Anlage Vertrag über die Verarbeitung von Daten im Auftrag

Version 1.3

zwischen

Kunde

- Auftraggeber -

und

Süddeutsche Datenschutzgesellschaft mbH
Von-Brettreich-Straße 4, 93049 Regensburg
93049 Regensburg

- Auftragnehmer -

1. Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i. S. d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i. S. d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

(3) Dieser Auftragsverarbeitungsvertrag ist Bestandteil der Allgemeinen Geschäftsbedingungen zwischen dem Kunden und der Süddeutschen Datenschutzgesellschaft mbH und wird automatisch mit Abschluss des Hauptvertrages abgeschlossen. Einer gesonderten Unterschrift bedarf es nicht.

(4) Sollten einzelne Teile der allgemeinen Geschäftsbedingungen unwirksam sein, so berührt dies die Wirksamkeit dieses Vertrages nicht.

2. Gegenstand des Auftrags

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag festgelegt.

3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 3 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen.

(4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

(5) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(6) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

(2) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers

nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

5. Meldepflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

(2) Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

6. Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 11 dieses Vertrages.

(2) Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber mit. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(3) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

7. Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i. S. d. Absatzes 1 erforderlich ist.

(3) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören. Die Parteien gehen davon aus, dass eine Kontrolle höchstens einmal jährlich erforderlich ist. Weitere Prüfungen sind vom Auftraggeber unter Angabe des Anlasses zu begründen. Im Falle von Vor-Ort-Kontrollen wird der Auftraggeber dem Auftragnehmer die entstehenden Aufwände inkl. der Personalkosten für die Betreuung und Begleitung der Kontrollpersonen vor Ort in angemessenen Umfang ersetzen. Die Grundlagen der Kostenberechnung werden dem Auftraggeber vom Auftragnehmer vor Durchführung der Kontrolle mitgeteilt.

(4) Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen anstatt einer 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 erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anlage 3 zu diesem Vertrag zu überzeugen. Sollte der Auftraggeber begründete Zweifel an der Eignung des Prüfdokuments i. S. d. Satzes 1 haben, kann eine Vor-Ort-Kontrolle durch den Auftraggeber erfolgen. Dem Auftraggeber ist bekannt, dass eine Vor-Ort-Kontrolle in Rechenzentren nicht oder nur in begründeten Ausnahmefällen möglich ist.

(5) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i. S. d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

8. Unterauftragsverhältnisse

(1) Der Auftragnehmer ist berechtigt, die in der **Anlage 2** zu diesem Vertrag angegebenen Unterauftragnehmer für die Verarbeitung von Daten im Auftrag einzusetzen. Der Wechsel von Unterauftragnehmern oder die Beauftragung weiterer Unterauftragnehmer ist unter den in Absatz 2 genannten Voraussetzungen zulässig.

(2) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Der Auftragnehmer wird den Auftraggeber im Falle eines geplanten Wechsels eines Unterauftragnehmers oder bei geplanter Beauftragung eines neuen Unterauftragnehmers rechtzeitig, spätestens aber 4 Wochen vor dem Wechsel bzw. der Neubeauftragung in Textform informieren („Information“). Der Auftraggeber hat das Recht, dem Wechsel oder der Neubeauftragung des Unterauftragnehmers unter Angabe einer Begründung in Textform binnen drei Wochen nach Zugang der „Information“ zu widersprechen. Der Widerspruch kann vom Auftraggeber jederzeit in Textform zurückgenommen werden. Im Falle eines Widerspruchs kann der Auftragnehmer das Vertragsverhältnis mit dem Auftraggeber mit einer Frist von mindestens 14 Tagen zum Ende eines Kalendermonats kündigen. Der Auftragnehmer wird bei der Kündigungsfrist die Interessen des Auftraggebers angemessen berücksichtigen. Wenn kein Widerspruch des Auftraggebers binnen drei Wochen nach Zugang der „Information“ erfolgt, gilt dies als Zustimmung des Auftraggebers zum Wechsel bzw. zur Neubeauftragung des betreffenden Unterauftragnehmers.

(3) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind.

(4) Nicht als Unterauftragsverhältnisse i. S. d. Absätze 1 bis 6 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-Systemen oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i. S. d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

9. Fernwartung

(1) Sofern der Auftragnehmer die Wartung und/oder Pflege der IT-Systeme auch im Wege der Fernwartung durchführt, ist der Auftragnehmer verpflichtet, dem Auftraggeber eine wirksame Kontrolle der Fernwartungsarbeiten zu ermöglichen. Dies kann z.B. durch Einsatz einer Technologie erfolgen, die dem Auftraggeber ermöglicht, die vom Auftragnehmer durchgeführten Arbeiten auf einem Monitor o.ä. Gerät zu verfolgen.

(2) Wenn der Auftraggeber bei Fernwartungsarbeiten nicht wünscht, die Tätigkeiten an einem Monitor o.ä. Gerät zu beobachten, wird der Auftragnehmer auf Wunsch des Auftraggebers die von ihm durchgeführten Arbeiten in geeigneter Weise dokumentieren.

10. Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet.

(2) Der Auftragnehmer hat seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht und zur Vertraulichkeit verpflichtet.

(3) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

11. Wahrung von Betroffenenrechten

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

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

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

(4) Für den Fall, dass ein Betroffener seine Rechte nach den Art. 12-23 DSGVO beim Auftragnehmer geltend macht, obwohl dies offensichtlich eine Verarbeitung personenbezogener Daten betrifft, für die der Auftraggeber verantwortlich ist, ist der Auftragnehmer berechtigt, dem Betroffenen mitzuteilen, dass der Auftraggeber der Verantwortliche für die Datenverarbeitung ist. Der Auftragnehmer darf dem Betroffenen in diesem Zusammenhang die Kontaktdaten des Verantwortlichen mitteilen.

12. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

13. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 3** zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann einmal jährlich oder bei begründeten Anlässen eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

14. Dauer des Auftrags

(1) Der Vertrag beginnt mit Unterzeichnung und läuft für die Dauer des zwischen den Parteien bestehenden Hauptvertrages über die Nutzung der Dienstleistungen des Auftragnehmers durch den Auftraggeber.

(2) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

15. Beendigung

Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt.

16. Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

17. Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Für Nebenabreden ist die Schriftform erforderlich.

(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Anlage 1 - Gegenstand des Auftrags

1. Gegenstand und Zweck der Verarbeitung

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

- Erkennen von Cybergefahren, automatische Sicherheits-Checks, Endpunktescans, Updates, Monitoring der IT-Infrastruktur, Überwachung der Webseiten und/oder Server des Auftraggebers.

- Auswertung und Einblick in die generelle Bedrohungs- und Sicherheitslage der IT-Infrastruktur durch PDF-Berichte, Analyse von Software auf Sicherheitslücken, Ermöglichung von automatisiert ausführbaren Skripten. Weiteres ergibt sich aus dem Hauptvertrag.

2. Art(en) der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

Metadaten, Benutzerdaten, Benutzerinformationen, Anwesenheits-, Abwesenheitszeiten, Prozessor, Arbeitsspeicher und Netzwerkauslastung, Geräte-ID, laufende Prozesse und Dienste, IP-Adressen, Sicherheitsstatus, Installierte Software, Kommunikationsdaten. Weiteres ergibt sich aus dem Hauptvertrag.

3. Kategorien betroffener Person

Kreis der von der Datenverarbeitung betroffenen Personen:

Auftraggeber, Beschäftigte des Auftraggebers, Interessenten, Ansprechpartner, Externe Mitarbeiter

Anlage 2 – Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende(s) Unternehmen:

Unternehmen	**Adresse**	**Leistung**	**Severstrandort**
Enginsight GmbH	Leutragraben 1 07743 Jena	Support & Programmierung	Deutschland
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen	Hosting Sicherheitsportal	Deutschland
AD IT Systems GmbH	Ostendstraße 132, 90482 Nürnberg	Support Sicherheitsportal	Deutschland
Amazon Web Services EMEA Sarl	38 Avenue John F. Kennedy, L-1855 Luxembourg	Versand der Benachrichtigungen/Alarme per SMS	Deutschland und EU
Microsoft Ireland Operations Ltd.	South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521 Irland	Versand der Benachrichtigungen/Alarme per E-Mail	Deutschland und EU

Anlage 3

Technische und organisatorische Maßnahmen des Auftragnehmers

1. Vertraulichkeit der Verarbeitung gem. Art. 32 Abs. 1 lit. b) Var. 1 DSGVO

1.1. Zugangskontrolle

Die Zugangskontrolle (vormals Zutrittskontrolle) beschreibt Maßnahmen, die Unbefugten den Zugang zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, verwehren.

Technische Maßnahmen
☒ Manuelles Schließsystem oder mechatronisches Schließsystem
☒ Arbeitsplatzrechner sind in verschlossenen Räumen
☒ Türen mit Knauf an der Außenseite
☒ Umfriedung des Betriebsgeländes
☒ Lichtschranken / Bewegungsmelder
☒ Keine Außenfenster im Rechenzentrum bzw. Serverraum
☒ Automatisches Sperren der Endgeräte nach einer gewissen Zeitspanne der Inaktivität (Bildschirmsperre)
☒ Deaktivierung von nicht genutzten Netzwerkdosen

Organisatorische Maßnahmen
☒ Dokumentierte Schlüsselverwaltung
☒ Schließregelung
☒ Empfang / Rezeption / Pförtner
☒ Gelebte Regelung für den Zutritt von Firmenfremden (z.B. Begleitung, Zutrittsverbote, Ausweise)

1.2. Datenträger- und Speicherkontrolle

Die Datenträgerkontrolle beschreibt Maßnahmen, die das unbefugte Lesen, Kopieren, Verändern oder Löschen von Datenträgern verhindern. Die Speicherkontrolle beschreibt Maßnahmen zur Verhinderung der unbefugten Eingabe sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

Technische Maßnahmen
☒ Einsatz von Aktenvernichter (mind. Sicherheitsstufe DIN 66399: P4 mit max. 160 mm² pro Partikel und 6mm Streifenbreite oder P5 mit max. 30 mm² pro Partikel und 2mm Streifenbreite)
☒ Dokumentation der Vernichtung von Papier

Organisatorische Maßnahmen
☒ Es gibt eine Regelung, welche Daten auf welcher Rechtsgrundlage aufbewahrt werden müssen und wie lange die Aufbewahrungsfrist ist.

Verschlüsselung gem. Art. 32 Abs. 1 lit. a) DSGVO
☒ Einsatz starker Verschlüsselung der mobilen Endgeräte (Smartphones und Tablets) und mobilen Datenträger (z.B. USB-Sticks, Festplatten)
☒ Alle produktiv eingesetzten Verschlüsselungstechnologien entsprechen dem Stand der Technik.
☒ Starke Verschlüsselung von Datenträgern in Laptops & Clients

1.3. Benutzerkontrolle

Die Benutzerkontrolle beschreibt Maßnahmen zur Verhinderung der Nutzung von automatisierten Verarbeitungssystemen unter Einsatz von Einrichtungen zur Datenübertragung durch Unbefugte. Hierunter kann auch der Schutz vor unberechtigter Systemnutzung, sowie vor Systemeinbrüchen und -missbrauch über Netzwerke gefasst werden.

Technische Maßnahmen
☒ Verwendung einer Anti-Viren-Lösung auf Client-Rechnern und Notebooks mit tagesaktueller Aktualisierung der Signaturdatenbanken
☒ Verwendung eines Endpoint-Protection-System auf Client-Rechnern und Notebooks mitsamt automatischen On-Access-Scans
☒ Prüfung eingehender E-Mails mittels Anti-Malwareschutz
☒ Einsatz von Intrusion Detection Systeme (Angriffserkennungssystem)
☒ Einsatz von Intrusion Prevention System (IPS)
☒ Einsatz von Funkzugängen per WLAN nur auf aktuellen WLAN-Routern mit wirksamen Zugangsmechanismen

☒ Nutzung eines WLAN-Gastzugang ohne Zugangsmöglichkeit zum internen Netzwerk
☒ Es wird nur Software eingesetzt, für die noch Sicherheitsupdates zeitnah zur Verfügung gestellt werden.

1.4. Zugriffskontrolle

Die Zugriffskontrolle beschreibt Maßnahmen zur Sicherstellung der ausschließlichen Benutzung von automatisierten Verarbeitungssystemen durch Berechtigte unter ihrer umfassten Zugangsberechtigung und bietet damit Gewährleistung, dass die Berechtigten nur Zugang zu Daten haben, die von ihrer Berechtigung umfasst sind.

Technische Maßnahmen
☒ Login mit Benutzername & Passwort
☒ Einsatz von biometrischen Merkmalen für den Login auf IT-Geräten oder in Sicherheitszonen (z.B. Fingerprint, FaceID etc.)
☒ Bei Smartphones: Zugang ausschließlich nach Authentifizierung (z. B. PIN, Passwort)
☒ Einsatz von Verfahren zur Zwei- oder Mehr-Faktor-Authentifizierung bei Verarbeitungstätigkeiten mit hohem Risiko
☒ Einsatz von Zwei- oder Mehr-Faktor-Authentifizierung bei Admin-Konten
☒ Für die Admin-Konten der IT-Systeme werden ausschließlich starke Passwörter verwendet (z.B. mind. 16 Zeichen, komplex und ohne übliche Wortbestandteile).
☒ Nicht-privilegierte Standardkonten auch für Administratoren für die sonstige Arbeit außerhalb der administrativen Tätigkeit.
☒ Keine Abhängigkeit des gesamten Betriebs von einzelnen Beschäftigten mit Administratorenkennungen.
☒ Sichere Aufbewahrung zentraler Administrationszugangsdaten (z. B. im Tresor) und Zugangsmöglichkeiten im Notfall.
☒ Verschiedene Administrationsrollen mit Rechten nach dem Least-Privileg-Prinzip für unterschiedliche Administrationsaufgaben (z. B. Softwareupdates, Konfiguration, Backup) einsetzen.
☒ Verpflichtende Verwendung starker Passwörter nach aktuellen Empfehlungen (z.B. durch BSI, NIST, ENISA)
☒ Veröffentlichung von Passwortregeln für Mitarbeiter (z.B. Verbot der Weitergabe, der Speicherung im Browser oder der Mehrfachverwendung)
☒ Passwort Manager im Einsatz
☒ Automatische Sperrung des Zugangs bei zu vielen Fehlversuchen (zeitweise oder komplett)

Organisatorische Maßnahmen
☒ Zentrale Passwortvergabe
☒ Standard-Authentifizierungsinformationen durch Hersteller bei Software sollten nach Installation geändert werden
☒ Verwaltung der Benutzerrechte durch den IT-Administrator
☒ Jedem Mitarbeiter ist ein eigenes Benutzerprofil zugeordnet in der Domäne
☒ Es erfolgt eine sichere Zustellung der Anmeldeinformationen für Benutzer (z.B. verschlüsselte Mail, getrennte Briefe für Benutzername und Passwort)
☒ Passwörter werden nach einem Sicherheitsvorfall, auch im Verdacht, gesperrt und müssen vom Nutzer neu vergeben werden.
☒ Dokumentiertes Berechtigungskonzept inkl. Rollenprofilen für die Beschäftigten um gezielt Zugang zu Informationen zu steuern und reglementieren und zu verwalten.
☒ Keine Administratorkennungen für Nutzer, die keine administrativen Tätigkeiten ausführen.
☒ Regelmäßige Überprüfung, ob die Zuweisung der Rollen den Vorgaben entspricht sowie, ob die Rollen noch den Anforderungen der Geschäftstätigkeit entspricht.
☒ Anzahl der IT-Administratoren auf ein Minimum reduziert

1.5. Trennbarkeit

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

Technische Maßnahmen
☒ Umsetzung der Mandantentrennung durch Trennung auf Datenebene

Organisatorische Maßnahmen
☒ Berechtigungskonzept
☒ Logische Mandantentrennung (softwareseitig)
☒ Trennung von Zugriffen mittels Datenbankrechten

1.6 Pseudonymisierung gem. Art. 32 Abs. 1 lit. a) Alt. 1 DSGVO

Pseudonymisierung beschreibt Maßnahmen zur Verarbeitung der Daten in solch eine Form, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen. Die Anwendung der Pseudonymisierung auf personenbezogene Daten kann die Risiken für die Daten der betroffenen Personen senken. Die Pseudonymisierung ist hinreichend, wenn die De-Pseudonymisierung durch interne Nutzer nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

☒ nicht relevant, da keine Pseudonymisierung stattfindet bzw. erforderlich ist

2. Integrität der Daten gem. Art. 32 Abs. 1 lit. b) Var. 2 DSGVO

2.1. Übertragungs- und Transportkontrolle

Die Übertragungskontrolle beschreibt Maßnahmen zur Überprüfung des Adressaten der Datenübertragung. Die Transportkontrolle beschreibt Maßnahmen zur Wahrung der Vertraulichkeit und Integrität der Daten bei Transport von Datenträgern.

Technische Maßnahmen
☒ Transportverschlüsselung wird ausschließlich Ende-zu-Ende implementiert.
☒ Bei Übertragung (z.B. E-Mail, Cloud-Plattformen) von personenbezogenen Daten mit hohem Risiko findet die Transportverschlüsselung und Inhaltsverschlüsselung nach Stand der Technik statt.
☒ Bei Massen-E-Mailversand wird die Offenlegung aller Empfänger technisch oder organisatorisch verhindert.
☒ Bei Messenger: Einsatz von Transport- und Inhaltsverschlüsselung der Nachrichten und Dateien nach Stand der Technik
☒ Einsatz von verschlüsselten und passwortgeschützten Datencontainern (z.B. ZIP, RAR Datei)
☒ Keine unverschlüsselten Protokolle (z. B. FTP, Telnet) bei Übertragung von personenbezogenen Daten verwenden
☒ Fernwartung für Clients zu IT-Administratorzwecken ausschließlich über verschlüsselte Verbindungen nach Authentifizierung durch den Administrator und Freigabe durch den Nutzer.

2.2. Eingabekontrolle

Die Eingabekontrolle beschreibt Maßnahmen zur (nachträglichen) Überprüfung, welche personenbezogene Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.

Technische Maßnahmen
☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch personalisierte (eindeutige) Kennungen bei IT-Anwendungen
☒ Protokollierungen von Zugriffen auf Server und Betriebssystem, um unbefugte Zugriffe festzustellen und zu analysieren
☒ Protokollierungen von Zugriffen auf IT-Applikationen mit kritischen Daten, um unbefugte Zugriffe festzustellen und zu analysieren
☒ Regelmäßige anlasslose Auswertung der Protokolle (Log-Dateien) zur Erkennung von ungewöhnlichen Einträgen – bevorzugt: Automatische Heuristiken
☒ Automatische Benachrichtigung an die IT-Administration bei Verdacht auf unbefugte Verarbeitungen

2.3. Zuverlässigkeit & Datenintegrität

Die Zuverlässigkeit beschreibt Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden. Die Datenintegrität stellt sicher, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktion des Systems beschädigt werden können.

Technische Maßnahmen
☒ Implementierung der Dateiintegritätsüberwachung für sensible Dateien (File Integrity Management)
☒ Regelmäßige Aktualisierung der Firewall sowie Netzwerkkomponenten
☒ Regelmäßige Aktualisierung des Spamfilters
☒ Regelmäßige Aktualisierung des Virenscanners
☒ Regelmäßige Überprüfung der ordnungsgemäßen Konfiguration der Firewall (z. B. mittels Portscans auf die eigenen IP-Adressen)
☒ Härtungsmaßnahmen werden umgesetzt (z.B. Einschränkung/Deaktivierung nicht notwendiger Berechtigungen, Ports, Protokolle, Server)
☒ Implementierung von Fehlfunktionsalarmen für IT-Systeme, -Applikationen und bei Installation neuer Software
☒ Schwachstellenmanagement
☒ Regelmäßiger Penetrationstest
☒ Nutzung eines Security Incident und Event Management

3. Verfügbarkeit und Belastbarkeit der Systeme (Resilienz) gem. Art. 32 Abs. 1 lit. b) Var. 3 DSGVO

3.1. Wiederherstellbarkeit gem. Art. 32 Abs. 1 lit. c) DSGVO

Die Wiederherstellbarkeit beschreibt Maßnahmen, die gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

☒ Dokumentiertes Datensicherungskonzept
☒ Dokumentierte Backup-Regelung für Server und Endgeräte
☒ Geeigneter Schutz von Backups vor Verschlüsselung durch Ransomware
☒ Dokumentiertes Wiederanlaufkonzept (Maßnahmen zur unverzüglichen Wiederherstellung der Verfügbarkeit bei Systemausfall)
☒ Kontrolle des Datensicherungsvorganges
☒ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung des Vorgangs (Empfehlung: vierteljährlich)
☒ Schnelle Wiederherstellung des Desaster Backups
☒ Geeignete physische Aufbewahrung von Backup-Medien an einem sicheren Ort außerhalb des Serverraums (z.B. Tresor, Feuerschutz, räumliche Trennung)
☒ Aufbewahrung der Datensicherung an einem sicheren Ort, außerhalb des Unternehmens (z.B. externe verschlüsselte Festplatte oder zweiter Server)

3.2. Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle beschreibt Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Technische Maßnahmen
☒ Serverräume und/oder Rechenzentren verfügen über Rauchmeldeanlagen
☒ Serverräume und/oder Rechenzentren verfügen über Feuerlöscher bzw. Feuerlöschanlagen
☒ Serverräume und/oder Rechenzentren verfügen über ausreichende Klimatisierung
☒ Serverräume und/oder Rechenzentren verfügen über Anlagen zur Überwachung von Temperatur und Feuchtigkeit
☒ Regelmäßige Kontrollen des Systemzustandes der relevanten Server (Monitoring)

☒ Einsatz von Anlagen zur Sicherstellung der Stromversorgung von Serversystemen (USV), insbesondere bei kurzfristigen Stromausfällen oder Schwankungen
☒ Serverräume und/oder Rechenzentren verfügen über Schutzsteckdosenleisten
☒ RAID-System / Festplattenspiegelung
☒ Datenschutzkonforme Videoüberwachung des Serverraums
☒ Protokollierung der Zutritte für den Serverraum
☒ Es sind keine Brandschutzrisiken vorhanden
☒ Physischer Schutz des Serverraums vor Einbruch
☒ Keine Risiken durch Überflutung/Starkregen, insbesondere bei Serverräumen im Keller
☒ Physischer Schutz des Routers

Organisatorische Maßnahmen
☒ Vollständige und aktuelle Netzwerkdokumentation
☒ Eine aktuelle Geräteverwaltung bzw. Dokumentation ist vorhanden.
☒ Dokumentierter IT-Notfallplan
☒ Dokumentierter Notfallplan inkl. Alarmkette

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung gem. Art. 32 Abs. 1 lit. d) Var. 3 DSGVO

Organisationen müssen nicht nur angemessene Sicherheitsmaßnahmen implementieren, sondern auch sicherstellen, dass diese Maßnahmen in regelmäßigen Abständen überprüft und bewertet werden. Dieser Prozess soll sicherstellen, dass die getroffenen Maßnahmen weiterhin wirksam sind und den aktuellen Anforderungen entsprechen, um Datenschutzrisiken zu minimieren.

Organisatorische Maßnahmen
☒ Zentrale Dokumentation aller Verfahrensanweisungen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter bei Bedarf
☒ Dokumentierter Prozess zur Erkennung, Meldung, Vorgehensweise und Nachbearbeitung von Sicherheits- und Datenschutzvorfällen.
☒ Dokumentation von Sicherheits- und Datenschutzvorfällen (z.B. Ticketsystem)
☒ Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

☒ Verzeichnis von Verarbeitungstätigkeiten im Sinne des Art. 30 Abs. 1 und 2 DSGVO

5. Sicherheit der Entwicklungsumgebung

5.1. Entwicklung von Software

Datenschutz und Sicherheit müssen frühzeitig bei der Entwicklung von eigenen Softwaresystemen bzw. bei der Auswahl von Softwareprodukten im eigenen Betrieb berücksichtigt werden.

☒ nicht relevant, da keine Entwicklung von Software stattfindet

5.2. Entwicklung von Webanwendungen (z.B. Onlineshop, Apps etc.)

Webseiten und Webanwendungen stellen meist leicht zugängliche Plattformen für Angriffe dar, die mit bekannten Best-Practice-Ansätzen meist gut abgesichert werden können.

☒ nicht relevant, da keine Entwicklung von Webanwendungen stattfindet

6. Sicherstellung von weisungsgebundener Verarbeitung gem. Art. 32 Abs. 4 DSGVO

Diese Maßnahmen schützen die Datensicherheit vor internen Beeinträchtigungen und reduzieren das Risiko der Umgehung der technischen Sicherheitsmaßnahmen durch die mit der Datenverarbeitung betrauten unterstellten, natürlichen Personen.

Organisatorische Maßnahmen
☒ IT-Richtlinie für Nutzer
☒ Regelung zur mobilen/privaten Nutzung von Endgeräten (z.B. Smartphones, Notebooks) durch Mitarbeiter sind getroffen.
☒ Clean Desk Policy
☒ Home-Office Richtlinie
☒ Vertraulichkeitsverpflichtung für Auftragnehmer
☒ Vertraulichkeitsvereinbarungen für Beschäftigte
☒ Onboarding Prozess für Mitarbeiter
☒ Offboarding Prozess für Mitarbeiter
☒ Regelmäßige Sensibilisierung für Datenschutz der Mitarbeiter (mind. jährlich)
☒ Regelmäßige Sensibilisierung für Informationssicherheit der Mitarbeiter
☒ Regelmäßige Sensibilisierung für Phishingangriffe

7. Sonstige Maßnahmen

Zusätzlich zu den Anforderungen der DSGVO werden folgende Maßnahmen und Anforderungen erfüllt.

☒ Benennung eines Informationssicherheitsbeauftragten und Kommunikation gegenüber dem Personal.
☒ Einsatz eines geeigneten Informationssicherheitsmanagementsystem (ISMS) z.B. nach ISO/IEC 27001, BSI Standards, ISIS12 oder TISAX
☒ Bei Microsoft Windows Betriebssystemen: Der kontrollierte Ordnerzugriff ist in den Windows Security Einstellungen aktiv geschaltet.
☒ Browser-Plugins werden nur dann installiert, wenn dies unbedingt erforderlich ist.
☒ Microsoft-Office-Pakete sind so konfiguriert, dass diese nur signierte Makros ausführen, sofern die Makro Ausführung überhaupt in den Sicherheitsrichtlinien vorgesehen ist.
☒ E-Mails mit gefährlichen Dateianhängen wie ausführbare Dateien, mit Passwort verschlüsselte ZIP-Archive oder Office-Dokumente mit Makros werden vom Mailserver in einen Quarantäne-Ordner zur Analyse verschoben.
☒ Ausführliche Softwareinventarisierung