Auftragsverarbeitungsvertrag

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DSGVO

zwischen

_____

_____

_____

als Verantwortliche/r - nachfolgend "**Auftraggeber**" genannt –

und

SUSTAYN GmbH

Lindenallee 41

45127 Essen

als Auftragsverarbeiter/in - nachfolgend "**Auftragnehmer**" genannt –

- Auftraggeber und Auftragnehmer nachfolgend jeder auch "Partei" und gemeinsam "Parteien" -

Präambel

Der Auftragnehmer erbringt für den Auftraggeber Leistungen gemäß dem zwischen ihnen geschlossenen Hauptvertrag (im Folgenden: "**Hauptvertrag"**). Teil der Durchführung des Hauptvertrags ist die Verarbeitung von personenbezogenen Daten im Sinne der Datenschutzgrundverordnung ("**DSGVO**"). Zur Erfüllung der Anforderungen der DSGVO an derartige Konstellationen schließen die Parteien den nachfolgenden Auftragsverarbeitungsvertrag (auch „**Vertrag**“), der mit Unterzeichnung bzw. Wirksamwerden des Hauptvertrages zustande kommt.

§ 1 Gegenstand/Umfang der Beauftragung

(1) Im Rahmen der Zusammenarbeit der Parteien nach Maßgabe des Hauptvertrages hat der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers (nachfolgend "**Auftraggeberdaten**"). Diese Auftraggeberdaten verarbeitet der Auftragnehmer im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 4 Nr. 8 und Art. 28 DSGVO.

(2) Die Verarbeitung der Auftraggeberdaten durch den Auftragnehmer erfolgt in der in **Anlage 1** beschriebenen Art sowie in dem dort spezifizierten Umfang und Zweck. Der Kreis der von der Datenverarbeitung betroffenen Personen wird dargestellt. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.
Ob die Leistungen des Auftragnehmers für die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO geeignet sind, bedarf einer Risikobewertung durch den Auftraggeber.

(3) Dem Auftragnehmer ist eine von den in **Anlage 1** genannten Verarbeitungen abweichende Verarbeitung von Auftraggeberdaten untersagt.

(4) Die Verarbeitung der Auftraggeberdaten findet grds. im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Sollte es eine Verlagerung der Auftragsverarbeitung in ein Drittland geben, bedarf dies der vorherigen Zustimmung des Auftraggebers und erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind. Der Auftraggeber stimmt bereits Abschluss dieses Auftragsverarbeitungsvertrages der Verarbeitung personenbezogener Daten durch die in Anlage 1 genannten Subunternehmen zu.

(5) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen. Gleiches gilt für alle Tätigkeiten, bei denen der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit Auftraggeberdaten in Berührung kommen.

§ 2 Weisungsbefugnisse des Auftraggebers

(1) Der Auftragnehmer verarbeitet die Auftraggeberdaten im Rahmen der Beauftragung und im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber hat das alleinige Recht, Weisungen über Art, Umfang, und Methode der Verarbeitungstätigkeiten zu erteilen (nachfolgend auch "**Weisungsrecht**"). Soweit eine Mitwirkung des Auftragnehmers erforderlich ist, ist der Auftraggebers zur Erstattung der anfallenden angemessenen Kosten verpflichtet. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Weisungen werden vom Auftraggeber grundsätzlich schriftlich oder in elektronischer Form (E-Mail ausreichend) erteilt; mündlich erteilte Weisungen sind vom Auftragnehmer in elektronischer Form zu bestätigen.

(3) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden

Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

§ 3 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Ferner wird der Auftragnehmer alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im Folgenden "**Mitarbeiter**" genannt), zur Vertraulichkeit verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO). Auf Verlangen des Auftraggebers wird der Auftragnehmer dem Auftraggeber die Verpflichtung der Mitarbeiter schriftlich oder in elektronischer Form nachweisen.

(3) Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er verpflichtet sich, alle geeigneten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Auftraggeberdaten gem. Art. 32 DSGVO, insbesondere die in **Anlage 2** zu diesem Vertrag aufgeführten Maßnahmen, zu ergreifen und diese für die Dauer der Verarbeitung der Auftraggeberdaten aufrecht zu erhalten.

(4) Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(5) Auf Verlangen des Auftraggebers wird der Auftragnehmer dem Auftraggeber die Einhaltung der technischen und organisatorischen Maßnahmen nachweisen.

§ 4 Informations- und Unterstützungspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der Auftraggeberdaten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte, wird der Auftragnehmer den Auftraggeber unverzüglich, spätestens aber innerhalb von 48 Stunden in Schriftform oder elektronischer Form informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Diese Meldungen sollten jeweils zumindest die in Art. 33 Absatz 3 DSGVO genannten Angaben enthalten.

