

Vereinbarung gemäß Art. 28 DSGVO über die Verarbeitung personenbezogener Daten im Auftrag

Zwischen

Vantarion GmbH
Mergenthalerallee 73-75
65760 Eschborn
- als Auftragsverarbeiter – (nachfolgend "Auftragnehmer")

und

- als Verantwortlicher – (nachfolgend "Auftraggeber")
(Auftraggeber und Auftragnehmer zusammen: "Parteien")

Präambel

Der Auftragnehmer erbringt auf Grundlage der bestehenden vertraglichen Vereinbarung vom [DATUM HAUPTVERTRAG] für den Auftraggeber (nachfolgend „Hauptvertrag“). Hierbei verarbeitet der Auftragnehmer personenbezogene Daten, für die der Auftraggeber verantwortlich im Sinne der DSGVO bzw. der datenschutzrechtlichen Vorschriften ist.

Mit der vorliegenden Vereinbarung zur Auftragsverarbeitung (nachfolgend „AVV“), sollen die jeweils damit verbundenen datenschutzrechtlichen Verpflichtungen konkret geregelt werden. Diese AVV soll dabei Anlage und Bestandteil des Hauptvertrages sein.

Begriffsbestimmungen:

In diesem Vertrag verwendete Begriffe, die in Artt. 4, 9 und 10 DSGVO definiert werden, sind im Sinne dieser gesetzlichen Definition zu verstehen.

§1 Umfang der Beauftragung

1.1. Die Regelungen dieser AVV gelten immer dann, sobald der Auftragnehmer im Rahmen seiner hauptvertraglichen Leistungserbringung Zugang/Zugriff zu personenbezogenen Daten (nachfolgend „Daten“) erhält, für die der Auftraggeber verantwortlich im Sinne der datenschutzrechtlichen Vorschriften ist. In diesen Fällen verarbeitet der Auftragnehmer Daten im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber bleibt hierbei Verantwortlicher im datenschutzrechtlichen Sinn. Für die Einhaltung aller datenschutzrechtlicher Vorgaben, insbesondere der DSGVO, aber auch dafür, dass die gesetzlichen Betroffenenansprüche im Zusammenhang mit personenbezogenen Daten eingehalten werden, ist insofern der Auftraggeber verantwortlich.

1.2. Die Datenverarbeitung durch den Auftragnehmer erfolgt in der Art, dem Umfang und zu dem Zweck wie in **Anlage 1** zu diesem Vertrag spezifiziert; die Verarbeitung betrifft die darin bezeichneten Arten personenbezogener Daten und Kategorien betroffener Personen. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.

1.3. Der Auftragnehmer ist berechtigt, die Daten zu anonymisieren oder zu aggregieren, so dass ein Rückschluss auf einzelne Betroffene nicht mehr möglich ist, und in dieser Form zum Zwecke der bedarfsgerechten Gestaltung, Weiterentwicklung und Optimierung sowie zur Erbringung des nach dem Hauptvertrag vereinbarten Dienstes zu verwenden. Die Parteien sind sich darüber einig, dass es sich bei den in vorgenannter Weise anonymisierten oder aggregierten Daten nicht mehr um personenbezogene Daten im Sinne dieses Vertrages handelt.

1.4. Die Datenverarbeitung durch den Auftragnehmer findet grundsätzlich innerhalb der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Es ist dem Auftragnehmer gleichwohl gestattet, Auftraggeberdaten unter Einhaltung der Bestimmungen dieses Vertrags auch außerhalb des EWR zu verarbeiten, wenn er den Auftraggeber vorab über den Ort der Datenverarbeitung informiert und die Voraussetzungen der Artt. 44 - 48 DSGVO erfüllt sind oder eine Ausnahme nach Art. 49 DSGVO vorliegt.

§2 Weisungsbefugnisse des Auftraggebers

2.1. Der Auftragnehmer verarbeitet die Daten entsprechend den Weisungen des Auftraggebers, sofern der Auftragnehmer nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

2.2. Die Weisungen des Auftraggebers sind grundsätzlich abschließend in den Bestimmungen dieses Vertrags festgelegt und dokumentiert. Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers und erfolgen nach Maßgabe des im Hauptvertrag festgelegten Änderungsverfahrens, in dem die Weisung zu dokumentieren und die Übernahme etwa dadurch bedingter Mehrkosten des Auftragnehmers durch den Auftraggeber zu regeln ist.

