Auftragsverarbeitungsvertrag

Zwischen

Name und Anschrift des Unternehmens
wie in AVV-Formular

– nachfolgend **Verantwortlicher** –

und

der **Smare Stefan Banse Michael Mühl GbR**
Hinter der Hage 25, 53501 Grafschaft

– nachfolgend **Auftragsverarbeiter** –

nachfolgend einzeln bezeichnet als „**Partei**“ sowie gemeinsam als „**Parteien**“.

Es ist Folgendes vereinbart:

Präambel

Der Auftragsverarbeiter lizenziert Smart-Rechner für die Integration auf Websites und erbringt im Rahmen der Bereitstellung der Smart-Rechner verschiedene Leistungen für den Verantwortlichen. Die Beauftragung des Auftragsverarbeiters erfordert eine Verarbeitung personenbezogener Daten. Dieser Auftragsverarbeitungsvertrag regelt für die Verarbeitung personenbezogener Daten die Rechte und Pflichten der Parteien nach Maßgabe der Standardvertragsklauseln der Europäischen Kommission (Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021, ABl. EU Nr. L 199 vom 7.6.2021 S. 18-30) gemäß Art. 28 Abs. 7 Datenschutz-Grundverordnung („**DSGVO**“). Sofern der Auftragsverarbeitungsvertrag punktuell Ergänzungen enthält, stehen diese weder unmittelbar noch mittelbar im Widerspruch zu den Standardvertragsklauseln oder beschneiden die Grundrechte oder Grundfreiheiten der betroffenen Personen.

Klausel 1

Zweck und Anwendungsbereich

a) Zweck der Klauseln: Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der 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) sichergestellt werden.

b) Zustimmung: Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.

c) Gegenstand der Verarbeitung: Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.

d) Bestandteile der Klauseln: Die Anhänge I bis IV sind Bestandteil der Klauseln.

e) Sonstige Verpflichtungen: Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

f) Ergänzung der Klauseln: Diese Klauseln stellen für sich allein genommen nicht sicher, dass die

Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

g) Vertragsverhältnisse: Die Parteien haben einen Lizenzvertrag über Nutzung der Smart-Rechner geschlossen („Hauptvertrag"). Grundlage dieses Vertragsverhältnisses sind die „Vertragsbedingungen zur Lizenzierung der Smart-Rechner".

Klausel 2

Unabänderbarkeit der Klauseln

a) Verpflichtung: Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

b) Erweiterung: Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3

Auslegung

a) Definitionen: Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Auslegung: Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.

c) Unvereinbarkeit: Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4

Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5

Beschreibung der Verarbeitung

a) Verarbeitungsvorgänge: Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 6

Pflichten der Parteien

6.1 Weisungen

a) Allgemeines: Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem

Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

b) Informationspflicht: Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

c) Anfängliche Weisungen: Dieser Auftragsverarbeitungsvertrag (Anhang II) und im Übrigen der Hauptvertrag beinhalten anfänglich dokumentierte Weisungen des Verantwortlichen an den Auftragsverarbeiter.

6.2 Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

6.3 Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

6.4 Sicherheit der Verarbeitung

a) Technische und organisatorische Maßnahmen: Der Auftragsverarbeiter ergreift mindestens die in seinem Verantwortungsbereich liegenden und in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) Vertraulichkeitsverpflichtung: Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

c) Alternative und adäquate Maßnahmen: Dem Auftragsverarbeiter ist es gestattet, alternative und adäquate technische und organisatorische Maßnahmen während der Laufzeit des Vertrages zu ändern oder anzupassen, solange sie das Sicherheitsniveau der bei Vertragsschluss implementierten Maßnahmen nicht unterschreiten und den gesetzlichen Anforderungen genügen.

