Datenschutzvereinbarung

zur Sicherstellung der Konformität zu Artikel 28 EU Datenschutz-Grundverordnung (DSGVO) für die Verarbeitung personenbezogener Daten im Auftrag

zwischen

als Verantwortlicher (nachstehend Auftraggeber genannt)

und der

Modix GmbH
Jakob-Hasslacher-Straße 4
56070 Koblenz

Als Auftragsverarbeiter (nachstehend Auftragnehmer genannt)

zur Hauptvereinbarung zwischen den Parteien (nachstehend Vertrag genannt).

§ 1
Definitionen

1. "**BDSG** " meint das Bundesdatenschutzgesetz.

2. "**EU-Datenschutz-Grundverordnung**" oder "**DSGVO**" meint die "Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)" sowie alles anwendbaren Gesetze der EU-Mitgliedstaaten, welche die DSGVO ausgestalten und spezifizieren.

§ 2
Gegenstand der Vereinbarung

1. Diese Vereinbarung regelt die Maßnahmen zur Sicherstellung der Durchführung der Vorschriften des Artikel 28 DSGVO bei der Datenverarbeitung im Auftrag, die sich aus der Beauftragung gemäß Ziffer 2.1. im Hinblick auf den Umgang mit personenbezogenen Daten ergeben.

2. Der Auftrag umfasst Folgendes:

   2.1 Gegenstand des Auftrages:

   Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich zur Durchführung des Vertrags. Eine detaillierte Beschreibung der Tätigkeiten des

Auftragnehmers, des Gegenstands und der Dauer des Auftrags sind dem Vertrag zu entnehmen. Dieser bildet einen wesentlichen Bestandteil dieser Vereinbarung.

2.2 Die Beschreibung des Umfangs, der Art und des Zwecks der Datenverarbeitung, der Art der personenbezogenen Daten sowie die Kategorien der betroffenen Personen wird in der Anlage A schriftlich oder in elektronischem Format vereinbart.

3. Die Bestimmungen dieser Vereinbarung mitsamt ihrer Anlagen haben Vorrang gegenüber den Regelungen des Vertrags.

§ 3
Pflichten des Auftraggebers

1. Für die Beurteilung der Zulässigkeit der Datenverarbeitung, für die Wahrung der Rechte der Betroffenen und sonstige datenschutzrechtliche Anforderungen (z.B. Durchführung einer Datenschutz-Folgeabschätzung, vorherige Konsultation der Datenschutzaufsichtsbehörde) ist im Außenverhältnis allein der Auftraggeber verantwortlich. Er sichert entsprechend zu, dass er berechtigt ist, die Daten für die Zwecke dieser Vereinbarung an den Auftragnehmer weiterzugeben und die Daten jeweils für die Zwecke die in der Anlage A aufgeführt sind verarbeitet werden dürfen. Der Auftraggeber informiert den Auftragnehmer über Änderungen im lokalen anwendbaren Datenschutzrecht, die Auswirkungen auf diese Vereinbarung und/oder die Verarbeitung der Daten unter dieser Vereinbarung haben bzw. haben können, rechtzeitig vor dem Inkrafttreten einer solchen Änderung.

2. Der Auftraggeber erteilt den Auftrag in schriftlicher [oder elektronischer] Form. Änderungen des Vertragsgegenstandes und Verfahrensänderungen sind abzustimmen und entsprechend §2 Abs. 2.2 festzulegen. Die Weisungsrechte des Auftraggebers nach § 4 bleiben unberührt.

3. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung des Ergebnisses der Auftragsleistung feststellt.

4. Der Auftraggeber ist verpflichtet, alle im Rahmen des Auftragsverhältnisses erlangten Kenntnisse über technische und organisatorische Maßnahmen beim Auftragnehmer vertraulich zu behandeln.