2.3. Der Auftraggeber hat dafür zu sorgen, dass Weisungen möglichst klar und nachvollziehbar sind. Weisungen dürfen dabei nicht gegen das Recht der EU oder der Mitgliedstaaten verstoßen. Ist eine Weisung aus der Sicht des Auftragnehmers unklar, so wird er den Auftraggeber unverzüglich schriftlich oder per E-Mail darauf hinweisen und um Klarstellung bitten.

2.4. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, ist er nach einer entsprechenden Mitteilung (z. B. per E-Mail oder über ein Ticketsystem) an den Auftraggeber berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen. Die Parteien stimmen darin überein, dass die alleinige Verantwortung für die weisungsgemäße Verarbeitung der Daten beim Auftraggeber liegt.

2.5. Der Auftraggeber benennt als weisungsbefugte Person gegenüber dem Auftragnehmer:

Vorname Nachname:

Tel. Nr.:

E-Mail:

2.6. Der Auftraggeber ist jederzeit berechtigt, die weisungsberechtigte Person und/oder deren Stellvertreter zu ersetzen. Änderungen sind jedoch zwingend vorab gegenüber dem Auftragnehmer in Textform anzuzeigen.

§3 Verantwortlichkeit des Auftraggebers

3.1. Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Daten sowie für die Wahrung der Rechte der Betroffenen im Verhältnis der Parteien zueinander allein verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund der

Verarbeitung von Daten nach Maßgabe dieses Vertrages Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.

3.2. Dem Auftraggeber obliegt es, dem Auftragnehmer die Daten rechtzeitig zur Leistungserbringung nach dem Hauptvertrag zur Verfügung zu stellen und er ist verantwortlich für die Qualität der Auftraggeberdaten. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

3.3. Der Auftraggeber wird dem Auftragnehmer auf Anforderung die in Art. 30 Abs. 2 DSGVO genannten Angaben zur Verfügung stellen, soweit sie dem Auftragnehmer nicht selbst vorliegen.

3.4. Ist der Auftragnehmer gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von Auftraggeberdaten zu erteilen oder mit diesen Stellen anderweitig zusammenzuarbeiten, so ist der Auftraggeber verpflichtet, den Auftragnehmer auf erstes Anfordern bei der Erteilung solcher Auskünfte bzw. der Erfüllung anderweitiger Verpflichtungen zur Zusammenarbeit zu unterstützen.

§4 Anforderung an das Personal

4.1. Zur Erfüllung seiner Verpflichtungen wird der Auftragnehmer ausschließlich Personen einsetzen, die sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheit unterliegen.

§5 Sicherheit der Verarbeitung (technisch organisatorische Maßnahmen)

5.1. Der Auftragnehmer wird gemäß Art. 32 DSGVO erforderliche, geeignete technische und organisatorische Maßnahmen ergreifen, die unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Datenverarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeberdaten zu gewährleisten.

5.2. Die aktuellen technisch organisatorischen Maßnahmen sind in der **Anlage 2** zu dieser AVV dargestellt.

5.3. Dem Auftragnehmer ist es gestattet, technische und organisatorische Maßnahmen während der Laufzeit des Vertrages zu ändern oder anzupassen, solange sie weiterhin den gesetzlichen Anforderungen genügen.

§6 Einschaltung von Subunternehmern

6.1. Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung, Subunternehmer hinsichtlich der Verarbeitung von Auftraggeberdaten hinzuzuziehen.

6.2. Die zum Zeitpunkt des Vertragsschlusses hinzugezogenen Subunternehmer ergeben sich aus der **Anlage 3**.

6.3. Der Auftragnehmer informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Der Einspruch ist innerhalb von 14 Tagen nach Zugang der Information über die Änderungen schriftlich gegenüber dem Auftragnehmer einzulegen. Kann keine einvernehmliche Lösung erzielt werden, erfolgt eine Einschränkung oder Beendigung der Auftragsverarbeitung.

6.4. Der Vertrag mit dem Unterauftragsverarbeiter muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann. In dem Vertrag mit dem Unterauftragsverarbeiter sind dieselben datenschutzrechtlichen Pflichten aus der vorliegenden Vereinbarung diesem wirksam aufzuerlegen.

6.5. Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Unterauftragsverarbeiter den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Abschnitt vertraglich auferlegt wurden.

6.6. Subunternehmer im Sinne dieser Vereinbarung sind nur solche, die Leistungen erbringen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung des Auftragnehmers aufweisen. Insbesondere stellen Dienstleister, die lediglich Nebenleistungen erbringen, wie die Prüfung oder Wartung von Datenverarbeitungsverfahren oder -anlagen durch andere Stellen, Telekommunikationsleistungen, Post- und Transportdienstleistungen, Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen keine Subunternehmer dar.

§7 Rechte der Betroffenen

7.1. Der Auftragnehmer wird den Auftraggeber mit technischen und organisatorischen Maßnahmen im Rahmen des Zumutbaren dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.

7.2. Soweit eine betroffene Person einen Antrag auf Wahrnehmung der ihr zustehenden Rechte unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen zeitnah an den Auftraggeber weiterleiten.

7.3. Der Auftragnehmer wird dem Auftraggeber Informationen über die gespeicherten Daten, die Empfänger von Daten, an die der Auftragnehmer sie auftragsgemäß weitergibt, und den Zweck der Speicherung mitteilen, sofern dem Auftraggeber diese Informationen nicht selbst vorliegen oder er sie sich selbst beschaffen kann.

7.4. Der Auftragnehmer wird es dem Auftraggeber ermöglichen, im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten, Auftraggeberdaten zu berichtigen, zu löschen oder ihre weitere Verarbeitung einzuschränken oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Einschränkung der weiteren Verarbeitung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.

7.5. Soweit die betroffene Person gegenüber dem Auftraggeber ein Recht auf Datenübertragbarkeit bezüglich der Auftraggeberdaten nach Art. 20 DSGVO besitzt, wird der Auftragnehmer den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei der Bereitstellung der Auftraggeberdaten in einem gängigen und maschinenlesbaren Format unterstützen, wenn der Auftraggeber sich die Daten nicht anderweitig beschaffen kann.

§8 Mitteilungs- und Unterstützungspflichten des Auftragnehmers

8.1. Trifft den Auftraggeber eine gesetzliche Melde- oder Benachrichtigungspflicht wegen einer Verletzung des Schutzes von Daten (insbesondere nach Artt. 33, 34 DSGVO), wird der Auftragnehmer den Auftraggeber unverzüglich über etwaige meldepflichtige Ereignisse in seinem Verantwortungsbereich informieren. Der Auftragnehmer wird den Auftraggeber bei der Erfüllung der Melde- und Benachrichtigungspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten unterstützen.

8.2. Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei etwa vom Auftraggeber durchzuführenden Datenschutz-Folgenabschätzungen und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Artt. 35, 36 DSGVO unterstützen.

§9 Datenlöschung

9.1. Überlassene Datenträger und Datensätze verbleiben im Eigentum des Verantwortlichen.

9.2. Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Auftraggeber, jedoch spätestens mit Beendigung der Leistungsvereinbarung, hat der Auftragnehmer sämtliche im Auftrag des Verantwortlichen verarbeitete personenbezogene Daten dem Verantwortlichen zurückzugeben oder nach vorheriger Zustimmung des Auftraggebers datenschutzgerecht zu löschen bzw. zu vernichten. Dies umfasst insbesondere dem Auftragsverarbeiter überlassene Daten, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigte Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen. Eine weitere Speicherung ist nur zulässig, wenn hierzu eine Verpflichtung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats besteht. Gleiches gilt für Test- und Ausschussmaterial. Ein Löschungsprotokoll ist dem Verantwortlichen auf Anforderung vorzulegen.

9.3. Der Auftragnehmer kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen bis zu deren Ende auch über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben. Für die nach Satz 1 aufbewahrten Daten gelten nach Ende der Aufbewahrungsfrist die Pflichten nach Ziffer 10.2. Nachweise und Überprüfungen

9.4. Der Auftragnehmer wird dem Auftraggeber auf dessen Anforderung alle erforderlichen und beim Auftragnehmer vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem Vertrag zur Verfügung stellen.

9.5. Der Auftraggeber ist berechtigt, den Auftragnehmer bezüglich der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, zu überprüfen; einschließlich durch Inspektionen.

9.6. Kommt es im Einzelfall zu einer Überprüfung durch den Auftraggeber oder von ihm beauftragten Prüfer, gilt Folgendes:

9.7. Überprüfungen und Kontrollen haben auf eigene Kosten des Auftraggebers zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs beim Auftragnehmer sowie unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers stattzufinden;

9.8. Überprüfungen und Kontrollen sind vorab unter Berücksichtigung einer angemessenen Vorlaufzeit beim Auftragnehmer anzumelden.

9.9. 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, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Überprüfungszwecke sind, zu erhalten.

9.10. Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Überprüfung zusammenhängenden Umstände zu informieren. Der Auftraggeber darf eine Überprüfung pro Kalenderjahr durchführen. Weitere Überprüfungen erfolgen gegen Kostenerstattung und nach Abstimmung mit dem Auftragnehmer.

9.11. Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Überprüfung, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund von dieser Ziffer 9.3 dieses Vertrags gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber ihm die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Wettbewerber des Auftragnehmers mit der Kontrolle beauftragen.

9.12. Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der Pflichten nach diesem Verträge anstatt durch eine Inspektion auch durch die Vorlage eines geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit – z. B. nach BSI-Grundschutz – („Prüfungsbericht“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

§10 Vertragsdauer und Kündigung

10.1. Die Laufzeit und Kündigung dieses Vertrags richten sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

§11 Haftung

11.1. Für die Haftung des Auftragnehmers nach diesem Vertrag gelten die Haftungsausschlüsse und -begrenzungen gemäß dem Hauptvertrag.

11.2. Soweit Dritte Ansprüche gegen den Auftragnehmer geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftraggebers gegen diesen Vertrag oder gegen eine seiner Pflichten als datenschutzrechtlich Verantwortlicher haben, stellt der Auftraggeber den Auftragnehmer von diesen Ansprüchen auf erstes Anfordern frei.

11.3. Der Auftragnehmer ist berechtigt, zum Zwecke der eigenen Enthaltung gemäß Art. 82 Abs. 3 DSGVO Details zu Weisungen des Auftraggebers sowie zur erfolgten Datenverarbeitung offenzulegen. Der Auftraggeber wird alles Erforderliche veranlassen, damit sich der Auftragnehmer in diesem Zusammenhang Dritten gegenüber enthaften kann.

11.4. Der Auftraggeber verpflichtet sich, den Auftragnehmer auch von allen etwaigen Geldbußen, die gegen den Auftragnehmer verhängt werden, in dem Umfang auf erstes Anfordern freizustellen, in dem der Auftraggeber Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

§12 Schlussbestimmungen

12.1. Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und dabei den Anforderungen des Art. 28 DSGVO genügt.

12.2. Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrags vor.

Datum, Ort, Unterschrift Auftraggeber

Datum, Ort, Unterschrift Auftragnehmer

Anlage 1

Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

Art und Zweck der beabsichtigten Verarbeitung

Der Auftragnehmer erbringt für den Auftraggeber Leistungen aus den Bereichen Informationssicherheit, Datenschutz und Compliance. Dazu zählen die Bereitstellung und der Betrieb der SaaS-Plattform VantarIS, Awareness-Schulungen und Phishing-Simulationen, Schwachstellenscans und Sicherheitsmonitoring, Penetrationstests und technische Sicherheitsanalysen, Managed Services und Managed Security Services, Beratung und Projektunterstützung, Audits und Reifegradbewertungen sowie der zugehörige Support. Welche Leistungen im Einzelnen geschuldet sind, ergibt sich aus dem Hauptvertrag nebst Leistungsbeschreibungen und Bestellungen.

Zweck der Verarbeitung ist ausschließlich die Erbringung dieser Leistungen. Dies umfasst insbesondere die Bereitstellung und Verwaltung von Nutzerzugängen, die Abbildung, Steuerung und Nachweisführung von Managementsystemen und regulatorischen Anforderungen, die Erkennung, Bewertung und Nachverfolgung von Schwachstellen und Sicherheitsvorfällen, die Durchführung und Auswertung von Schulungs- und Sensibilisierungsmaßnahmen, den Betrieb und die Administration der betreuten Systeme, die Erstellung von Dokumentationen, Prüfberichten und Auswertungen sowie die Bearbeitung von Support- und Serviceanfragen.

Die Verarbeitung umfasst das Erheben, Erfassen, Ordnen, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung an den Auftraggeber, Abgleichen, Einschränken, Löschen und Vernichten personenbezogener Daten. Sie erfolgt überwiegend automatisiert in den Systemen des Auftragnehmers und ergänzend nicht automatisiert im Rahmen von Beratungs-, Prüf- und Supporttätigkeiten. Bei Penetrationstests, Managed Services und Auditleistungen kann der Auftragnehmer prüfungs- oder betriebsbedingt Kenntnis von produktiven personenbezogenen Daten des Auftraggebers erlangen. Eine Kenntnisaufnahme erfolgt nur, soweit sie für die Leistungserbringung erforderlich ist.

Eine Verarbeitung zu eigenen Zwecken des Auftragnehmers findet nicht statt. Eine automatisierte Entscheidungsfindung einschließlich Profiling im Sinne des Art. 22 DSGVO erfolgt nicht. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.

Arten der personenbezogenen Daten

Verarbeitungsgegenstand personenbezogener Daten sind folgende Datenarten/-kategorien;

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Adressdaten, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, z.B. Auskunftsteilen, oder aus öffentlichen Verzeichnissen)
- IP- und Verbindungsdaten
- Protokoll- und Logdaten
- Nutzerkonten und Zugangsdaten
- Verhaltensdaten aus den Phishing-Tests

Arten personenbezogener Daten besonderer Art

- Keine -

Kategorien der betroffenen Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden
- Interessenten
- Beschäftigte
- Lieferanten
- Geschäftspartner
- Ansprechpartner
- Webseitenbesucher/-Nutzer
- Teilnehmer

Vantarion GmbH

Mergenthalerallee 73-75
65760 Eschborn
Geschäftsführer: Tobias Frank

Tel: 06196 / 573 82 0
mail@vantarion.de
www.vantarion.de

Amtsgericht Frankfurt am Main, HRB 142344
Steuernummer: 19/662/54567
USt-IdNr.: DE462847379

Bank: BANKING CIRCLE S.A. - GERMAN BRANCH
IBAN: DE90 2022 0800 0059 4178 40
BIC: SXPYDEHXXX

Anlage 2

Technische und organisatorische Maßnahmen des Auftragnehmers

1 Vertraulichkeit

1.1 Zutrittskontrolle

Mit welchen Maßnahmen wird der Zutritt zur Datenverarbeitungsanlage gegenüber unberechtigten Dritten gesichert?

Eigene Geschäftsräume des Auftragnehmers

- Gebäude und Zu- und Ausgangssicherung
- Alarmanlage
- Bewegungsmelder
- Einbruchmeldeanlagen (EMA)
- Schließanlage
- Sicherheitsschlösser
- Schlüsselkonzept (Schlüsselliste)
- Besucherregelung
- persönliche Besucherführung
- Keine Verarbeitung personenbezogener Daten des Auftraggebers auf lokalen Servern in den Geschäftsräumen

Externes Rechenzentrum (erbracht durch einen Subunternehmer nach Anlage 3)

- Zutritt ausschließlich für namentlich benannte und autorisierte Personen
- Vereinzelungsanlage bzw. Sicherheitsschleuse
- Magnet- oder Chipkarten
- Biometrische Zutrittskontrolle zu den Serverbereichen
- Videoüberwachung der Zutritts- und Serverbereiche
- Werkschutz/Wachpersonal, 24/7 besetzt
- Pförtner
- Besucherregelung mit Voranmeldung
- Besucherprotokollierung
- Besucherausweis
- Besucherbuch
- Ständige Begleitung von Besuchern und Fremdpersonal
- Standort des Rechenzentrums ausschließlich in Deutschland
- Regelmäßige Überprüfung der Maßnahmen des Rechenzentrumsbetreibers durch Zertifikate und Prüfberichte

1.2 Zugangskontrolle

Wie erfolgt der Zugang zur Systembenutzung bzw. zu den personenbezogenen Daten/ wie wird eine unbefugte Systembenutzung verhindert?

- Zwei-Faktor-Authentifizierung
- Authentifizierung mit Benutzername und Passwort
- Passwortvergabe

- Passwortrichtlinie zur Gewährleistung eines sicheren und vertraulichen Passworts
- automatische Sperrmechanismen, z.B. Passwortwiederholungssperre nach Fehlversuchen
- Verschlüsselung von abgelegten Passwörtern
- Anti-Viren-Software
- Anti-Spam-Gateway
- Software-Firewall
- Web Application Firewall (WAF) mit regelbasiertem Schutz auf Basis des OWASP Core Rule Set
- Verschlüsselung von Datenträgern und/oder externen Schnittstellen (USB, HDMI etc.)
- Verschlüsselung von mobilen Endgeräten
- Virtual Private Networks (VPN)
- Absicherung WLAN
- Netzwerksegmentierung
- Richtlinien Löschen/Vernichten von Daten
- Allgemeine Mitarbeiterrichtlinien zum Datenschutz und zur IT-Sicherheit (z. B. manuelle Desktopsperre, „Clean Desk“, ... gesunder Menschenverstand)

1.3 Zugriffskontrolle

Wie wird der Zugriff auf die Daten geschützt, so dass kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems möglich ist?

- Begrenzung der Administratoren auf das erforderliche Minimum
- Funktions- und rollenbasiertes Berechtigungskonzept
 - Leseberechtigung
 - Schreibberechtigung
 - Regelung zur Rechtegestaltung bei Urlaubsvertretung
- bedarfsgerechte Zugriffsrechte
- Protokollierung von Zugriffen
- Maßnahmen zur Speicherbegrenzung
- Protokollierte Datenvernichtung
- ordnungsgemäße Vernichtung von Datenträgern (ISO/IEC 21964);
- ordnungsgemäße Vernichtung von Papier (ISO/IEC 21964)
- Richtlinie zum Homeoffice/Telearbeit
- Dokumentiertes Löschkonzept mit definierten Löschfristen je Datenkategorie
- Technisch umgesetzte, automatisierte Löschroutinen
- Regelmäßige Überprüfung der Einhaltung der Löschfristen
- Löschung aus Datensicherungen im Rahmen der regulären Sicherungszyklen
- Dokumentation durchgeführter Löschungen

1.4 Trennungskontrolle

Gewährleisten Sie, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden getrennt verarbeitet werden?

- Festlegung von Datenbankrechten
- Logische Mandantentrennung
- Trennung von Produktiv- und Testsystem

- interne Anweisung, dass personenbezogene Daten bei Weitergabe zu pseudonymisieren oder nach Ablauf der Löschfrist zu anonymisieren sind.

2 Integrität

2.1 Weitergabekontrolle

Wie gewährleisten Sie, dass ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei einer elektronischen Übertragung oder einem Transport verhindert wird?

- Verschlüsselung
- Einsatz eines kryptographischen Verfahrens nach dem Stand der Technik
- E-Mail- Verschlüsselung
- Verschlüsselung von Datenträgern und Laptops/Notebooks
- Verschlüsselung von Inhalten auf Smartphones
- Verschlüsselung von mobilen Datenträgern (USB-Sticks, DVD etc.)
- Verschlüsselung von Passwörtern
- Datenaustausch über eine gesicherte Downloadplattform, Anbieter: VantarIS
- Virtual Private Networks (VPN)
- Richtlinie zum Homeoffice/Telearbeit
- Verpflichtung der Mitarbeiter zur Verschwiegenheit
- Verpflichtung der Mitarbeiter auf das Fernmeldegeheimnis (§ 3 TDDDG)
- Verpflichtung der Mitarbeiter auf das Sozialgeheimnis (§ 35 SGB I)

2.2 Eingabekontrolle

Können Sie feststellen, ob und von wem personenbezogene Daten in Ihr Datenverarbeitungssystem eingegeben, verändert oder entfernt worden sind?

- Protokollierung der Eingabe, Veränderung und Löschung von Daten
- Funktions- und rollenbasiertes Berechtigungskonzept
- Schreibberechtigung
- Leseberechtigung
- Dokumentenmanagement
- Nachvollziehbarkeit von Eingaben
- Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) → Benutzeridentifikation
- Klare Zuständigkeiten für Löschungen

3 Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Gewährleisten Sie den Schutz der Daten gegen mutwillige oder zufällige Zerstörung?

- Backup-Strategie (online/offline; on-site/off-site)[Bsp. NAS- System: verschlüsseltes Back UP Auslagerung bei einem externen Anbieter]
- Verschlüsselte Backupdatenträger

- unterbrechungsfreie Stromversorgung (USV)
- Virenschutz, eingesetzte(s) System(e): ClamAV, Microsoft Defender
- Firewall, eingesetzte(s) System(e): PfSense
- Festplatten im RAID-Verbund
- Redundantes Netzteil
- Überwachung Zustand/Funktionen relevanter Systeme (Monitoring)
- Regelmäßige Updates / Patchmanagement
- Meldewege und Notfallpläne (z. B. BSI IT-Grundschutz 200-4¹)
- Feuer- und Rauchmelder
- Feuerlöschgeräte vor Serverraum
- Schutzsteckdosenleisten Serverraum
- Alarmmeldung bei unberechtigtem Zutritt zum Serverraum
- Überwachung Temperatur und Feuchtigkeit in Serverraum

3.2 Rasche Wiederherstellbarkeit

Setzen Sie Maßnahmen ein, welche die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen?

- dokumentiertes Notfallkonzept

3.3 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Welche Prozesse und Abläufe haben Sie auf organisatorischer Ebene im Unternehmen umgesetzt, um die Sicherheit der Datenverarbeitung zu gewährleisten?

- Datenschutz-Management
- Bestellung von Datenschutzkoordinatoren
- zentrale Dokumentation aller Verarbeitungstätigkeiten
- Richtlinie für Mitarbeiter zum Umgang mit Datenpannen
- Richtlinie für Mitarbeiter zum Umgang mit Betroffenenrechten
- Schulungskonzept zum Datenschutz
- IT-Sicherheitsbeauftragter
- Datenschutzinformationen gemäß Artt. 13, 14 DSGVO (Datenschutzerklärung),
- Unterstützung bei Reaktionen auf Sicherheitsverletzungen
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO); z.B. keine vorangeklickten Checkboxen in Onlineformularen
- Auftragskontrolle, d.h. keine Auftragsdatenverarbeitung im Sinne von Artt. 28, 29 DSGVO ohne entsprechende Weisung des Auftraggebers
- eindeutige Vertragsgestaltung
- formalisiertes Auftragsmanagement
- strenge Auswahl des Dienstleisters
- Vorabüberzeugungspflicht, z. B. durch Zertifikate
- Nachkontrollen

¹ https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard04/ITGStandard04_node.html

- Regelmäßige automatisierte Schwachstellenscans der Systeme und der Anwendung
- Penetrationstests der Anwendung und der Infrastruktur
- Bewertung, Priorisierung und Nachverfolgung festgestellter Schwachstellen bis zur Behebung
- Regelmäßige Überprüfung und Wirksamkeitskontrolle der technischen und organisatorischen Maßnahmen (Art. 32 Abs. 1 lit. d DSGVO)

Anlage 3

Subunternehmer

Für die Datenverarbeitung im Auftrag des Auftraggebers setzt der Auftragnehmer die Leistungen von Dritten ein, die in seinem Auftrag Daten verarbeiten („Subunternehmer“).

Unternehmen	Anschrift	Zweck der Datenverarbeitung	Ort der Datenverarbeitung
centron GmbH	Heganger 29 96103 Hallstadt	Hosting des Webserver und der Infrastruktur.	Deutschland
Enginsight GmbH	Leutragraben 1, 07743 Jena	Support für die Plattform zur Durchführung von Schwachstellenscans und Penetrationstests	Deutschland
IONOS SE	Elgendorfer Str. 57 56410 Montabaur	Bereitstellung von KI-Diensten zur Datenanalyse und Vorschlagsgenerierung	Deutschland