6.5 Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten

enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

6.6. Dokumentation und Einhaltung der Klauseln

a) Nachweis: Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

b) Anfragen des Verantwortlichen: Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

c) Zurverfügungstellung von Informationen: Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

d) Prüfung: Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

e) Verweigerungsrecht: Der Auftragsverarbeiter ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Verantwortlichen, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragsverarbeiters sind oder wenn der Auftragsverarbeiter durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Verantwortliche ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragsverarbeiters, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragsverarbeiters, die nicht unmittelbar relevant für die vereinbarten Kontrollzwecke sind, zu erhalten.

f) Aufsichtsbehörden: Die Parteien stellen der zuständigen Aufsichtsbehörde die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

g) Beauftragung eines Dritten: Beauftragt der Verantwortliche einen Dritten mit der Durchführung der Kontrolle, hat der Verantwortliche den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftragsverarbeiter gegenüber dem Verantwortlichen verpflichtet ist. Zudem hat der Verantwortliche den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragsverarbeiters hat der Verantwortliche diesem die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Verantwortliche darf keinen Konkurrenten des Auftragsverarbeiters mit der Kontrolle beauftragen.

h) Verzicht auf eine Vor-Ort-Kontrolle: Nach Wahl des Verantwortlichen kann der Nachweis der Einhaltung der Pflichten nach diesem Vertrag anstatt durch eine Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit – z.B. nach BSI-Grundschutz – „Prüfungsberichts“) erbracht werden, sofern der Prüfbericht es dem Verantwortlichen in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

6.7 Einsatz von Unterauftragsverarbeitern

a) Allgemeine schriftliche Genehmigung: Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 14 Tage

im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann. Erhebt der Verantwortliche Einspruch, ist der Auftragsverarbeiter berechtigt, den Hauptvertrag und diesen Vertrag mit einer Frist von drei Monaten zu kündigen.

b) Datenschutzpflichten: Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

c) Kopien: Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Haftung: Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

e) Drittbegünstigtenklausel: Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

6.8 Internationale Datenübermittlungen

a) Dokumentierte Weisung: Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

b) Drittlandtransfer: Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 6.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

6.9. Pflichten des Verantwortlichen

a) Datenschutzrechtliche Vorschriften: Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung der Verantwortlichen-Daten sowie für die Wahrung der Rechte der Betroffenen im Verhältnis der Parteien zueinander allein verantwortlich.

b) Informationspflicht: Dem Verantwortlichen obliegt es, dem Auftragsverarbeiter die Daten rechtzeitig zur Leistungserbringung nach dem Hauptvertrag zur Verfügung zu stellen und er ist verantwortlich für die Qualität dieser Daten. Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung dieser Daten feststellt.

c) Zusammenarbeit mit Aufsichtsbehörden: Ist der Auftragsverarbeiter gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung der Daten zu erteilen oder mit diesen Stellen anderweitig zusammenzuarbeiten, so ist der Verantwortliche verpflichtet, den Auftragsverarbeiter auf erstes Anfordern bei der Erteilung solcher Auskünfte bzw. der Erfüllung anderweitiger Verpflichtungen zur Zusammenarbeit zu unterstützen.

Klausel 7

Unterstützung des Verantwortlichen

a) Unterrichtung über Anfragen: Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Pflichten: Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Unterstützung: Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

1. Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung"), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

2. Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

3. Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

4. Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.

d) Technische und organisatorische Maßnahmen: Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 8

Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

8.1 Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Meldung bei der Aufsichtsbehörde: Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

   1. die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
   2. die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
   3. die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

c) Meldung bei Betroffenen: bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

8.2 Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Informationspflicht: Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Verfügbarkeit von Informationen: Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Umfang der Informationen: Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

Klausel 9

Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Aussetzungsrecht: Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Kündigungsrecht für Verantwortliche: Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

1. der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

2. der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;

3. der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

c) Kündigungsrecht für Auftragsverarbeiter: Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

d) Löschung oder Anonymisierung: Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

e) Löschung oder Anonymisierung: Einer Löschung steht das Anonymisieren der Daten gleich.

f) Laufzeit und Kündigung: Die Laufzeit und Kündigung dieses Vertrags richten sich im Übrigen nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte ordentliche Kündigung dieses Vertrags ist ausgeschlossen. Das Recht zur außerordentlichen Kündigung bleibt unberührt.

g) Salvatorische Klausel: Sollte eine Bestimmung dieser Vereinbarung unwirksam sein oder werden, so wird dadurch die Gültigkeit dieser Vereinbarung im Übrigen nicht berührt. Die Parteien werden in einem solchen Fall die unwirksame Bestimmung durch eine gesetzeskonforme Regelung ersetzen.

h) Anwendbares Gericht und Gerichtsstand: Dieser Vertrag unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Frankfurt a.M.