(2) Der Auftragnehmer wird den Auftraggeber im o.g. Falle bei der Erfüllung seiner diesbezüglichen Aufklärungs-, Abhilfe- und Informationsmaßnahmen im Rahmen des zumutbaren unterstützen.

(3) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen Anforderung innerhalb angemessener Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle erforderlich sind.

§ 5 Sonstige Verpflichtungen des Auftragnehmers

(1) Der Auftragnehmer ist, sofern die Voraussetzungen des Art. 30 DSGVO auf ihn zutreffen, verpflichtet, ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung gem. Art. 30 Absatz 2 DSGVO zu führen. Das Verzeichnis ist dem Auftraggeber auf Verlangen zur Verfügung zu stellen.

(2) Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Erstellung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und einer etwaigen vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO zu unterstützen.

(3) Der Auftragnehmer bestätigt, dass er – soweit eine gesetzliche Verpflichtung hierzu besteht – einen Datenschutzbeauftragten bestellt hat.

(4) Sollten die Auftraggeberdaten 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 ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DSGVO liegt.

§ 6 Subunternehmerverhältnisse

(1) Der Auftragnehmer darf die Verarbeitung personenbezogener Daten ganz oder teilweise durch weitere Auftragsverarbeiter (nachfolgend „**Unterauftragnehmer**“) erbringen lassen. Der Auftragnehmer informiert den Auftraggeber in Textform rechtzeitig vorab über die Beauftragung von Unterauftragnehmern oder Änderungen in der Unterbeauftragung. Der Auftraggeber kann bei Vorliegen sachlicher Gründe der Unterbeauftragung innerhalb von vier Wochen nach Kenntnisnahme in Textform widersprechen.

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z.B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Bewachungsdienste, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Die Pflicht des

Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

(3) Der Auftragnehmer wird mit dem Unterauftragnehmer die in diesem AVV getroffenen Regelungen inhaltsgleich vereinbaren. Insbesondere müssen die mit dem Unterauftragnehmer zu vereinbarenden TOM ein gleichwertiges Schutzniveau aufweisen.

(4) Der Auftragnehmer hat mit den in **Anlage 1** genannten Unternehmen Subunternehmerverhältnisse begründet, denen der Auftraggeber mit Abschluss dieses Auftragsverarbeitungsvertrages zustimmt.

(5) Mit den Unterauftragnehmern hat der Auftragnehmer den Anforderungen aus § 6 Abs. 3 entsprechende Auftragsverarbeitungsverträge geschlossen. Mit Wirksamwerden dieses AVV genehmigt der Auftraggeber die vorgenannten Unterauftragnehmer.
Bestandteil der Auftragsverarbeitungsverträge mit den Unterauftragnehmern ist insbesondere auch, dass die Unterauftragnehmer sicherstellen, ihrerseits angemessene und geeignete technische und organisatorische Maßnahmen nach Art. 32 DSGVO wegen der von ihnen im Auftrag durchgeführten Verarbeitungen personenbezogener Daten getroffen zu haben.

§ 7 Kontrollrechte

(1) Der Auftraggeber ist berechtigt, sich regelmäßig von der Einhaltung der Regelungen dieses Vertrages zu überzeugen. Hierfür kann er z.B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers zu den üblichen Geschäftszeiten selbst persönlich bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

(2) Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und angemessene Rücksicht auf die Betriebsabläufe des Auftragnehmers nehmen. Über den Zeitpunkt sowie die Art der Prüfung verständigen sich die Parteien rechtzeitig.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

§ 8 Rechte Betroffener

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten

nach Art. 12 bis 22 sowie Art. 32 bis 36 DSGVO. Er wird dem Auftraggeber unverzüglich, spätestens aber innerhalb von 14 Werktagen, die gewünschte Auskunft über Auftraggeberdaten geben, sofern der Auftraggeber nicht selbst über die entsprechenden Informationen verfügt.

(2) Macht der Betroffene seine Rechte gemäß Art. 16 bis 18 DSGVO geltend, ist der Auftragnehmer dazu verpflichtet, die Auftraggeberdaten auf Weisung des Auftraggebers unverzüglich, spätestens binnen einer Frist von 7 Werktagen zu berichtigen, löschen oder einzuschränken. Der Auftragnehmer wird dem Auftraggeber die Löschung, Berichtigung bzw. Einschränkung der Daten auf Verlangen schriftlich nachweisen.