§ 4
Weisungen

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich in Übereinstimmung mit den Weisungen des Auftraggebers, wie sie abschließend in den Bestimmungen dieser Vereinbarung und der jeweils projektbezogenen Anlage A Ausdruck finden. Der Auftragnehmer erkennt die Datenherrschaft des Auftraggebers als Dateneigentümer an und übernimmt diesem gegenüber die Verantwortung, dass diese Daten ausschließlich im Rahmen dieser Vereinbarung verwendet werden.

2. Weisungsberechtigte Personen des Auftraggebers sind in Ziffer 2 der Anlage A festgelegt. Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner der Nachfolger bzw. der Vertreter in schriftlicher oder elektronischer Form mitzuteilen.

3. Der Auftraggeber ist verpflichtet, dem Auftragnehmer ausschließlich datenschutzrechtlich zulässige Weisungen zu erteilen. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt oder eine Schadenersatzpflicht gegenüber einem Dritten begründen würde. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung nach vorheriger Mitteilung solange auszusetzen, bis der Auftraggeber die Weisung geändert hat oder die Parteien im Rahmen des jeweils anwendbaren Eskalationsverfahrens zum Ergebnis kommen, dass kein Verstoß gegen Datenschutzrecht vorliegt.

4. Unabhängig von anderen Regelungen in dieser Vereinbarung ist der Auftragnehmers berechtigt, personenbezogene Daten ohne oder entgegen der Weisungen des Auftraggebers zu verarbeiten, sofern er durch das Recht der EU oder der EU-Mitgliedstaaten, dem der Auftragnehmer unterliegt, zu einer weitergehenden Verarbeitung verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. In jedem Fall darf der Auftragnehmer die Daten anonymisieren und in anonymisierter Form für eigene Zwecke verarbeiten und nutzen.

5. Die Verarbeitung der Daten außerhalb des Gebiets der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum ("Drittland"), einschließlich der Übermittlung in ein und Zugriff aus einem Drittland, wenn die besonderen Voraussetzungen der Übermittlung personenbezogener Daten in ein Drittland erfüllt sind. Das angemessene Schutzniveau Drittland kann wie folgt hergestellt werden:

    a) durch einen Angemessenheitsbeschluss der Kommission ;
    b) durch verbindliche interne Datenschutzvorschriften (sog. Binding Corporate Rules);
    c) durch Standarddatenschutzklauseln/Standardvertragsklauseln;
    d) durch genehmigte Verhaltensregeln;
    e) durch einen genehmigten Zertifizierungsmechanismus;
    f) durch Genehmigung der zuständigen Datenschutzaufsichtsbehörde im Einzelfall.

    Falls ein Unterauftragnehmer beauftragt werden soll, gelten diese Anforderungen zusätzlich zu den Bestimmungen in § 15.

§ 5
Allgemeine Unterstützungspflichten des Auftragnehmers

1. Soweit erforderlich, wenn der Auftraggeber tatsächlich nicht in der Lage ist, dies selbst vorzunehmen, ist der Auftraggeber verpflichtet den Auftragnehmer in angemessenem Umfang bei der Wahrung der Rechte und Erfüllung der Ansprüche der betroffenen Personen, insbesondere bei der Berichtigung, Löschung und Einschränkung der Verarbeitung personenbezogener Daten, sowie bei der Bereitstellung von Informationen und Daten für betroffene Personen zu unterstützen.

2. Sofern sich eine betroffene Person oder eine Datenschutzaufsichtsbehörde im Zusammenhang mit den unter dieser Vereinbarung verarbeiteten personenbezogenen Daten direkt an den Auftragnehmer wendet, wird dieser den Auftraggeber hierüber unverzüglich informieren und alle weiteren Schritten mit dem Auftraggeber abstimmen, soweit dies rechtlich zulässig ist.

3. Für Unterstützungsleistungen nach diesem § 5, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

§ 6
Beauftragter für den Datenschutz des Auftragnehmers

Beim Auftragnehmer ist als Beauftragte(r) für den Datenschutz
Herr/Frau

Dr. Frank Eickmeier, ePrivacy GmbH, Große Bleichen 21, 20354 Hamburg, f.eickmeier@eprivacy.eu, Tel. 040 6094518-12.

bestellt. Ein Wechsel des Beauftragten für den Datenschutz ist dem Auftraggeber mitzuteilen.

§ 7
Datentransport und -übermittlung, Trennungsprinzip

1. Die Datenträger sind vom Auftraggeber und Auftragnehmer als Einschreiben oder Wertsendung oder durch Boten zu versenden. Hierfür sind - soweit Behälter erforderlich sind - stabile Transportbehältnisse zu verwenden. Lässt der Auftraggeber Unterlagen durch Boten beim Auftragnehmer abholen, stattet der Auftraggeber seinen Boten mit einem schriftlichen Berechtigungsnachweis aus.

2. Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden vom Auftragnehmer besonders gekennzeichnet und unterliegen der laufenden automatisierten Verwaltung. Der Auftragnehmer dokumentiert Eingang und Ausgang.

3. Daten können auch mittels Datenfernübertragung unter Einhaltung der in Anlage A dokumentierten Maßnahmen sicher übersendet werden.
4. Sofern nicht Abweichend vereinbart und soweit dies nicht Gegenstand des Auftrages ist, gewährleistet der Auftragnehmer, dass die verarbeiteten Daten von sonstigen Datenbeständen Dritter oder des Auftraggebers getrennt erhoben, verarbeitet oder genutzt werden.

§ 8
Vertraulichkeit

1. Der Auftragnehmer verpflichtet sich, bei der Verarbeitung der personenbezogenen Daten des Auftraggebers das Datengeheimnis sowie Vertraulichkeit zu wahren. § 4 Abs. 4 dieser Vereinbarung gilt entsprechend.

2. Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und diese sich schriftlich auf das Datengeheimnis und zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Der Auftragnehmer überwacht die

Einhaltung der datenschutzrechtlichen Vorschriften.

§9
Sicherheit der Verarbeitung

Der Auftragnehmer hat dafür zu sorgen und hinreichende Garantien dafür zu bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen des BDSG bzw. der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet sowie seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Insbesondere hat der Auftragnehmer unter Berücksichtigung des jeweiligen Stands der Technik die angemessene Sicherheit der Verarbeitung, insbesondere die Vertraulichkeit (inklusive Pseudonymisierung und Verschlüsselung), Verfügbarkeit, Integrität, und Belastbarkeit der für die Datenverarbeitung verwendeten Systeme und Dienstleistungen sicherzustellen. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintritts-wahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Das im Anhang B beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

§ 10
Informationspflichten, Verletzung des Schutzes personenbezogener Daten

1. Der Auftragnehmer informiert den Auftraggeber unverzüglich sobald er Kenntnis einer tatsächlichen oder vermuteten Verletzung des Schutzes personenbezogener Daten im Sinne des Artikel 4 Nr. 12 DSGVO, die beim Auftragnehmer oder bei einem Unterauftragnehmer auftritt, erhält und hat den Auftraggeber in angemessenem Umfang bei der Untersuchung, Schadensbegrenzung und Behebung und, falls erforderlich, bei der Meldung an die zuständigen Datenschutzaufsichtsbehörden und der Benachrichtigung der betroffenen Personen zu unterstützen.

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

§ 11
Kontrollrechte des Auftraggebers und Mitwirkungspflichten des Auftragnehmers

1. Der Auftragnehmer kontrolliert regelmäßig die eigenen internen Prozesse sowie die technischen und organisatorischen Maßnahmen sowie die seiner Unterauftragnehmer, 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.

2. Auf Nachfrage stellt der Auftragnehmer dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der Voraussetzungen des Artikel 28 DSGVO zur Verfügung. Die entsprechenden Nachweise können insbesondere durch

a) die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 DSGVO;
b) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Artikel 42 DSGVO;
c) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren); oder
d) eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz)

erfolgen.

3. Unter den Voraussetzungen des § 11 Abs. 4 und soweit datenschutzrechtlich erforderlich, ist der Auftraggeber oder ein vom Auftraggeber beauftragter unabhängiger Dritter in den nachfolgenden Fällen berechtigt, die Einhaltung der Voraussetzungen dieser Vereinbarung durch den Auftragnehmer, insbesondere die internen Kontrollprozesse und Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen, zu überprüfen; soweit erforderlich schließt dies Vor-Ort-Kontrollen ein:

   a) Der Auftragnehmer hat für die Einhaltung dieser Vereinbarung trotz Aufforderung durch den Auftraggeber keine ausreichenden Nachweise nach § 11 Abs. 2 vorgelegt;
   b) Es ist zu einer Verletzung des Schutzes personenbezogener Daten gekommen;
   c) Der Auftraggeber kann tatsächliche Anhaltspunkte vorbringen, die den Verdacht begründen, dass der Auftragnehmer seine Verpflichtungen nach dieser Vereinbarung nicht erfüllt;
   d) Die Überprüfung wurde durch eine für den Auftraggeber zuständige Datenschutzaufsichtsbehörde oder andere zuständige Behörde (einschließlich Strafverfolgungsbehörden) angeordnet.

4. Die Prüfungsrechte des Auftraggebers bestehen im folgenden Umfang:

   a) Soweit nicht datenschutzrechtlich zwingend erforderlich, kann eine Überprüfung nach § 11 Abs. 3 lediglich einmal pro Kalenderjahr durchgeführt werden;
   b) Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens vier Wochen vorher) über die Überprüfung und alle mit der Durchführung der Überprüfung zusammenhängenden Umstände zu informieren, soweit eine behördliche Anordnung oder andere zwingende rechtliche Gründe nicht eine kürzere Frist oder unangekündigte Überprüfung erforderlich machen;
   c) Die Überprüfung erfolgt im Rahmen der üblichen Geschäftszeiten auf Kosten des Auftraggebers, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers;
   d) Der Auftragnehmer ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten – es sei denn, dass diese die Basis des erstattungsfähigen oder durchlaufenden Aufwandes darstellen – zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Kontrollzwecke sind, zu erhalten.
   e) Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Kontrolle, hat der Auftraggeber den Dritten schriftlich auf Verschwiegenheit und Geheimhaltung

zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber diesem die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Konkurrenten des Auftragnehmers mit der Kontrolle beauftragen;

f) Der Auftraggeber stellt dem Auftragnehmer eine kostenlose Kopie des Prüfungsberichts zur Verfügung.

5. Der Auftragnehmer wird der Datenschutzaufsichtsbehörde oder andere zuständige Behörde (einschließlich Strafverfolgungsbehörden) unmittelbar alle Informationen im Zusammenhang mit dieser Vereinbarung geben und entsprechende Auskünfte erteilen und der Aufsichtsbehörde die Möglichkeit einräumen, Prüfungen in demselben Umfang durchzuführen wie sie die Aufsichtsbehörde beim Auftraggeber durchführen darf. Der Auftragnehmer gewährt der zuständigen Aufsichtsbehörde auch in diesem Rahmen alle erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte.

§ 12
Laufzeit

Diese Beauftragung gilt für die Dauer des folgenden zwischen den Parteien bestehenden Vertrages:

_____

(Benennung des Vertrages)

§ 13
Löschung und Rückgabe personenbezogener Daten

1. Überlassene Dokumente, personenbezogene Daten und Datenträger sowie Kopien derselben sind grundsätzlich nach Beendigung des Auftrags nach Wahl des Auftraggebers entweder durch den Auftragnehmer zu löschen bzw. zu vernichten oder zurückzugeben, sofern für den Auftragnehmer nicht nach dem Recht der Europäischen Union oder dem Recht der Mitgliedsstaaten der Europäischen Union eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Besteht eine weitere Verpflichtung zur Speicherung hat der Auftragnehmer die Verarbeitung der personenbezogenen Daten einzuschränken und die Daten nur für die Zwecke zu nutzen, für die Verpflichtung zur Speicherung besteht. Die Pflichten zur Sicherheit der Verarbeitung nach § 9 bestehen für den Zeitraum der Speicherung fort. Der Auftragnehmer hat die Daten unverzüglich zu löschen, sobald die Pflicht zur Speicherung entfällt.

2. Der Auftraggeber kann auch vorher jederzeit die Löschung bzw. Vernichtung oder Herausgabe verlangen, sofern die in § 13 Abs. 1 aufgeführten Aufbewahrungspflichten des Auftragnehmers nicht entgegenstehen.

3. Test und Ausschussmaterial ist unverzüglich datenschutzgerecht zu vernichten oder ebenfalls dem Auftraggeber auszuhändigen.

§ 14
Haftung

Der Auftragnehmer haftet im Rahmen der gesetzlichen Bestimmungen und der vereinbarten Haftungsbeschränkung für Schäden, die infolge schuldhaften Verhaltens gegen die Datenschutzbestimmungen oder gegen diese Datenschutzvereinbarung entstehen. Ebenso haftet er für schuldhaftes Verhalten seiner Unterauftragnehmer sowie deren Unterauftragnehmer.

§ 15
Unterauftragnehmer

1. Die vertraglich vereinbarten Leistungen werden unter Einschaltung der über diesen Link (https://www.modix.de/de/dsgvo/dienstleister) abrufbaren Subunternehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern ("Subunternehmerverhältnis") befugt. Der Wechsel des oder die neue Beauftragung eines Subunternehmers sind zulässig, soweit eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird. Der jeweils aktuelle Status der eingesetzten Dienstleister ist über den oben angegeben Link jederzeit abrufbar. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

2. Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch Im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

§ 16
Sonstiges

1. Erweist sich eine Bestimmung dieser Vereinbarung als unwirksam, so berührt dies die Wirksamkeit der übrigen Bestimmungen der Vereinbarung nicht. Beide Seiten sind in diesem Fall verpflichtet, unverzüglich in eine nachträgliche Zusatz-bestimmung einzuwilligen, die nach Sinn und Zweck der unwirksamen Bestimmung am nächsten kommt.

2. Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

3. Für Nebenabreden ist die Schriftform oder elektronische Form erforderlich.

4. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder in Zusammenhang mit

dieser Vereinbarung ist Koblenz.

5. Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.

6. Dieser Vertrag ist in 2 (zwei) Exemplaren, von denen jeder Vertragspartner eines erhält, ausgefertigt. Die Vertragspartner dürfen den Vertrag übersetzen, jedoch ist die deutsche Originalfassung maßgebend.

Anlagen zur Datenschutzvereinbarung im Auftrag:

Anlage A - Beschreibung der Datenverarbeitung
Anlage B - Beschreibung der technischen und organisatorischen Maßnahmen

_____ , den _____

Stempel und Unterschrift des Auftragnehmers	Stempel und Unterschrift des Auftraggebers
Name in Druckbuchstaben	Name in Druckbuchstaben
_____	_____

Anlage A zur Datenschutzvereinbarung

Beschreibung der Datenverarbeitung

1. Gegenstand des Auftrages

1.1. Gegenstand des Auftrages:
(Beschreibung des Auftrags in Bezug auf den Umgang mit personenbezogenen Daten – nachfolgend „Daten“ genannt)

- Bereitstellung der Modix-Applikation
- IT-, insbesondere Support der Applikation und der Modix Umgebung.
- Wartungs- und Serviceaufgaben
- Hosting und Backup

…….

1.2. Umfang, Art und Zweck der Datenverarbeitung:

Sämtliche Tätigkeiten, die zur Erfüllung des unter Ziff.1.1.benanten Zweckes erforderlich sind.

……..

1.3. Art der Daten:

Namen
Anschriften
Kommunikationsdaten
Daten im Rahmen von Fahrzeuginseraten

……..

1.4. Kreis der Betroffenen:

Besucher der Website des Auftraggebers
Kunden des Auftraggebers
Sonstige Interessenten des Auftraggebers.

……..

Anlage B zur Datenschutzvereinbarung

Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

der Modix GmbH

Stand: 26.09.2018

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die og. Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

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
☒ Alarmanlage	☒ Mitarbeiter- / Besucherausweise
☒ Automatisches Zugangskontrollsystem	☒ Besucher in Begleitung durch Mitarbeiter
☒ Biometrische Zugangssperren	☒ Sorgfalt bei Auswahl des Sicherheitspersonals
☒ Chipkarten / Transpondersysteme	☒ Registrierung von Besuchern
☒ Kameraüberwachung der Eingänge	
☒ Sicherheitsschlösser	
☒ Kameraüberwachung der Eingänge	
☒ Sorgfältige Auswahl des Reinigungspersonals	
☒ Security Awareness-Schulungen	

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, Benutzerkennung 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**
☒Login mit Benutzername + Passwort	☒ Verwalten von Benutzerberechtigungen
☒ Login mit biometrischen Daten	
☒ Anti-Viren-Software Server	☒ Zentrale Passwortvergabe
☒ Anti-Virus-Software Clients	☒ Richtlinie „Sicheres Passwort"
☒ Softwate-Firewall	☒ Richtlinie „Löschen / Vernichten"
☒ Intrusion Detection Systeme	☒ Richtlinie „Clean desk"
☒ Einsatz VPN bei Remote-Zugriffen	
☒ Verschlüsselung von Datenträgern	
☒ Verschlüsselung Smartphones	

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.

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**
☒ Trennung von Produktiv- und Testumgebung	☒ Trennung von Produktiv- und Testumgebung
☒ Mandantenfähigkeit relevanter Anwendungen	

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
☒ Anonymisierung von IP-Adressen.	☒ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

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
☒ Einsatz von VPN	☒ Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
☒ Protokollierung der Zugriffe und Abrufe	☒ Sorgfalt bei Auswahl von Transport-, Personal und Fahrzeugen
☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	

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.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
☒ Automatisierte Kontrolle der Protokolle	☒ 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)

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, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Feuer- und Rauchmeldeanlagen	☒ Backup & Recovery-Konzept (ausformuliert)
☒ Feuerlöscher Serverraum	☒ Kontrolle des Sicherungsvorgangs
☒ Serverraumüberwachung Temperatur und Feuchtigkeit	☒ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
☒ Serverraum klimatisiert	☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☒ USV	☒ Getrennte Partitionen für Betriebssysteme und Daten
☒ Schutzsteckdosenleisten Serverraum	
☒ RAID System / Festplattenspiegelung	
☒ Videoüberwachung Serverraum	
☒ Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	

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

☒ Zentrale Dokumentation aller Verfahrens-weisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …)	☒ Interner / externer Datenschutzbeauftragter
☒ Anderweitiges dokumentiertes Sicherheitskonzept	☒ Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet
☒ Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	☒ Regelmäßige Sensibilisierung der Mitarbeiter Mindestens jährlich
	☒ Interner / externer Informationssicherheits-beauftragter Name / Firma Kontakt

4.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von Firewall und regelmäßige Aktualisierung	☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
☒ Einsatz von Spamfilter und regelmäßige Aktualisierung	☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☒ Einsatz von Virenscanner und regelmäßige Aktualisierung	☒ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen
☒ Intrusion Detection System (IDS)	
☒ Intrusion Prevention System (IPS)	

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

Privacy by design / Privacy by default

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	

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
☒ Zugriffsbeschränkungen	☒ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
	☒ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
	☒ Schriftliche Weisungen an den Auftragnehmer
	☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
	☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags