte Datenübertragung
- VPN
- Fernwartung nur bei Anwesenheit Mitarbeiter

Eingabekontrolle wird gewährleistet durch:

- Protokollierung
- Nachvollziehbarkeit von Eingabe, Änderung, Löschung von Daten durch eigene Benutzernamen

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

Verfügbarkeit und Belastbarkeit wird gewährleistet durch:

- Klimaanlage in den Serverräumen
- Einsatz von Geräten zur Überwachung von Temperatur und Feuchtigkeit in den Serverräumen
- Schutzsteckdosenleitungen in den Serverräumen
- Feuer- und Rauchmeldeanlagen in den Serverräumen
- Feuerlöschgeräte in den Serverräumen
- Unterbrechungsfreie Stromversorgung (USV)
- Backup- und Recovery-Konzept
- Tests zur Datenwiederherstellung
- Räumlich getrennte Aufbewahrung der Sicherungsdatenträger
- Serverräume nicht unter sanitären Anlagen
- Virenschutz
- Firewall

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

- Datenschutz-Management
- Datenschutzorganisation
- Tätigkeit des Datenschutzbeauftragten
- Auftragskontrolle durch eindeutige Vertragsgestaltung und strenge Auswahl der Dienstleister