(3) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, wird der Auftragnehmer dieses Ersuchen an den Auftraggeber weiterleiten und wartet dessen Weisungen ab. Ohne entsprechende Einzelweisung wird der Auftragnehmer nicht mit der betroffenen Person in Kontakt treten.

§ 9 Laufzeit und Kündigung

Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Ist der Hauptvertrag ordentlich kündbar, gelten die Regelungen zur ordentlichen Kündigung für diesen Vertrag entsprechend.

§ 10 Löschung und Rückgabe nach Vertragsende

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Verlangen alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder auf Wunsch des Auftraggebers, sofern nicht eine gesetzliche Aufbewahrungsfrist besteht, vollständig und unwiderruflich löschen. Dies gilt auch für Vervielfältigungen der Auftraggeberdaten beim Auftragnehmer, wie etwa Datensicherungen, nicht aber für Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung der Auftraggeberdaten dienen. Solche Dokumentationen sind vom Auftragsnehmer für eine Dauer von 6 Monaten aufzubewahren und auf Verlangen an den Auftragsgeber herauszugeben.

(2) Der Auftragnehmer wird dem Auftraggeber die Löschung elektronisch bestätigen. Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

(3) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln.

§ 11 Haftung

(1) Die Haftung der Parteien richtet sich nach Art. 82 DSGVO. Eine Haftung des Auftragnehmers gegenüber dem Auftraggeber wegen Verletzung von Pflichten aus diesem Vertrag oder dem Hauptvertrag bleibt hiervon unberührt.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist. Dies gilt im Falle einer gegen eine Partei verhängte Geldbuße entsprechend, wobei die Freistellung in dem Umfang erfolgt, in dem die jeweils andere Partei Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

§ 12 Vertraulichkeit & Datengeheimnis

(1) Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen.

(2) Es besteht eine Verschwiegenheitspflicht für die Mitarbeiter des Auftragnehmers und durch ihn beauftragte Dritte. Der Auftragnehmer hat die bei der Verarbeitung von Auftraggeberdaten beschäftigten Personen gemäß Art. 28 Abs. 3 lit. b DSGVO schriftlich auf die Vertraulichkeit zu verpflichten. Dies ist nicht erforderlich, wenn die beschäftigten Personen bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Der Auftragnehmer wird die in dieser Ziffer niedergelegte Verpflichtung schriftlich dokumentieren und sie auf Verlangen des Auftraggebers diesem vorlegen.

(3) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und er diese auf die Einhaltung der geltenden Datenschutzvorschriften zu verpflichten. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

(4) Diese in dieser Ziffer geregelten Verschwiegenheitspflichten besteht auch nach der Beendigung des Vertragsverhältnisses fort.

(5) Darüber hinaus ist der Auftragnehmer neben den jeweils geltenden gesetzlichen Bestimmungen (insbesondere § 3 TTDSG, § 203 StGB, §§ 4, 23 GeschGehG sowie ggf. besondere berufsständische Verschwiegenheitspflichten) auch verpflichtet, alle Informationen und Daten, die ihm im Rahmen der vertraglich vereinbarten Leistungen zur Kenntnis gelangen, geheim zu halten und nicht an Dritte weiterzugeben (vertrauliche Informationen). Vertrauliche Informationen sind insbesondere Geschäfts- und Betriebsgeheimnisse, Vertragsschlüsse, technische oder kaufmännische Informationen jedweder Art bzw. anderweitige Angaben, die als vertraulich bezeichnet oder ihrer Natur nach als vertraulich anzusehen sind. Dies gilt insbesondere auch für:

Namen, Anschriften sowie die persönlichen, rechtlichen und wirtschaftlichen Verhältnisse aller Kunden vom Auftraggeber und die persönlichen, rechtlichen und wirtschaftlichen Verhältnisse vom Auftraggeber und aller anderen für Auftraggeber tätigen Personen.

Eine Information ist nicht als vertraulich anzusehen, wenn sie zu der Zeit, zu der der Auftragnehmer von der Information Kenntnis erlangt hat, bereits öffentlich bekannt gewesen ist. Ebenso als nicht vertraulich sind solche Informationen anzusehen, die zeitlich später mit Zustimmung des Auftraggebers öffentlich bekannt geworden sind bzw. bekannt gemacht wurden.

Der Auftragnehmer verpflichtet sich, sämtliche Mitarbeiter, die im Rahmen der Tätigkeit für Auftraggeber Kenntnis von vorgenannten vertraulichen Informationen von Auftraggeber erlangen, ebenso wie sich selbst zu verpflichten.