ANHANG I

Liste der Parteien

Verantwortliche(r):

Name: (wie in AVV-Formular)

Anschrift: (wie in AVV-Formular)

Kontaktperson (Name, Funktion und Kontaktdaten): (wie in AVV-Formular)

Datenschutzbeauftragte(r) (Name, Funktion und Kontaktdaten):

Unterschrift und Beitrittsdatum:

Auftragsverarbeiter:

Name: Smare Stefan Banse Michael Mühl GbR

Anschrift: Hinter der Hage 2553501 Grafschaft, Deutschland

Kontaktperson:

Stefan Banse (Geschäftsführer)

0221 177 399 40

info@smart-rechner.de

Unterschrift und Beitrittsdatum:

Grafschaft, 08.02.2023

ANHANG II

Beschreibung der Verarbeitung

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

- Besucher digitaler Angebote wie Websites des Verantwortlichen, auf denen die Smart-Rechner integriert sind.
- Beschäftigte des Verantwortlichen, die mit der Integration der Smart-Rechner betraut sind.

Kategorien personenbezogener Daten, die verarbeitet werden

- Informationen über die aufgerufene Website des Verantwortlichen: Domain der Website, Art und Inhalt der Website, technische Informationen über die Website, Weiterleitungslink oder Suchanfrage, die den Nutzer auf die Website geleitet hat.
- Informationen über das verwendete Gerät von Nutzern der Website des Verantwortlichen**:** Informationen über den verwendeten Browser; Verbindungsdaten (IP-Adresse, Verbindungstyp, Datum und Uhrzeit der Serveranfrage sowie Anbieter der Verbindung); Hard- und Softwareinformationen des Geräts.

Art der Verarbeitung

- Beim Aufruf der Website werden Zugriffsdaten wie IP-Adresse, Browser- und Geräteinformationen aus der Serveranfrage der Nutzer an Smart-Rechner übermittelt, um die jeweils aktuelle und korrekte Berechnungslogik für die Smart Rechner von Servern des Hosting-Anbieters (IONOS SE, (Elgendorfer Str. 57, 56410 Montabaur, Deutschland) zu laden, und in Protokolldateien (Logfiles) gespeichert. Außerdem werden die von Nutzer:innen in der Eingabemaske angegeben Daten zur Berechnung der ausgewählten Resultate der Online-Rechner verarbeitet.
- Zugriffsdaten aus Serveranfragen und von Nutzer:innen eingegebene Daten werden nicht zur Identifizierung von einzelnen Nutzern verwendet und nicht mit anderen Datenquellen zusammengeführt.
- (Optional): Nach Einzelweisung des Verantwortlichen durch Aktivierung der Option „Google Charts Library“ in den Systemeinstellungen der Smart-Rechner werden beim Aufruf der Webseite zur Visualisierung von Ergebnissen der Smart-Rechner grafische Charts Programmbibliotheken (Google Charts Library) aus dem Content-Delivery-Network „jQuery“ von Google-Servern (Google Ireland Ltd., Gordon House, Barrow Street, Dublin 4, Irland und Google, LLC, 1600 Amphitheatre Parkway Mountain View, CA 94043, USA) geladen und zu diesem Zweck Zugriffsdaten wie IP-Adresse, Browser- und Geräteinformationen aus der Serveranfrage an Server von Google übermittelt.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden

- Laden der jeweils aktuellen und korrekten Berechnungslogik der Smart-Rechner
- Speicherung in Protokolldateien (Logfiles) zur Funktionsfähigkeit der Website und zur Gewährleistung der Sicherheit der informationstechnischen Systeme
- Bei Aktivierung der optionalen Verarbeitung: Visualisierung von Ergebnissen der Smart-Rechner mittels grafischer Charts durch Nutzung des Content-Delivery-Networks von Google

Dauer der Verarbeitung

- Nutzerdaten, insbesondere IP-Adressen, werden auf Servern der Smart-Rechner beim Hosting-Anbieter IONOS SE nach 7 Tagen anonymisiert und nach 9 Wochen vollständig gelöscht.

Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.

- Informationen zu Unterauftragsverarbeitern sind Anhang IV zu entnehmen.

Anfängliche Weisung

- Die Weisung zum Laden der jeweils aktuellen und korrekten Berechnungslogik der Smart-Rechner erteilt der Verantwortliche durch Implementierung des Programmcodes für das JavaScript des Auftragsverarbeiters.
- Durch Aktivierung von optionalen Verarbeitungen in den Systemeinstellungen der Smart-Rechner wie die Nutzung der Google Charts Library erteilt der Verantwortliche die Weisung, dass die Smart-Rechner die Programmbibliotheken zur Visualisierung von Ergebnissen aus dem Content-Delivery-Networks von Google lädt.

ANHANG III

Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten

I. Technische und organisatorische Maßnahmen von IONOS SE

Die stets aktualisierte Liste der technischen und organisatorischen Maßnahmen von IONOS SE kann hier hier abgerufen werden.

II. Technische und organisatorische Maßnahmen von Google (bei optionaler Verarbeitung)

Die stets aktualisierte Liste der technischen und organisatorischen Maßnahmen von Google kann hier (Appendix 2) abgerufen werden.

III. Technische und organisatorische Maßnahmen von Smart-Rechner

1. Management und Organisation

- Eine geeignete Organisationstruktur für Informationssicherheit ist vorhanden und die Informationssicherheit ist in die organisationsweiten Prozesse und Abläufe integriert
- Die Rollen der einzelnen Mitarbeiter im Sicherheitsprozess sind eindeutig festgelegt
- Konzepte und Dokumentationen im Sicherheitsumfeld werden regelmäßig überprüft und aktuell gehalten
- Die Rollen und Verantwortlichkeiten im Bereich der Sicherheit sind im eigenen Betrieb bekannt und besetzt (u.a. Informationssicherheitsbeauftragter (ISB), IT-Leiter, Datenschutzbeauftragter (DSB)
- Konsequente Einbindung des DSB bei Sicherheitsfragen
- Kenntnis der zuständigen Datenschutzaufsichtsbehörde sowie Wissen über die Meldeverpflichtungen nach Art. 33 und 34 DSGVO (Verletzung der Sicherheit)
- Vorhandensein von Eskalationsprozessen bei Sicherheitsverletzungen (Wer ist wann wie zu informieren?), u.a. im Notfallmanagement
- Aktive Unterstützung der Zusammenarbeit des DSB mit dem ISB durch die Unternehmensleitung Erkenntnisse über (neue) digitale Bedrohungen sind zu sammeln und potentielle Auswirkungen auf den eigenen Betrieb abzuleiten

2. Physikalische Sicherheit der Infrastruktur

- Es besteht ein umfassendes Gesamtkonzept zur Gebäudeabsicherung im Allgemeinen (z.B. Brandschutz, Zutrittsbeschränkung und -kontrolle)
- Es besteht ein Konzept zu Zutrittsregelungen und zur physischen Zugangskontrolle (Perimeterschutz)
- Klare Regelungen zum Umgang mit Besuchern (z.B. Begleitung, Sicherheitszonen, Besucherausweise, Protokollierung, Zuständiger Mitarbeiter für Besucher) als Bestandteil des Konzepts
- Verwendung von Feuer-/Rauchmeldeanlagen (im Rahmen des Brandschutzkonzepts)
- Das Gebäude (z.B. Wände, Fenster) und die Infrastruktur (z.B. Leitungen, Gefahrenmeldeanlagen) werden regelmäßig geprüft und gewartet
- Umzäunung des Betriebsgeländes
- Risiken durch Überflutung/Starkregen werden geprüft, insbesondere bei Serverräumen im Keller oder anderen gefährdeten Bereichen

3. Authentifizierung

- Einweisung aller Mitarbeiter in den Umgang mit Authentifizierungsverfahren und -mechanismen
- Verwendung von starken Passwörtern
- Überprüfung der Regel, dass Passwörter nach festgelegten Zeiträumen (z.B. 60 Tage) geändert werden müssen – falls diese Passwörter „stark“ sind, kann ein anlassloses Passwortwechselintervall deutlich länger ausfallen (z.B. einmal pro Jahr)
- Passwörter werden nach einem Sicherheitsvorfall, auch im Verdacht, gesperrt und müssen vom Nutzer neu vergeben werden

- Passwörter dürfen nicht weitergegeben werden (auch nicht an Kollegen, Vorgesetze oder die IT-Abteilung) – im Ausnahmefall (z.B. längere Erkrankung) wird das Passwort durch die IT zurückgesetzt und dieser Vorgang dokumentiert
- Unterrichtung der Beschäftigten, dass Passwörter nicht auf Zettel oder Pinnwänden aufgezeichnet werden dürfen
- Keine Speicherung von Passwörtern im Browser ohne Sicherung durch ein Masterpasswort
- Keine Mehrfachverwendung eines Passworts für verschiedene Dienste, sofern kein zentrales Identitätsmanagement (z.B. Active Directory) verwendet wird
- Es werden keine Passwörter per E-Mail übermittelt (z.B. für einen Firmenaccount zu einem Cloud-Dienst)
- Für lokale Admin-Konten werden besonders starke Passwörter verwendet (z.B. mind. 16-stellig, komplex und ohne übliche Wortbestandteile sowie unterschiedlich für jeden PC)

4. Rollen-/Rechtekonzept

- Keine Administratorkennungen für Nutzer, die keine administrativen Tätigkeiten ausführen
- Die Nutzung von Superuser (z.B. root unter Linux) wird soweit möglich nicht verwendet

5. Endgeräte (Clients)

- Eine Geräteverwaltung (Wer setzt welche Geräte in welchem Bereich ein?) ist vorhanden
- Automatisches Sperren nach einer gewissen Zeitspanne der Inaktivität, falls manuelles Sperren bei Verlassen des Einflussbereichs nicht gewährleistet werden kann
- Aktivierung einer Firewall, die unerwünschte Servicedienste auf dem Endgerät blockiert (z.B. versehentlich installierter Webserver)
- Verwendung einer Anti-Viren-Lösung bzw. eines Endpoint-Protection-Systems mit regelmäßigen, mindestens tagesaktuellen Signatur-Updates und Regelungen, wie im Falle einer Warnmeldung zu verfahren ist
- Konzept zum Patch Management vorhanden (u.a. Update-Plan mit Übersicht der eingesetzten Software)
- Regelmäßige Auswertung von Informationen zu Sicherheitslücken der eingesetzten Software wie Betriebssysteme, Office-Software und Fachanwendungen (z.B. durch E-Mail-Newsletter, Herstellerveröffentlichungen, Fachmedien, Sicherheitswarnungen)
- Automatisches Einspielen von Sicherheitsupdates des Betriebssystems, der installierten Software (z.B. PDF-Reader) oder von Softwarebibliotheken (z.B. Java), sofern möglich
- Personenbezogene Daten werden auf einem Speichermedium gespeichert, das von dem Backup erfasst wird (z.B. Netzlaufwerk)
- Die Einbindung von externen Geräten durch technische Maßnahmen wird auf das erforderliche Mindestmaß begrenzt (z.B. bei USB-Sticks, Smartphones, externe Festplatten)
- Nur Betriebssysteme und Software werden eingesetzt, für die noch Sicherheitsupdates zeitnah zur Verfügung gestellt werden
- Verhinderung der Ausführung von (aus dem Internet) heruntergeladener Software, deren Quellen als unsicher gekennzeichnet werden
- Anwendungen werden an den Endgeräten möglichst ohne Administratorrechte ausgeführt

6. Mobile Datenspeicher

- Einsatz von Backup- und Synchronisierungsmechanismen zur Verhinderung eines größeren Datenverlusts bei Verlust und Diebstahl
- Bei Smartphones: Zugang ausschließlich nach Authentifizierung (z.B. PIN, Passwort) – Länge der Kennung in Abhängigkeit von automatischen Sperr- und Löschfunktionen
- Bei Smartphones: Einsatz von biometrischen Zugangsverfahren nur bei ausschließlich lokaler Speicherung der biometrischen Templates innerhalb eines Secure-Chips auf dem Smartphone und bei personenbezogenen Daten mit keinem hohen Risiko
- Bei Smartphones: Nur sichere Quellen werden für die Installation von Apps verwendet. Apps werden vorher getestet und freigegeben
- Regelungen werden geprüft, ob es ausreichend ist, bei Nutzung mobiler Arbeitsplätze (z.B. Notebook auf Dienstreise) auf weniger Daten als innerhalb des internen Unternehmensnetzes zugreifen zu können
- Bei mobilen Datenträgern: Sicheres Löschen der Datenträger vor und nach der Verwendung ist sichergestellt

7. **Serversysteme**
   - Nur kompetent geschulte Personen dürfen Administrationstätigkeiten auf den Servern durchführen

8. **Websites und Webanwendungen**
   - Verwendung des HTTPS-Protokolls nach Stand der Technik (TLS1.2 oder TLS1.3)
   - Nur geschulte bzw. kompetente Personen dürfen Administrationstätigkeiten auf den Servern durchführen
   - Sperrung der Auffindung von Inhalten durch Suchmaschinen (über robots.txt), sofern diese Inhalte nicht durch eine Suchmaschine gefunden werden sollen

9. **Netzwerk**
   - Einsatz von Funkzugängen per WLAN nur auf aktuellen WLAN-Routern mit wirksamen Zugangsmechanismen (z.B. WPA-2 mit mind. 24-stelligem Passwort, WP3-Enterprise oder Einsatz eines Radius-Servers)
   - Nutzung eines WLAN-Gastzugang ohne Zugangsmöglichkeit zum internen Netzwerk
   - Prüfung eingehender E-Mails mittels Anti-Malwareschutz
   - Keine unverschlüsselten Protokolle (z. B. FTP, Telnet) werden verwendet

10. **Business Continuity**
    - Regelmäßige Tests, ob alle relevanten Daten im Backup-Prozess enthalten sind und die Wiederherstellung funktioniert
    - Weitestgehender Verzicht auf Makros in Office-Dokumenten im Betriebsalltag zum Schutz vor Ransomware
    - Zulassen ausschließlich signierter Microsoft Office-Makros oder (regelmäßige) Information, bspw. einmal pro Jahr, der Beschäftigten über Risiken einer Makro-Aktivierung (z.B. in Microsoft Word)

11. **Kryptographie**
    - Beschaffung von SSL-Zertifikaten bei vertrauenswürdigen Zertifizierungsstellen
    - HTTPS werden nach Stand der Technik (z.B. mind. 2048-Bit RSA, Perfect Forward Secrecy, HSTS, ggf. Client Zertifikate) eingesetzt

12. **Entwicklung und Auswahl von Software**
    - Es findet eine Trennung von Produktivsystem zu Entwicklungs-/Testsystem statt
    - Der Zugang zum Source-Code bei der Entwicklung von Software ist beschränkt
    - System- und Sicherheitstests, wie z.B. Code-Scan und Penetrationstests, werden durchgeführt
    - Ausreichende Testzyklen werden berücksichtigt
    - Standardsoftware und entsprechende Updates werden nur aus vertrauenswürdigen Quellen bezogen

13. **Auftragsverarbeiter**
    - Es werden nur Dienstleister verwendet, die die Garantien (in Form von Dokumenten) zur Verfügung stellen können
    - Sicherheitsmaßnahmen nach Art. 32 DSGVO als Bestandteil eines AV-Vertrags müssen zur Dienstleistung passen – das Abstraktionsniveau der Maßnahmen ist mitunter leicht höher als bei internen TOM-Listen eines Verantwortlichen

ANHANG IV

Liste der Unterauftragsverarbeiter

Der Verantwortliche nimmt für die Bereitstellung des Smart-Rechners folgende Unterauftragsverarbeiter in Anspruch:

Name: IONOS SE

Anschrift: Elgendorfer Str. 57, 56410 Montabaur

Beschreibung der Tätigkeiten: Eine stets aktualisierte Leistungsbeschreibung der Tätigkeiten von IONOS SE kann hier abgerufen werden.

Name: Google Ireland Ltd. und **Google LLC** (bei Aktivierung optionaler Verarbeitung, vgl. ANHANG II)

Anschriften:

Google Ireland Ltd.: Gordon House, Barrow Street, Dublin 4, Irland

Google LLC: 1600 Amphitheatre Parkway Mountain View, CA 94043, USA

Beschreibung der Tätigkeiten: Eine stets aktualisierte Leistungsbeschreibung der Tätigkeiten des Google CDN kann hier abgerufen werden. Weitere Informationen zur Verarbeitung können hier abgerufen werden.