Auftragsverarbeitungsvertrag (AVV)

V1.1

Stand: 01.01.2023

ais-security.de

advanced
it-security
solutions

AIS Advanced IT Security Solutions GmbH
Ensheimer Straße 42 | 66386 St. Ingbert
Germany

Kontakt:
+49 6894 38879 80
kontakt@ais-security.de

Steuernummer: 040/118/08439
Gerichtsstand: Amtsgericht Saarbrücken
Handelsregister: HRB 19077

Sparkasse Saarbrücken
IBAN: DE08 5905 0101 0067 1522 98
BIC: SAKSDE55XXX

Auftragsverarbeitungsvertrag (AVV)

Zwischen

dem Kunden

– nachstehend **„Auftraggeber“** genannt –

und

Advanced IT-Security Solutions GmbH, Ensheimer Straße 42, 66386 St. Ingbert

– nachstehend **„Auftragnehmer“** genannt –

wird vereinbart:

1. Präambel

Der Auftraggeber beauftragt den Auftragnehmer als Auftragsverarbeiter oder – wenn der Auftraggeber selbst Auftragsverarbeiter ist – als Unterauftragsverarbeiter mit der Verarbeitung von personenbezogenen Daten des Auftraggebers. Dieser Auftragsverarbeitungsvertrag (im Folgenden „AVV“) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien unter Berücksichtigung der Anforderungen des geltenden Datenschutzrechts. Er findet Anwendung auf alle Tätigkeiten, bei denen durch den Auftragnehmer eingesetzte Personen personenbezogene Daten des Auftraggebers verarbeiten.

2. Begriffsbestimmungen

Die in diesem AVV verwendeten Begriffe wie z.B. „personenbezogene Daten“, „Verarbeitung“, „Verantwortlicher“, „Auftragsverarbeiter“ oder „betroffene Person“ entsprechen den Begriffsbestimmungen der DSGVO, soweit in diesem AVV keine anderweitigen Definitionen enthalten sind. Unter „Daten des Auftraggebers“ sind ausschließlich solche personenbezogenen Daten zu verstehen, die entweder dem Auftragnehmer vom Auftraggeber überlassen oder vom Auftragnehmer ausschließlich für den Auftraggeber in dessen Auftrag verarbeitet wurden.

3. Gegenstand und Dauer, Art, Zweck und Mittel der Datenverarbeitung

Sparkasse Saarbrücken
IBAN: DE08 5905 0101 0067 1522 98
BIC: SAKSDE55XXX

Steuernummer: 040/118/08439
Gerichtsstand: Amtsgericht Saarbrücken
Handelsregister: HRB 19077

Kontakt:
+49 6894 38879 80
kontakt@ais-security.de

AIS Advanced IT Security Solutions GmbH
Ensheimer Straße 42 | 66386 St. Ingbert
Germany

(1) Der Gegenstand und die Dauer der Verarbeitung, die Art, der Zweck und die Mittel der Verarbeitung sowie die Art der personenbezogenen Daten und die Kategorien der betroffenen Personen sind in **Anhang 1** dieses AVV niedergelegt.

(2) Der Auftragnehmer ist im Rahmen der Erfüllung des Auftragsgegenstandes unter Einhaltung der Bestimmungen dieses AVV zur Durchführung aller erforderlichen Verarbeitungsschritte hinsichtlich der Daten des Auftraggebers (z.B. Duplizieren von Beständen für die Verlustsicherung, Anlegen von Logfiles, Zwischendateien und Arbeitsbereichen) berechtigt, soweit dies nicht zu einer inhaltlichen Umgestaltung der Daten des Auftraggebers führt.

4. Pflichten des Auftraggebers

(1) Der Auftraggeber ist allein gegenüber Dritten verantwortlich für die Einhaltung der auf den Verantwortlichen anwendbaren Vorschriften der Datenschutzgesetze; die Pflichten des Auftragnehmers und etwaige Rückgriffs- oder Schadensersatzansprüche bleiben hiervon unberührt. Der Auftraggeber hat die datenschutzrechtliche Zulässigkeit der Auftragsdatenverarbeitung und des Auftrages eigenverantwortlich selbst zu beurteilen. Der Auftraggeber ist für die Erfüllung der in den Artikeln 32 bis 36 DSGVO geregelten Pflichten des Verantwortlichen verantwortlich.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Der wird dem Auftragnehmer alle Informationen zur Verfügung stellen, die der Auftragnehmer zum Führen des Verzeichnisses nach Art. 30 Abs. 2 DSGVO benötigt.

(4) Dem Auftraggeber obliegt die Evaluierung und Bewertung der Wirksamkeit der getroffenen technischen und organisatorischen Maßnahmen (im Folgenden auch „TOMs“) zur Gewährleistung der Sicherheit der Verarbeitung. Soweit diese aus Sicht des Auftraggebers zur Gewährleistung der Sicherheit der Verarbeitung nicht ausreichend sind, werden die Parteien entsprechende Änderungen und deren kommerzielle Auswirkungen abstimmen und auf Basis einer entsprechenden schriftlichen Änderungsvereinbarung umsetzen.

(5) Im Fall einer Inanspruchnahme des Auftragnehmers oder des Auftraggebers durch eine betroffene Person oder eine in Art. 80 DSGVO genannte Stelle hinsichtlich etwaiger Ansprüche nach Art. 79 oder 82 DSGVO, verpflichten sich die Parteien, sich gegenseitig bei der Abwehr der Ansprüche zu unterstützen. Beide Parteien sind in diesem Zusammenhang berechtigt, Details des AVV, der Datenverarbeitung und von Weisungen des Auftraggebers zum Zwecke der Abwehr dieser Ansprüche oder zur Exkulpation nach Art. 82 Abs. 3 DSGVO gegenüber Dritten offenzulegen.

(6) Über die Aufbewahrung, Herausgabe oder Löschung der Daten des Auftraggebers nach Beendigung dieses AVV muss der Auftraggeber innerhalb einer vom Auftragnehmer gesetzten angemessenen Frist entscheiden. Geht dem Auftragnehmer innerhalb dieser Frist keine Entscheidung zu, ist der Auftragnehmer zur Löschung dieser Daten berechtigt, soweit keine rechtlichen Verpflichtungen des Auftragnehmers zur Aufbewahrung dieser Daten bestehen (ggf. in gesperrter Form).

(7) Soweit der Auftraggeber aufgrund des AVV Leistungen zu vergüten oder Aufwendungen zu erstatten hat, gelten die vom Auftragnehmer üblicherweise angebotenen Tagessätze.

Sparkasse Saarbrücken
IBAN: DE08 5905 0101 0067 1522 98
BIC: SAKSDE55XXX

Steuernummer: 040/118/08439
Gerichtsstand: Amtsgericht Saarbrücken
Handelsregister: HRB 19077

Kontakt:
+49 6894 38879 80
kontakt@ais-security.de

AIS Advanced IT Security Solutions GmbH
Ensheimer Straße 42 | 66386 St. Ingbert
Germany

(8) Der Auftraggeber wird Anfragen hinsichtlich der rechtlichen Anforderungen an die Datenverarbeitung, die seitens des Auftragnehmers nicht endgültig geklärt werden können, zeitnah bearbeiten und erforderlichenfalls durch Weisung regeln.

5. Pflichten des Auftragnehmers

(1) Der Auftragnehmer wird, unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, in seinem Verantwortungsbereich technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit dieser Auftragsverarbeitung auf Dauer sicherstellen sowie die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. Die vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sind in **Anhang 2** niedergelegt. Dem Auftraggeber sind diese TOMs bekannt. Er trägt die alleinige Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden personenbezogenen Daten ein angemessenes Schutzniveau bieten, und wird den Auftragnehmer von allen Ansprüchen Dritter freistellen, die daraus resultieren oder damit zusammenhängen, dass diese TOMs nicht ausreichend sind, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(2) Eine Änderung der getroffenen TOMs bleibt dem Auftragnehmer vorbehalten, es sei denn, dass das im **Anhang 2** niedergelegte Schutzniveau damit unterschritten wird.

(3) Der Auftragnehmer hat ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der TOMs zur Gewährleistung der Sicherheit der Verarbeitung etabliert.

(4) Der Auftragnehmer gewährleistet, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und anderen für den Auftragnehmer tätigen Personen diese Daten nur gemäß den Weisungen des Auftraggebers verarbeiten, sofern sie nicht gesetzlich zur Verarbeitung verpflichtet sind. Der Auftragnehmer gewährleistet ferner, dass sich die von ihm zur Verarbeitung der Daten des Auftraggebers eingesetzten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Diese Verpflichtung besteht auch nach Beendigung des Auftrags fort.

(5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes der Daten des Auftraggebers bekannt werden. Der Auftragnehmer kann in diesem Fall einstweilig und nach eigenem Ermessen in seinem Verantwortungsbereich angemessene Maßnahmen zum Schutze der Daten des Auftraggebers und zur Minderung möglicher nachteiliger Folgen treffen. Der Auftragnehmer informiert den Auftraggeber über etwaige von ihm getroffene Maßnahmen möglichst zeitnah.

(6) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO geregelten Pflichten des Auftraggebers. Der Auftragnehmer kann für diese Unterstützung eine angemessene Vergütung und die Erstattung von Aufwendungen verlangen.

Sparkasse Saarbrücken
IBAN: DE08 5905 0101 0067 1522 98
BIC: SAKSDE55XXX

Steuernummer: 040/118/08439
Gerichtsstand: Amtsgericht Saarbrücken
Handelsregister: HRB 19077

Kontakt:
+49 6894 38879 80
kontakt@ais-security.de

AIS Advanced IT Security Solutions GmbH
Ensheimer Straße 42 | 66386 St. Ingbert
Germany

(7) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

6. Geheimhaltungspflicht, Beachtung der datenschutzrechtlichen Regelungen und Grundsätze

(1) Der Auftragnehmer stellt sicher, dass alle Personen (Dritte oder Mitarbeiter), die Kenntnis von Daten des Auftraggebers erlangen können, personenbezogene Daten ausschließlich auf Weisung oder Anweisung verarbeiten und diesen AVV einhalten. Der Auftraggeber kann entsprechende Nachweise verlangen.

(2) Der Auftragnehmer stellt sicher, dass alle Personen (Dritte oder Mitarbeiter), die Kenntnis von Daten des Auftraggebers erlangen können, auf Geheimhaltung verpflichtet sind. Diese Verpflichtung besteht unter der DSGVO weiterhin für alle im vorstehenden Satz genannten Personen. Der Auftragnehmer stellt sicher, dass diese Personen davon unterrichtet sind, dass es untersagt ist, personenbezogene Daten unbefugt zu verarbeiten, sowie dass Sie personenbezogene Daten nur auf rechtmäßige Weise verarbeiten dürfen und die Vertraulichkeit und die Integrität personenbezogener Daten gewährleisten müssen. Der Auftraggeber kann entsprechende Nachweise verlangen.

(3) Der Auftragnehmer wird alle Daten des Auftraggebers logisch getrennt von eigenen Daten oder Daten Dritter halten. Test- und Ausschussmaterial wird der Auftragnehmer datenschutzgerecht vernichten. Dem Auftragnehmer ist es nicht gestattet, unautorisiert Kopien der personenbezogenen Daten zu erstellen; hiervon ausgenommen sind erforderliche Sicherheitskopien sowie elektronische Kopien, deren Erstellung zur Erfüllung des Leistungsvertrages erforderlich sind.

7. Bindung an Weisungen

(1) Der Auftragnehmer darf die Daten des Auftraggebers nur im Rahmen dieses AVV und der Weisungen des Auftraggebers – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeiten, sofern er nicht gesetzlich zur Verarbeitung verpflichtet ist. In diesem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen schriftlich oder per E-Mail (Textform) mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) „Weisungen“ sind die auf eine bestimmte Verarbeitung der Daten des Auftraggebers durch den Auftragnehmer gerichteten, dokumentierten Anordnungen des Auftraggebers. Sie werden anfänglich durch diesen AVV festgelegt und können vom Auftraggeber danach durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden (Einzelweisung). Tätigkeiten des Auftragnehmers auf Grund von Weisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind vom Auftraggeber nach Aufwand zusätzlich zu vergüten.

(3) Die Weisungen des Auftraggebers sind grundsätzlich in Textform zu erteilen; im Ausnahmefall erforderliche mündliche Weisungen sind vom Auftraggeber unverzüglich in Textform zu bestätigen. Weisungsberechtigte Personen auf Seiten des Auftraggebers und empfangsberechtigte Personen auf Seiten des Auftragnehmers werden der jeweils anderen Partei mitgeteilt.

Sparkasse Saarbrücken
IBAN: DE08 5905 0101 0067 1522 98
BIC: SAKSDE55XXX

Steuernummer: 040/118/08439
Gerichtsstand: Amtsgericht Saarbrücken
Handelsregister: HRB 19077

Kontakt:
+49 6894 38879 80
kontakt@ais-security.de

AIS Advanced IT Security Solutions GmbH
Ensheimer Straße 42 | 66386 St. Ingbert
Germany

(4) Es besteht keine materiell-rechtliche Prüfpflicht seitens des Auftragnehmers in Hinblick auf vom Auftraggeber erteilte Weisungen. Ist der Auftragnehmer jedoch der Auffassung, dass eine Weisung des Auftraggebers gegen die DSGVO oder andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt, informiert er den Auftraggeber unverzüglich in Textform. Der Auftragnehmer ist insoweit berechtigt, die Durchführung der vereinbarten Tätigkeit solange auszusetzen, bis der Auftraggeber über das weitere Vorgehen entschieden und den Auftragnehmer in Textform informiert hat. Etwaig hierdurch entstehende Mehraufwände des Auftragnehmers trägt der Auftraggeber. Der Auftraggeber trägt die alleinige Verantwortung für die von ihm getroffene Entscheidung. Hält der Auftraggeber an der erteilten Weisung fest und verlangt deren Umsetzung aus Sicht des Auftragnehmers ihm weiterhin ein rechtswidriges Handeln ab, ist der Auftragnehmer ist berechtigt, (i) die entsprechende Verarbeitung von der Stellung einer Sicherheit durch den Auftraggeber (z.B. Bürgschaft) abhängig zu machen, oder (ii) eine Entscheidung der zuständigen Aufsichtsbehörde einzuholen, oder (iii) die Verarbeitung nicht durchzuführen.

(5) Sollte der Auftragnehmer oder dessen Subunternehmer auf Grund der Umsetzung einer Weisung des Auftraggebers oder einer Entscheidung gemäß vorstehendem Abs. 4 von einem Dritten mit der Behauptung in Anspruch genommen werden, dass ihm wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, oder eine Aufsichtsbehörde infolgedessen eine Geldbuße gegen den Auftragnehmer oder dessen Subunternehmer verhängen oder androhen, stellt der Auftraggeber den in Anspruch Genommenen vollumfänglich von einer solchen Inanspruchnahme bzw. der Geldbuße frei. Der Freistellungsanspruch umfasst dabei auch die angemessenen Kosten der Rechtsverteidigung. Entsprechendes gilt, wenn eine Inanspruchnahme auf eine Verletzung der vertraglichen oder gesetzlichen Pflichten durch den Auftraggeber zurückzuführen ist.

8. Einschaltung von Unterauftragnehmern

(1) Der Auftragnehmer ist nach Maßgabe der in **Anhang 1** unter Ziffer 6 getroffenen Regelungen berechtigt, Subunternehmer als weitere Auftragsverarbeiter einzusetzen. Der Auftragnehmer wird die vertraglichen Vereinbarungen mit dem Subunternehmer so gestalten, dass dem Subunternehmer gegenüber dem Auftragnehmer dieselben datenschutzrechtlichen Verpflichtungen auferlegt werden, die in diesem AVV in Bezug auf den Auftragnehmer festgelegt sind, soweit in diesem AVV keine abweichenden Verpflichtungen zu Gunsten eines Subunternehmers vereinbart wurden. Die vorstehende Verpflichtung gilt insbesondere hinsichtlich der Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit hinsichtlich der personenbezogenen Daten. Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über die datenschutzrelevanten Verpflichtungen des Subunternehmers zu erhalten.

(2) Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Subunternehmers wie für eigenes Verschulden.

Sparkasse Saarbrücken
IBAN: DE08 5905 0101 0067 1522 98
BIC: SAKSDE55XXX

Steuernummer: 040/118/08439
Gerichtsstand: Amtsgericht Saarbrücken
Handelsregister: HRB 19077

Kontakt:
+49 6894 38879 80
kontakt@ais-security.de

AIS Advanced IT Security Solutions GmbH
Ensheimer Straße 42 | 66386 St. Ingbert
Germany

9. Hinweis-, Informations- und Auskunftspflichten

(1) Hinsichtlich dieses AVV ist der Auftraggeber für die Wahrung der nach Kapitel III der DSGVO vorgesehenen Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber im Rahmen seiner Möglichkeiten mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung seiner diesbezüglichen Verpflichtungen unterstützen. Der Auftragnehmer kann für diese Unterstützung eine angemessene Vergütung und die Erstattung von Aufwendungen verlangen, soweit nicht im Hauptvertrag ausdrücklich etwas anderes vereinbart ist.

(2) Wendet sich ein Betroffener mit der Geltendmachung von in der DSGVO geregelten datenschutzrechtlichen Betroffenenrechten an den Auftragnehmer, wird der Auftragnehmer den Betroffenen an den Auftraggeber verweisen, sofern eine Zuordnung der Betroffenenanfrage an den Auftraggeber nach den Angaben des Betroffenen möglich ist.

(3) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen.

(4) Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber zur Entscheidung weiterleiten.

10. Nachweise des Auftragnehmers, Inspektionen

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem AVV niedergelegten Pflichten nach und stellt dem Auftraggeber die hierfür erforderlichen Informationen zur Verfügung.

(2) Sollten im Einzelfall datenschutzrechtlich gebotene Inspektionen oder Überprüfungen durch den Auftraggeber oder einen von diesem beauftragten unabhängigen externen Prüfer, dessen Namen dem Auftragnehmer rechtzeitig im Voraus mitgeteilt wird, erforderlich sein (z.B. wenn der Auftraggeber begründete Zweifel an einem vom Auftragnehmer vorgelegten Selbstaudit hat), werden diese im Beisein eines Mitarbeiters des Auftragnehmers zu den üblichen Geschäftszeiten sowie ohne Störung des Betriebsablaufs in der Betriebsstätte des Auftragnehmers nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit (welche im Regelfall mindestens 4 Wochen beträgt) durchgeführt. Der Auftragnehmer darf diese von der Unterzeichnung einer angemessenen Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zum Auftragnehmer oder dessen Subunternehmer stehen, kann der Auftragnehmer eine Prüfung durch den Prüfer ablehnen.

(3) Der Auftraggeber stellt dem Auftragnehmer eine Kopie des vollständigen Auditberichts in digitaler Form zur Verfügung. Der Auftragnehmer darf den Auditbericht insbesondere auch seinen Subunternehmern überlassen.

Sparkasse Saarbrücken
IBAN: DE08 5905 0101 0067 1522 98
BIC: SAKSDE55XXX

Steuernummer: 040/118/08439
Gerichtsstand: Amtsgericht Saarbrücken
Handelsregister: HRB 19077

Kontakt:
+49 6894 38879 80
kontakt@ais-security.de

AIS Advanced IT Security Solutions GmbH
Ensheimer Straße 42 | 66386 St. Ingbert
Germany

(4) Für die Unterstützung bei der Durchführung der Inspektion bzw. Überprüfung darf der Auftragnehmer eine Vergütung gemäß Ziffer 4 Abs. 7 des AVV verlangen. Das Recht des Auftraggebers zur Inspektion bzw. Überprüfung gemäß vorstehenden Abs. 2 ist auf einen Tag pro Kalenderjahr begrenzt; Abweichungen sind mit dem Auftragnehmer in Textform zu vereinbaren.

11. Rückgabe und Löschung von Daten bei Vertragsbeendigung

(1) Nach Beendigung des AVV wird der Auftragnehmer, sofern technisch möglich und vom Auftraggeber gewünscht, die Daten des Auftraggebers gegen Vergütung des damit verbundenen Aufwandes herausgeben. Elektronisch gespeicherte Daten sind auf Wunsch und gegen Vergütung des damit verbundenen Aufwandes entweder in einem marktüblichen Format auf Datenträgern herauszugeben, wobei der Auftraggeber das Versandrisiko trägt, oder verschlüsselt online dem Auftraggeber zu übermitteln, wobei der Auftraggeber das Übermittlungsrisiko trägt.

(2) Der Auftragnehmer wird sämtliche elektronisch gespeicherte Daten des Auftraggebers, von denen der Auftraggeber keine Herausgabe gemäß Abs. 1 wünscht oder bei denen eine Herausgabe technisch nicht möglich ist, löschen oder im Fall von Backups oder Logfiles eine Beschränkung der Datenverarbeitung bis zum Zeitpunkt der Löschung sicherstellen. Der Auftragnehmer wird dem Auftraggeber die Löschung in Textform bestätigen.

(3) Daten des Auftraggebers, die nicht in elektronischer Form gespeichert sind und von denen der Auftraggeber keine Herausgabe gemäß Abs. 1 wünscht, werden durch den Auftragnehmer gegen Vergütung des damit verbundenen Aufwandes datenschutzkonform vernichtet. Auf Wunsch stellt der Auftragnehmer dem Auftraggeber einen Vernichtungsbeleg zur Verfügung. Der Vernichtungsbeleg seitens des Auftragnehmers für einen Zeitraum von 1 Jahr aufbewahrt.

(4) Die Verpflichtung zur Herausgabe oder Löschung besteht nicht, wenn der Auftragnehmer gesetzlich zur Aufbewahrung oder sonst zur Speicherung dieser Daten verpflichtet ist.

(5) Sofern der Auftraggeber eine Aufbewahrung seiner Daten über das Vertragsende hinaus wünscht, bedarf dies einer gesonderten Vereinbarung zwischen den Parteien. Die Parteien werden die entsprechenden Leistungen und kommerziellen Auswirkungen abstimmen und in einer entsprechenden schriftlichen Änderungsvereinbarung festlegen.

12. Datenschutzbeauftragter

Der Auftragnehmer hat – soweit dies Vorgaben der DSGVO gemäß Art. 37 ff. DSGVO vorschreiben – einen Datenschutzbeauftragten zu bestellen, der seine Tätigkeit gemäß den gesetzlichen Vorgaben ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zwecke der direkten Kontaktaufnahme mitgeteilt.

13. Kontrollen des Auftragnehmers und durch den Auftraggeber

(1) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion bei dem Auftragnehmer vornehmen, gelten grundsätzlich Ziffer 10 Abs. 2 und Abs. 4 Satz 1 des AVV entsprechend. Eine Unterzeichnung der Verschwiegenheitsverpflichtung ist in diesem Fall nicht erforderlich.

Sparkasse Saarbrücken
IBAN: DE08 5905 0101 0067 1522 98
BIC: SAKSDE55XXX

Steuernummer: 040/118/08439
Gerichtsstand: Amtsgericht Saarbrücken
Handelsregister: HRB 19077

Kontakt:
+49 6894 38879 80
kontakt@ais-security.de

AIS Advanced IT Security Solutions GmbH
Ensheimer Straße 42 | 66386 St. Ingbert
Germany

(2) Die Vertragsparteien werden sich wechselseitig über sämtliche behördliche Anfragen/Anordnungen und Verfahren, sämtliche Maßnahmen einer der in Art. 80 DSGVO genannten Stellen (wie z.B. Beschwerden, Abmahnungen, Geltendmachung von Ansprüchen) sowie sämtliche drohende oder laufende gerichtliche Verfahren, die die in diesem AVV geregelte Zusammenarbeit zum Gegenstand haben, unverzüglich informieren, im Zusammenhang mit diesen Anfragen, Anordnungen, Maßnahmen oder Verfahren eng zusammenarbeiten und sich wechselseitig alle erforderlichen Unterlagen und Angaben zur Verfügung stellen. Jede Partei ist in diesem Zusammenhang berechtigt, sämtliche diesen AVV, einschließlich der Details der Datenverarbeitung, betreffende Informationen und Unterlagen gegenüber der für sie zuständigen Aufsichtsbehörde oder sonstigen Dritten offenzulegen, soweit dies aus Sicht der Partei erforderlich ist.

14. Allgemeine Bestimmungen

(1) Änderungen und Ergänzungen dieses AVV und seiner Bestandteile bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(2) Die Parteien vereinbaren für diesen AVV die Geltung deutschen Rechts unter Ausschluss der Regelungen des internationalen Privatrechts. Der ausschließliche Gerichtstand für sämtliche Streitigkeiten aus oder im Zusammenhang mit diesem AVV ist der Sitz des Auftragnehmers.

Anhang 1: Einzelheiten zum Auftrag

Anhang 2: Technische und organisatorische Maßnahmen

Sparkasse Saarbrücken
IBAN: DE08 5905 0101 0067 1522 98
BIC: SAKSDE55XXX

Steuernummer: 040/118/08439
Gerichtsstand: Amtsgericht Saarbrücken
Handelsregister: HRB 19077

Kontakt:
+49 6894 38879 80
kontakt@ais-security.de

AIS Advanced IT Security Solutions GmbH
Ensheimer Straße 42 | 66386 St. Ingbert
Germany

Anhang 1: Einzelheiten zum Auftrag

1.) Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten:

- Durchführung von automatisierten IT-Sicherheitsanalysen über Findalyze entsprechend der von AIS bereitgestellten Produktinformationen, insbesondere:
  - Übermittlung von E-Mailadressen an die Plattform „Have I Been Pwned“ (https://haveibeenpwned.com) zum Abgleich mit bereits bekannten Datenabflüssen aus IT-Sicherheitsvorfällen
  - Übermittlung von IP-Adressen an die DNS-Dienste von Google und Cloudflare
  - Abruf von öffentlich zugänglichen Webinhalten (TLS-Zertifikate, Offene Ports, etc.)

2.) Dauer der Verarbeitung

Mindestens für die Dauer der Nutzung von Findalyze, danach solange es die gesetzlichen Aufbewahrungsfristen erfordern.

3.) Art der Daten:

☐ E-Mailadressen

☐ IP-Adressen

☐ Notizen und Anmerkungen zu Vorfällen und Ereignissen

☐ Inhalte öffentlich erreichbarer Webseite und sonstiger IT-Infrastruktur

☐ …

4.) Kreis der Betroffenen:

☐ Beschäftigte des Auftraggebers i. S. d. § 26 Abs. 8 BDSG

☐ Kunden des Auftraggebers

☐ Partner des Auftraggebers

5.) Frist nach Ziffer 4 Abs. 6 des AVV

Der Auftraggeber muss nach schriftlicher Aufforderung durch den Auftragnehmer innerhalb einer 14-tägigen Frist über die Herausgabe oder Löschung der Daten nach Beendigung des AVV entscheiden.

6.) Beauftragung von Subunternehmern

(1) Der Einsatz von Subunternehmern als weitere Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber eine vorherige Zustimmung in Textform erteilt.

Sparkasse Saarbrücken
IBAN: DE08 5905 0101 0067 1522 98
BIC: SAKSDE55XXX

Steuernummer: 040/118/08439
Gerichtsstand: Amtsgericht Saarbrücken
Handelsregister: HRB 19077

Kontakt:
+49 6894 38879 80
kontakt@ais-security.de

AIS Advanced IT Security Solutions GmbH
Ensheimer Straße 42 | 66386 St. Ingbert
Germany

(2) Zum Zeitpunkt des Vertragsabschlusses erteilt der Auftraggeber seine Zustimmung, dass die nachfolgend beschriebenen Teilleistungen unter Einschaltung folgender Subunternehmer durchgeführt werden:

Subunternehmer: Mircosoft Azure

Anschrift: Mircosoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA

Beschreibung der Teilleistung: Hosting

(3) Vor Hinzuziehung weiterer oder Ersetzung der aufgeführten Subunternehmer holt der Auftragnehmer die Zustimmung des Auftraggebers ein, wobei diese nicht ohne einen wichtigen datenschutzrechtlichen Grund verweigert werden kann.

(4) Der Auftragnehmer wird ggf. Verträge mit Subunternehmern unter Berücksichtigung der Art. 44 DSGVO ff. insbesondere auf Basis von EU-Standardverträgen abschließen.

Sparkasse Saarbrücken
IBAN: DE08 5905 0101 0067 1522 98
BIC: SAKSDE55XXX

Steuernummer: 040/118/08439
Gerichtsstand: Amtsgericht Saarbrücken
Handelsregister: HRB 19077

Kontakt:
+49 6894 38879 80
kontakt@ais-security.de

AIS Advanced IT Security Solutions GmbH
Ensheimer Straße 42 | 66386 St. Ingbert
Germany

1. Vertraulichkeit

a) <u>Zutrittskontrolle</u>

Maßnahmen, die geeignet sind, Unbefugten den Zugang zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet werden.

- Der Zutritt zum Gebäude ist durch ein Chipkarten-/Transponder-Schließsystem geregelt. Die besondere Schlossanlage lässt sich über zwei Methoden öffnen:
  1. Authentifizierung des Mitarbeiters über geeignete Software
  2. Zugang durch Ausgabe physikalischer Tokens.
- Die Ausgabe der Hardware-Tokens wird protokolliert.
- Eine Türsicherung (Tür lässt sich nur öffnen, wenn diese von innen aktiviert wird) ist vorhanden.
- Alle Mitarbeiter sind angewiesen, die Räumlichkeiten beim Verlassen zu verschließen.
- Eine Alarmanlage und Videoüberwachung sind installiert.
- Kunden – und Personalakten befinden sich in verschlossenen Schränken.
- Das Gebäude verfügt über feuerfeste Türen und über Panzerglasscheiben.

b) <u>Zugangs- und Benutzerkontrolle</u>

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

- Jeder Mitarbeiter benutzt einen Passwortmanager. Die zufällig generierten Passwörter folgen best practices was Länge und Komplexität anbelangt
- Auf allen Arbeitsplätzen ist eine automatische Bildschirmsperre mit Passwort-Aktivierung Pflicht
- Es werden getrennte Netzwerke für Arbeitsplätze, die Telefonanlage und den Applikationsserver verwendet. Die Netzwerke sind physikalisch voneinander getrennt und werden nach den gängigen Standards abgesichert.
- Für den Zugang über mobile Endgeräte nutzen wir eine MDM-Lösung zur Separierung von privaten und Geschäftsdaten

Sparkasse Saarbrücken
IBAN: DE08 5905 0101 0067 1522 98
BIC: SAKSDE55XXX

Steuernummer: 040/118/08439
Gerichtsstand: Amtsgericht Saarbrücken
Handelsregister: HRB 19077

Kontakt:
+49 6894 38879 80
kontakt@ais-security.de

AIS Advanced IT Security Solutions GmbH
Ensheimer Straße 42 | 66386 St. Ingbert
Germany

c) ***Zugriffskontrolle***

Maßnahmen, die gewährleisten, dass Personen nur im Rahmen ihrer Zugriffsberechtigung auf Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Jeder Mitarbeiter hat einen individuellen Login für seinen Arbeitsplatz und vorhandene Server-Zugriffe.
- Die Zugriffsrechte auf die verwendeten Systeme werden nach dem Need-to-Know-Need-to-Have Prinzip vergeben. Hierzu zählen insbesondere das Buchhaltungssystem, das CRM-System, Telefon-System und das Netzwerk.
- Die Zugriffsrechteverwaltung erfolgt durch dafür vorgesehene Systemadministratoren
- Die Verarbeitung sensibler persönlicher Daten erfolgt nur durch gesondert ernannte Mitarbeiter

d) ***Trennungskontrolle***

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Für Entwicklungs-, Test- und Produktionsbetrieb werden getrennte Umgebungen verwendet
- Innerhalb der Umgebungen werden Daten in getrennten Ordnern abgelegt
- Die logische Mandantentrennung ist softwareseitig umgesetzt

e) ***Pseudonymisierung & Verschlüsselung***

- Soweit möglich werden personenbezogener Daten pseudonymisiert verarbeitet. Dies betrifft insbesondere die automatische Überwachung der Systeme.

Sparkasse Saarbrücken
IBAN: DE08 5905 0101 0067 1522 98
BIC: SAKSDE55XXX

Steuernummer: 040/118/08439
Gerichtsstand: Amtsgericht Saarbrücken
Handelsregister: HRB 19077

Kontakt:
+49 6894 38879 80
kontakt@ais-security.de

AIS Advanced IT Security Solutions GmbH
Ensheimer Straße 42 | 66386 St. Ingbert
Germany

2. Integrität

a) <u>Eingabekontrolle/Verarbeitungskontrolle</u>

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Durch beschränkte Zugriffsrechte kann nicht jeder Mitarbeiter auf sämtliche Daten zugreifen
- Alle Mitarbeiter haben eine Verschwiegenheitserklärung unterzeichnet.

b) <u>Dokumentationskontrolle</u>

Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.

- Die zum Zweck der Entwicklung eingesetzten Software-Tools werden in einem Repository geführt

Sparkasse Saarbrücken
IBAN: DE08 5905 0101 0067 1522 98
BIC: SAKSDE55XXX

Steuernummer: 040/118/08439
Gerichtsstand: Amtsgericht Saarbrücken
Handelsregister: HRB 19077

Kontakt:
+49 6894 38879 80
kontakt@ais-security.de

AIS Advanced IT Security Solutions GmbH
Ensheimer Straße 42 | 66386 St. Ingbert
Germany

3. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und im Störfall wieder hergestellt werden können.

- Aufgrund einer cloudbasierten Lösung sind alle in der Software verwendeten (personenbezogenen) Daten vor physikalischen Einflüssen geschützt.
- Die Infrastruktur wird von Marktführern bereitgestellt, gesichert und unterliegt den gängigen Normen und Regelungen
- Alle Backups werden von externen Dienstleistern nach vereinbarten Zyklen gesichert

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Datenschutzfreundliche Voreinstellungen (Art.25 Abs 2 DSGVO): es werden nicht mehr personenbezogene Daten erhoben als für den jeweiligen Zweck erforderlich sind

Alle Mitarbeiter werden auf die geltenden datenschutzrechtlichen Grundlagen gemäß DSGVO hingewiesen. Alle Mitarbeiter unterzeichnen eine Verschwiegenheitserklärung

Sparkasse Saarbrücken
IBAN: DE08 5905 0101 0067 1522 98
BIC: SAKSDE55XXX

Steuernummer: 040/118/08439
Gerichtsstand: Amtsgericht Saarbrücken
Handelsregister: HRB 19077

Kontakt:
+49 6894 38879 80
kontakt@ais-security.de

AIS Advanced IT Security Solutions GmbH
Ensheimer Straße 42 | 66386 St. Ingbert
Germany