(6) Beauftragt der Auftragnehmer Dritte, hat er dafür Sorge zu tragen, dass die Forderungen der Absätze 1 bis 5 entsprechend umgesetzt werden.

§ 13 Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer iSd § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der elektronischen Form.

(3) Die Regelungen dieses Vertrags gehen im Zweifel den Regelungen des Hauptvertrags vor. Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen einer Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist der Sitz des Auftragnehmers.

Anlagen

Anlage 1 Festlegungen zum Vertrag

Anlage 2 Technische und organisatorische Maßnahmen des Auftragnehmers (Art. 32 DSGVO)

Anlage 1 – Festlegungen zum Vertrag

Gegenstand und Dauer des Auftrages Übersicht der Anforderungen und Festlegungen	
(1) Hauptvertrag	Lizenz-& Kooperations-Vertrag
(2) Gegenstand des Auftrages	SUSTAYN ist ein Unternehmen, das mit seinen Softwarelösungen (nachfolgend auch „Software“ genannt) und Beratungsdienstleistungen ein nachhaltiges und umweltbewusstes Handeln von den Mitarbeiter:innen seiner Kund:innen fördert.
(3) Zweck der Datenerhebung, Datenverarbeitung oder Datennutzung	Zur Erfüllung der Pflichten des Auftragnehmers aus dem Hauptvertrag werden personenbezogene Daten aus dem Herrschaftsbereich des Auftraggebers durch den Auftragnehmer vollumfänglich i.S.d. Art. 4 Nr. 2 DSGVO verarbeitet, insbesondere soweit jeweils erforderlich erhoben, gespeichert, verändert, ausgelesen, abgefragt, verwendet, offengelegt, abgeglichen, verknüpft und gelöscht. Der Zweck der Verarbeitung hängt damit von dem jeweils im Hauptvertrag beschriebenen Auftrag ab.
(4) Art der Daten	Die von der Verarbeitung betroffenen Kategorien personenbezogener Daten hängen von der Nutzung der Leistungen des Auftragnehmers durch den Auftraggeber ab. Als Gegenstand der Verarbeitung in Betracht kommende Kategorien von Daten sind möglich · Stammdaten (z.B. Namen), · Kontaktdaten (z.B. E-Mail-Adressen), · Inhaltsdaten (z.B. Fotografien, Videos), · Nutzungsdaten (z.B. Verlauf Web-Dienste, Zugriffszeiten), · Verbindungsdaten (z.B. Geräte-ID, IP-Adressen, URL-Referrer)
(5) Kreis der Betroffenen	Die von der Verarbeitung betroffenen Kategorien betroffener Personen hängen von der Nutzung der Leistungen des

Kommentiert [DS1]: Muss das jetzt anders heißen?

Kommentiert [DS2]: Angepasst - ok?

	Auftragnehmers durch den Auftraggeber ab. Als Kategorien betroffener Personen kommen dabei in Betracht: · Beschäftigte · Auszubildende und Praktikanten · ehemalige Arbeitnehmer · freie Mitarbeiter

Weisungsgeber und Weisungsempfänger

Weisungsbefugte des Auftraggebers

Nr.	Firma	Name / Funktion	Kontaktdaten
1			
2			
3			
4			

Weisungsempfänger des Auftragnehmers

Nr.	Firma	Name / Funktion	Kontaktdaten
1	SUSTAYN GmbH	Janik Seitzer (Geschäftsführung)	e: janik@sustayn.de

Unterauftragnehmer

Beauftragte Subunternehmer für die Gewährleistung der Funktionalität der Sustayn Software

Derzeit sind nachfolgende Rechenzentren vom Sustayn beauftragt:

1. Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxembourg, https://www.aws.amazon.com
    - Hosting-Anbieter zum Betrieb der Sustayn Anwendung
    - Die Verarbeitung der Daten beim Subunternehmen findet ausschließlich innerhalb der europäischen Union statt (Ausschließlich in der „Region Frankfurt“).

- Betroffen sind sämtliche Datenkategorien, die bei der Verwendung der Sustayn Anwendung gemäß unserer geschlossenen Verträge entstehen. Siehe Anhang 1
- AWS konnte seine Eignung durch ISO/IEC-Zertifizierungen (9001, 27001, 27017, 27018) nachweisen. Einen ausführlichen allgemeinen Überblick zur Sicherheit und EU-DSGVO erhalten Sie auf der Webseite von AWS unter https://aws.amazon.com/de/security.
- Mit AWS wurde eine Vereinbarung zur Auftragsverarbeitung AVV nach EU-DSGVO) getroffen.

Anlage 2 - Technische und organisatorische Maßnahmen

Verantwortliche für die Datenverarbeitung sind gem. Art. 32 DSGVO verpflichtet, technische und organisatorische Maßnahmen zu treffen, durch die die Sicherheit der Verarbeitung personenbezogener Daten gewährleistet wird. Maßnahmen müssen dabei so gewählt sein, dass durch sie in der Summe ein angemessenes Schutzniveau sichergestellt wird. Diese Übersicht erläutert vor diesem Hintergrund, welche konkreten Maßnahmen durch den Auftragnehmer im Hinblick auf die Verarbeitung personenbezogener Daten im konkreten Fall getroffen sind.

Grundsätzliche Maßnahmen, die der Wahrung der Betroffenenrechte, unverzüglichen Reaktion in Notfällen, den Vorgaben der Technikgestaltung und dem Datenschutz auf Mitarbeiterebene dienen:

- Es besteht ein betriebsinternes Datenschutz-Management, dessen Einhaltung ständig überwacht wird sowie anlassbezogenen und mindestens halbjährlichen evaluiert wird.
- Es besteht ein Konzept, welches die Wahrung der Rechte der Betroffenen (Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Datentransfer, Widerrufe & Widersprüche) innerhalb der gesetzlichen Fristen gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen.
- Es besteht ein Konzept, das eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Verletzungen des Schutzes personenbezogener Daten (Prüfung, Dokumentation, Meldung) gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen.

- Der Schutz von personenbezogenen Daten 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 der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen bereits bei der Entwicklung, bzw. Auswahl von Hardware, Software sowie Verfahren, entsprechend dem Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigt (Art. 25 DSGVO).
- Die eingesetzte Software wird stets auf dem aktuell verfügbaren Stand gehalten, ebenso wie Virenscanner und Firewalls.
- Mitarbeiter werden im Hinblick auf den Datenschutz auf Verschwiegenheit verpflichtet, belehrt und instruiert, als auch auf mögliche Haftungsfolgen hingewiesen. Sofern Mitarbeiter außerhalb betriebsinterner Räumlichkeiten tätig werden oder Privatgeräte für betriebliche Tätigkeiten einsetzen, existieren spezielle Regelungen zum Schutz der Daten in diesen Konstellationen und der Sicherung der Rechte von Auftraggebern einer Auftragsverarbeitung.
- Die an Mitarbeiter ausgegebene Schlüssel, Zugangskarten oder Codes sowie im Hinblick auf die Verarbeitung personenbezogener Daten erteilte Berechtigungen, werden nach deren Ausscheiden aus dem Unternehmen, bzw. Wechsel der Zuständigkeiten eingezogen, bzw. Entzogen.
- Das Reinigungspersonal, Wachpersonal und übrige Dienstleister, die zur Erfüllung nebengeschäftlicher Aufgaben herangezogen werden, werden sorgfältig ausgesucht und es wird sichergestellt, dass sie den Schutz personenbezogener Daten beachten.

Zutrittskontrolle

- Sicherheitsschlösser
- Chipkarten-/Transponder-Schließsystem
- Fenstersicherung

Zugangskontrolle / Zugriffskontrolle

- Firewall (Software)
- Stets aktueller Virenschutz
- Stets aktuelle Softwareversionen
- Berechtigungs-/ Authentifizierungskonzepte mit auf Nötigste beschränkten
- Zugriffsregulierungen

- Mindestpasswortlängen und Passwortmanager
- Ordnungsgemäße Vernichtung von Datenträgern
- Authentifikation mit Benutzer und Passwort und bei erhöhtem Schutzbedarf durch eine zusätzliche Multifaktor-Authentisierung
- Verschlüsselung von Festplatten (FileVault, Bitlocker)

Weitergabekontrolle

- Festlegung und Dokumentation der Empfänger
- Verschlüsselung data-at-rest (AES 256-Bit) der Dateien im Rechenzentrum

Eingabekontrolle

- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

Auftragskontrolle

- Auswahl von Auftragnehmern unter Sorgfaltsgesichtspunkten
- Schriftliche Festlegung der Weisungen
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Abschluss von Auftragsverarbeitungsverträgen

Verfügbarkeitskontrolle / Integrität

- Ständig kontrolliertes Backup- und Recoverykonzept
- Durchführung von Belastbarkeitstests
- Unterbrechungsfreie Stromversorgung und Überspannungsschutz
- Sicherstellung einer funktionsfähigen Klimatisierung

Gewährleistung des Zweckbindungs-/Trennungsgebotes

- Trennung von Produktiv- und Testsystem
- Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten System