Auftragsverarbeitung nach Art. 28 Datenschutz-Grundverordnung (DSGVO)[1]

Vereinbarung

zwischen

– Verantwortlicher, nachfolgend „Auftraggeber“ genannt –

und

The Team Enablers GmbH (Produkt Surwayne)

Baumwall 7

20459 Hamburg

– Auftragsverarbeiter, nachfolgend „Auftragnehmerin“ oder „TTE“ genannt –

Auftraggeber und Auftragnehmer jeweils einzeln als „Partei“ und gemeinsam als „Parteien“ bezeichnet.

---

1. Vertragsgegenstand

Im Rahmen des zwischen den Parteien bestehenden Liefer- und Leistungsverhältnisses (nachfolgend „Hauptvertrag“ genannt) ist es erforderlich, dass die Auftragnehmerin als Auftragsverarbeiter i. S. d. Art. 4 Nr. 8 DSGVO mit personenbezogenen Daten umgeht, für die der Auftraggeber als Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO fungiert (nachfolgend „Auftraggeber-Daten“ genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang der Auftragnehmerin mit Auftraggeber-Daten zur Durchführung des Hauptvertrags.

2. Art und Zweck der Auftragsverarbeitung

2.1 Die Auftragnehmerin verarbeitet die Auftraggeber-Daten im Auftrag und nur nach Weisung des Auftraggebers. Der Auftraggeber bleibt gemäß Art. 5 Abs. 2 DSGVO im datenschutzrechtlichen Sinn Verantwortlicher („Herr der Daten“).

2.2 Die Verarbeitung der Auftraggeber-Daten im Rahmen der Auftragsverarbeitung erfolgt entsprechend den in **Anlage 1** zu diesem Vertrag enthaltenen Festlegungen zu Art und Zweck der Verarbeitung. Sie bezieht sich auf die in **Anlage 1** festgelegte Art der Auftraggeber-Daten und auf die dort bestimmten Kategorien betroffener Personen.

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 4.5.2016, S. 1–88. AN

2.3 Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union statt. Jede Verlagerung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

3. Weisungsrechte des Auftraggebers

3.1 Die Auftragnehmerin verwendet die Auftraggeber-Daten ausschließlich in Übereinstimmung mit den Weisungen des Auftraggebers, wie sie abschließend in den Bestimmungen dieses Vertrags Ausdruck finden. Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung der Auftragnehmerin und erfolgen nach Maßgabe des im Hauptvertrag festgelegten Änderungsverfahrens.

3.2 Ist dir Auftragnehmerin der Ansicht, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der EU oder der Mitgliedstaaten verstößt, wird sie den Auftraggeber möglichst zeitnah darauf hinweisen. Außerdem ist die Auftragnehmerin berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen.

3.3 Soweit die Auftragnehmerin durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist, die personenbezogenen Daten auch ohne Weisung des Auftraggebers zu verarbeiten, teilt die Auftragnehmerin dem Auftraggeber die entsprechenden rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.4 Weisungen des Auftraggebers sind mindestens in Textform (z.B. E-Mail) zu erteilen. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich mindestens in Textform (z.B. E-Mail).

3.5 Sofern gegen die Auftragnehmerin wegen eines Verstoßes gegen die DSGVO Ansprüche auf Zahlung von Schadenersatz gemäß Art. 82 DSGVO geltend gemacht werden, ohne dass die Auftragnehmerin gegen eine vom Auftraggeber erlassene Weisung verstoßen hat, stellt der Auftraggeber die Auftragnehmerin auf erstes Anfordern von allen Ansprüchen frei. Der Auftraggeber übernimmt hierbei auch die Kosten der notwendigen Rechtsverteidigung der Auftragnehmerin einschließlich sämtlicher Gerichts- und Anwaltskosten. Die Freistellungspflicht gilt nicht, soweit eine Weisung rechtswidrig und dies für die Auftragnehmerin offensichtlich war oder der Schadenersatzanspruch auf die Verletzung einer speziell den Auftragsverarbeitern auferlegten Pflicht aus der DSGVO gestützt wird.

4. Pflichten des Auftraggebers

4.1 Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund der Verarbeitung von Auftraggeber-Daten Ansprüche geltend machen, wird der Auftraggeber die Auftragnehmerin von allen solchen Ansprüchen auf erstes Anfordern freistellen.

4.2 Der Auftraggeber ist Eigentümer der Auftraggeber-Daten und Inhaber aller etwaigen Rechte, die die Auftraggeber-Daten betreffen.

4.3 Der Auftraggeber hat der Auftragnehmerin unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse der Auftragnehmerin Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

4.4 Soweit sich die Auftragnehmerin gegen einen Anspruch auf Schadenersatz nach Art. 82 DSGVO, gegen ein drohendes oder bereits verhängtes Bußgeld nach Art. 83 DSGVO oder sonstige Sanktionen im Sinne des Art. 84 DSGVO mit rechtlichen Mitteln verteidigen will, erlaubt der Auftraggeber der

Auftragnehmerin Details der Auftragsverarbeitung inklusive erlassener Weisungen zum Zweck der Verteidigung offenzulegen.

4.5 Der Auftraggeber unterstützt die Auftragnehmerin bei Kontrollen durch eine Aufsichtsbehörde, bei Ordnungswidrigkeits- oder Strafverfahren, bei der Geltendmachung eines Haftungsanspruchs einer betroffenen Person oder eines Dritten oder bei der Geltendmachung eines anderen Anspruchs im Rahmen des Zumutbaren und Erforderlichen, soweit ein Zusammenhang mit dieser Auftragsverarbeitung besteht.

5. Pflichten der Auftragnehmerin

5.1 Die Auftragnehmerin darf ohne vorherige Zustimmung durch den Auftraggeber im Rahmen der Auftragsverarbeitung keine Kopien oder Duplikate der Auftraggeber-Daten anfertigen. Hiervon ausgenommen sind jedoch Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung und zur ordnungsgemäßen Erbringung der Leistungen gemäß dem Hauptvertrag (einschließlich der Datensicherung) erforderlich sind, sowie Kopien, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

5.2 Die Auftragnehmerin unterstützt den Auftraggeber bei Kontrollen durch die Aufsichtsbehörde, bei Ordnungswidrigkeits- oder Strafverfahren, bei der Geltendmachung eines Haftungsanspruchs einer betroffenen Person oder eines Dritten oder bei der Geltendmachung eines anderen Anspruchs im Rahmen des Zumutbaren und Erforderlichen, soweit ein Zusammenhang mit dieser Auftragsverarbeitung besteht.

5.4 Die Auftragnehmerin hat die bei der Verarbeitung von Auftraggeber-Daten beschäftigten Personen gemäß Art. 28 Abs. 3 Satz 2 lit. b) DSGVO schriftlich auf die Vertraulichkeit zu verpflichten und sie zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut zu machen. Dies ist nicht erforderlich, wenn die bei der Verarbeitung von Auftraggeber-Daten beschäftigten Personen bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

5.5 Sofern und solange die gesetzlichen Voraussetzungen für eine Benennungspflicht gegeben sind, ist die Auftragnehmerin verpflichtet, einen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis fachkundigen, für die Aufgaben nach Art. 39 DSGVO fähigen und zuverlässigen betrieblichen Datenschutzbeauftragten schriftlich zu benennen, der seine Tätigkeit gemäß Art. 38, 39 DSGVO und § 38 Abs. 2 BDSG ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zwecke der direkten Kontaktaufnahme mindestens in Textform (z.B. E-Mail) mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

5.6 Die Auftragnehmerin unterliegt der behördlichen Aufsicht nach § 40 BDSG sowie den Bußgeld- und Strafvorschriften in § 42, 43 BDSG sowie in Art. 83 Abs. 4-6 DSGVO nach Maßgabe von § 41 BDSG.

5.7 Die Auftragnehmerin stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Die Auftragnehmerin verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der nach **Anlage 2** zu treffenden technischen und organisatorischen Maßnahmen im Rahmen der Kontrollrechte nach Ziffer 8 dieses Vertrages nachzuweisen.

6. Technische und organisatorische Maßnahmen

6.1 Die Auftragnehmerin hat vor Beginn der Verarbeitung der Auftraggeber-Daten die in **Anlage 2** dieses Vertrags aufgelisteten technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 Satz 2 lit. c), Art. 32 DSGVO zu implementieren und während des Vertrags aufrechtzuerhalten. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit,

Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

6.2 Da die technischen und organisatorischen Maßnahmen dem technischen Fortschritt und der technologischen Weiterentwicklung unterliegen, ist es der Auftragnehmerin gestattet, alternative adäquate Maßnahmen umzusetzen, sofern dabei das Sicherheitsniveau der in **Anlage 2** festgelegten Maßnahmen nicht unterschritten wird. Die Auftragnehmerin wird solche Änderungen dokumentieren. Wesentliche Änderungen der Maßnahmen bedürfen der vorherigen schriftlichen Zustimmung des Auftraggebers und sind von der Auftragnehmerin zu dokumentieren und dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

7. Unterstützung des Auftragnehmers zur Einhaltung der Pflichten des Auftraggebers nach Art. 32 – 36 DSGVO

Die Auftragnehmerin unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherige Konsultationen. Hierzu gehören

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen,

b) die Unterstützung des Auftraggebers im Falle einer Verletzung des Schutzes personenbezogener Daten nach Art. 33 DSGVO,

c) die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht nach Art. 34 DSGVO gegenüber einem Betroffenen zu unterstützen,

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzungen i. S. d. Art. 35 DSGVO,

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde nach Art. 36 DSGVO.

8. Kontrollrechte des Auftraggebers

8.1 Der Auftraggeber ist berechtigt, im Rahmen der üblichen Geschäftszeiten auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen der Auftragnehmerin die Geschäftsräume der Auftragnehmerin, in denen Auftraggeber-Daten verarbeitet werden, zu betreten, um sich von der Einhaltung der aus dieser Vereinbarung ergebenden Pflichten, insbesondere der technischen und organisatorischen Maßnahmen gemäß **Anlage 2** zu diesem Vertrag, zu überzeugen. Die Auftragnehmerin weist dem Auftraggeber auf Anforderung die Umsetzung der technischen und organisatorischen Maßnahmen nach.

8.2 Die Auftragnehmerin gewährt dem Auftraggeber die zur Durchführung der Kontrollen nach Ziffer 8.1 erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte.

8.3 Der Auftraggeber hat der Auftragnehmerin rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände zu informieren. Der Auftraggeber darf in der Regel eine Kontrolle pro Kalenderjahr durchführen. Hiervon unbenommen

ist das Recht des Auftraggebers, weitere Kontrollen im Fall von besonderen Vorkommnissen durchzuführen.

8.4 Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Kontrolle, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund von dieser Ziffer 8 dieses Vertrags gegenüber der Auftragnehmerin 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 der Auftragnehmerin hat der Auftraggeber diesem die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Konkurrenten der Auftragnehmerin mit der Kontrolle beauftragen.

8.5 Nach Wahl der Auftragnehmerin kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen gemäß **Anlage 2** anstatt einer Vor-Ort-Kontrolle auch durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren nach Art. 42 DSGVO, die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit – z.B. nach BSI-Grundschutz – („Prüfungsberichts“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß **Anlage 2** zu diesem Vertrag zu überzeugen.

9. Unterauftragsverhältnisse

9.1 Die Auftragnehmerin darf Unterauftragsverhältnisse (Unterauftragnehmer) hinsichtlich der Verarbeitung oder Nutzung von Auftraggeber-Daten begründen. Zurzeit sind für die Auftragnehmerin die in **Anlage 3** mit Namen, Anschrift und Auftragsinhalt bezeichneten Unterauftragnehmer beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden. Die Auftragnehmerin informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines Unterauftragnehmers. Sofern der Auftraggeber keine Einwände gegen neue Unterauftragnehmer innerhalb von 2 Wochen ab Zugang der Mitteilung über den neuen Unterauftragnehmer erhebt, gilt dessen Einschaltung als durch den Auftraggeber genehmigt.

9.2 Nicht als Unterauftragsverhältnis im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die die Auftragnehmerin bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Die Auftragnehmerin ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

9.3 Die Verpflichtung des Unterauftragnehmers muss schriftlich erfolgen, was auch in einem elektronischen Format erfolgen kann (z.B. E-Mail). Die Auftragnehmerin hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmerin getroffenen Vereinbarungen einhalten kann. Die Auftragnehmerin stellt bei jeder Unterbeauftragung sicher, dass die in Art. 28 Abs. 2 und Abs. 4 DSGVO genannten Bedingungen eingehalten werden.

9.4 Die Auftragnehmerin hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten. Die Ausübung der Kontrollrechte des Auftraggebers nach Ziffer 8 muss gegenüber dem Unterauftragnehmer grundsätzlich möglich sein. Durch schriftliche Aufforderung ist der

Auftraggeber berechtigt, von der Auftragnehmerin Auskunft über den datenschutzwesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

9.5 Die Regelungen in dieser Ziffer 9 gelten auch, wenn ein Unterauftragnehmer in einem Drittstaat eingeschaltet wird. Die Auftragnehmerin stellt in einem solchen Fall die datenschutzrechtliche Zulässigkeit durch geeignete Rechtsinstrumente, beispielsweise EU-Standardvertragsklauseln, sicher.

9.6 Die Weitergabe von Auftraggeber-Daten an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

10. Rechte der Betroffenen

10.1 Die Rechte der durch die Datenverarbeitung betroffenen Personen nach Kapitel 3 DSGVO (Art. 12-23 DSGVO) unter Berücksichtigung von Teil 2, Kapitel 2 BDSG (§§ 32-37 BDSG), insbesondere auf Information, Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit oder Widerspruch der gespeicherten Auftraggeber-Daten, sind gegenüber dem Auftraggeber geltend zu machen.

10.2 Soweit ein Betroffener sich unmittelbar an die Auftragnehmerin zwecks der unter Ziffer 10.1 aufgeführten Rechte wenden sollte, wird die Auftragnehmerin dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

10.3 Für den Fall, dass eine betroffene Person ihre Rechte im Sinne von Ziffer 10.1 geltend macht, hat die Auftragnehmerin den Auftraggeber bei der Erfüllung dieser Ansprüche angesichts der Art der Verarbeitung in angemessenem und für den Auftraggeber erforderlichen Umfang mit geeigneten technischen und organisatorischen Maßnahmen zu unterstützen. Dies setzt voraus, dass der Auftragsgeber TTE schriftlich oder in Textform darum gebeten hat, und dass der Auftragsgeber TTE die Kosten ersetzt, die ihr dadurch entstanden sind, dass sie dem Ersuchen entspricht.

10.4 Die Auftragnehmerin wird es dem Auftraggeber ermöglichen, Auftraggeber-Daten zu berichtigen, zu löschen oder zu sperren oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Löschung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.

11. Rückgabe und Löschung überlassener Daten und Datenträger

11.1 Die Auftragnehmerin hat sämtliche Auftraggeber-Daten nach Beendigung der vertragsgegenständlichen Leistungserbringung (insbesondere bei Kündigung oder sonstiger Beendigung des Hauptvertrags) oder früher nach Aufforderung durch den Auftraggeber datenschutzgerecht zu löschen und von dem Auftraggeber erhaltene Datenträger, die zu diesem Zeitpunkt noch Auftraggeber-Daten enthalten, an den Auftraggeber zurückzugeben. Gleiches gilt für Test- und Ausschussmaterial. Dies gilt nicht, sofern nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Zusätzliche Kosten durch verschiedene Angaben zur Rückgabe oder Löschung trägt der Auftraggeber.

11.2 Über eine Löschung bzw. Vernichtung von Auftraggeber-Daten hat die Auftragnehmerin ein Protokoll zu erstellen, das dem Auftraggeber auf Anforderung vorzulegen ist.

11.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung oder gesetzlichen Aufbewahrungsfristen dienen, sind durch die Auftragnehmerin entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

12. Vertragsdauer und Kündigung

Die Laufzeit und Kündigung dieses Vertrags richtet 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.

13. Verhältnis zum Hauptvertrag

Soweit in diesem Vertrag keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Hauptvertrags. Im Fall von Widersprüchen zwischen diesem Vertrag und Regelungen aus sonstigen Vereinbarungen, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus diesem Vertrag vor.

14. Geltungszeitraum

Dieser Vertrag gilt ab Unterzeichnung. Da die Bestimmungen des Art. 28 DSGVO erst ab dem 25. Mai 2018 gelten, ist der Vertrag bis zum Ablauf des 24. Mai 2018 im Lichte des § 11 Bundesdatenschutzgesetz (BDSG) auszulegen.

15. Schriftformklausel

Änderungen und Ergänzungen dieser Unterlage und aller ihrer Bestandteile - einschließlich etwaiger Behauptungen - benötigen eine schriftliche Vereinbarung und den ausdrücklichen Vermerk, dass sie sich auf eine Änderung oder Ergänzung dieser Bedingungen beziehen. Dies gilt auch für den Verzicht auf diese Formvorschrift.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift Auftraggeber	Unterschrift Auftragnehmerin

Anlagen:

Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kreis der Betroffenen

Anlage 2: Technische und organisatorische Maßnahmen

Anlage 3: Unterauftragnehmer

Anlage 1: Art und Zweck der Datenverarbeitung, Art der Daten und Kategorien betroffener Personen

Art und Zweck der Datenverarbeitung:

Die Auftragnehmerin betreibt das Online-Anwendungsprogramm Surwayne. Dieses dient dazu, anonyme firmeninterne Umfragen zu erleichtern und Methoden zur Verbesserung der bewerteten Projekte und der allgemeinen Teamarbeit anzuregen. Mit Surwayne ermöglicht es die Auftragnehmerin dem Auftraggeber, die vorgenommenen Verbesserungsmethoden zu analysieren und zu bewerten sowie ihre unmittelbaren Auswirkungen z.B. auf den Teamgeist und die Leistungsfähigkeit, um Projekte und Teamwork individuell und wirkungsvoll zu optimieren. Zur Nutzung von Surwayne werden durch den Auftraggeber personenbezogene Daten (z.B. die betreffenden, für die Umfragen genutzten E-Mail-Adressen) an die Auftragnehmerin weitergegeben. Die Auftragnehmerin leitet die personenbezogenen Daten des Auftraggebers an ein Datenverarbeitungszentrum weiter. Das Datenverarbeitungszentrum verarbeitet und speichert Kundendaten der Auftragnehmerin für die Auftragnehmerin.

Art der personenbezogenen Daten:

Namen und E-Mail-Adressen der Mitarbeiter (des Auftraggebers)

Kategorien betroffener Personen:

Die Mitarbeiter des Auftraggebers, Freiberufler oder Dritte, deren Daten gemeinsam mit der Auftragnehmerin zum Zwecke der Erbringung der Surwayne Leistung genutzt werden.

Anlage 2: Technische und organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO) und Verschlüsselung (Art. 32 Abs. 1 lit. a) DSGVO)

Zutrittskontrolle

Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

- Alle Orte der Auftragnehmerin (und/oder des Unterauftragnehmers), an denen sich ein Informationssystem befindet, in welchem personenbezogene Daten genutzt werden oder untergebracht sind, haben angemessene Sicherheitssysteme. TTE beschränkt vernünftig den Zutritt zu diesen personenbezogenen Daten.
- Eine Zutrittskontrolle ist bei allen Datenzentren des Verarbeiters eingerichtet worden. Unbefugter Zutritt zu den Datenzentren wird durch 24x7 Überwachung und Zutritts-beschränkung verhindert.
- Überwachungskameras sind an der Eingangstür zu den Datenzentren installiert und Sicherheitsüberwachung durch die Hausverwaltung ist eingerichtet.
- Büros und Arbeitsbereiche, in denen personenbezogene Informationen verarbeitet werden, sind durch "clear desk" und "clear screen" -Anforderungen, Büroschließungsverfahren und die Benutzung sicherer Schränke und Behälter gesichert.
- Liefer- und Ladebereiche werden kontrolliert und sind von Informationsverarbeitungsanlagen getrennt, um unbefugten Zutritt zu vermeiden.
- Sicherheitsbereiche werden durch angemessene Eingangskontrollen geschützt, um zu gewährleisten, dass nur befugte Personen Zutritt haben. Zu den Maßnahmen zum Schutz dieser Sicherheitsbereiche gehören Passier- und Ausweiskontrollen, Besuchereintragung und Anforderungen an Mitarbeiter, jede Person ohne Ausweismarke oder jede unbekannte Person abzufragen.
- Technische Kontrollen sind eingesetzt, um die physische Sicherheit von Informationssystem-komponenten vor Sicherheitsbedrohungen zu gewährleisten.
- Netzwerk- und Servergeräte einschließlich LAN-Server, Netzbrücken und Wegewähler sind durch Unterbringung in abgeschlossenen Räumen oder Schränken physisch vor unbefugtem Zutritt gesichert.
- Sicherheitsrichtlinien sind erstellt, um die Vorgehensweise zur Sicherung von Systemen und Daten insgesamt zu steuern

Zugangskontrolle/Verschlüsselung

Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

- Geräte, Informationen oder Software werden nicht ohne Genehmigung und/oder Protokollierung aus den Räumlichkeiten der TTE (und/oder des Subunternehmers) entfernt.
- Wenn Datenträger entsorgt oder wiederverwendet werden sollen, sind Verfahren eingerichtet worden, um die anschließende Wiedergewinnung der auf ihnen gespeicherten Informationen zu verhindern.
- Wenn Datenträger wegen Wartungsarbeiten die Räumlichkeiten verlassen sollen, in denen die Dateien sich befinden, sind Verfahren eingerichtet worden, um die unzulässige Wiedergewinnung der auf ihnen gespeicherten Informationen zu verhindern.
- Verarbeitung gemäß gängiger Verfahren und Weisungen.
- Verschlüsselungsverfahren werden verwendet, um die Vertraulichkeit der Informationen bei der Übermittlung zu schützen.
- Der Zugriff auf Informationen wird durch Festlegung von Verfahren zum Handhaben, zur Kennung, zum Kopieren, Verteilen, Speichern, Transportieren, Entsorgen und Drucken von Informationen als Hartkopie beschränkt.
- Speichergeräte, die Informationen enthalten, werden physisch zerstört oder sicher über-schrieben und nicht vor Entsorgung oder Wiederverwendung mit einer Löschfunktion behandelt.
- Die Auftragnehmerin (und/oder der Unterauftragnehmer) hat Bereiche für die Aufbewahrung gesammelter Datenträger vorgesehen und gesichert.
- Ein Passwortverwaltungssystem ist eingerichtet worden, um die Nutzerberechtigung zum Zugriff auf die Informationsressourcen zu prüfen.

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass ausschließlich die zur Benutzung der Datenverarbeitungsverfahren Befugten auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

- Sicherheitsrichtlinien sind aufgestellt, um die Vorgehensweise zur Sicherung von Systemen und Daten insgesamt zu steuern, Datenbestände einzustufen, Sicherheitsaufgaben zu klären und das Bewusstsein der Mitarbeiter zu fördern.
- Nur befugte Personen dürfen den Zugriff auf ein Informationssystem gewähren, verändern oder widerrufen, in dem personenbezogene Daten genutzt werden oder untergebracht sind.
- Benutzerverwaltungsverfahren definieren Nutzerrollen und ihre Rechte wie der Zugriff gewährt, verändert und beendet wird; sorgen für die angemessene Trennung der Pflichten; und definieren die Protokollierungs-/Überwachungsanforderungen und -mechanismen.
- Alle Mitarbeiter der Auftragnehmerin (und/oder des Unterauftragnehmers) erhalten eine singuläre Nutzerkennung.
- Zugriffsrechte werden unter Einhaltung der Methode "der geringsten Rechte" realisiert. Nutzer erhalten die geringste Anzahl an Rechten, die zur Erfüllung ihrer Arbeitsaufgaben erforderlich sind.
- Es gibt ein formelles Nutzerregistrierungsverfahren für die Gewährung und Untersagung des Zugriffs auf die Informationsressourcen.
- Die Systeme führen Konfigurationen durch, um Klangpasswörter zu fördern und die Möglichkeit unbefugter Nutzung der Konten zu minimieren.
- Mitarbeiter der Auftragnehmerin (und/oder des Unterauftragnehmers) werden eindeutig identifiziert und durchlaufen eine strenge Anmeldeprozedur bevor sie Zugriff auf Informationsressourcen erhalten.
- Der Systemzugriff wird aufgehoben, wenn der Mitarbeiter der Auftragnehmerin (und/oder des Unterauftragnehmers) den Arbeitsplatz verlässt.
- Protokollierungsmechanismen sind eingesetzt, um sicherzustellen, dass die Person und die Zeit des Datenzugriffs sich später nachvollziehen lassen.
- Deutlich getrennte Produktions- und Prüfbereiche werden von der Auftragnehmerin (und/oder dem Unterauftragnehmer) unterhalten.
- Datenerhebungen und -behandlung werden gemäß den maßgebenden Verfahren und Weisungen durchgeführt.
- Verschlüsselungsmethoden werden eingesetzt, um die Vertraulichkeit der Informationen bei der Übermittlung zu schützen.
- Der Zugriff auf Informationen wird durch Festlegung von Verfahren zum Handhaben, zur Kennung, zum Kopieren, Verteilen, Speichern, Transportieren, Entsorgen und Drucken von Informationen als Hartkopie beschränkt.
- Alle Mitarbeiter der Auftragnehmerin (und/oder des Unterauftragnehmers) erhalten eine singuläre Nutzerkennung.
- Der Fernzugriff auf Systeme und Daten erfordert eine Zweistufenzugriffsberechtigungs-prüfung.
- Es werden periodische Prüfungen von Nutzerkonten durchgeführt, um sicherzustellen, dass die angemessenen Mindestrechte gewährt sind und Konten unbefugter Nutzer entfernt worden sind.

Trennungskontrolle/Zweckbindungskontrolle

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

- Zugriffsrechte werden unter Einhaltung der Methode "der geringsten Rechte" realisiert.
- Zum Schutz von Informationen werden große Netzwerke in einzelne logische Bereiche unterteilt.
- Sämtliches Material wird auf der Anwendungsschicht unter Verwendung von separaten Containern mit Kontrollen, darunter Zugriffs- und Berechtigungskontrollen, logisch getrennt.
- Alle Daten werden in separaten logischen Datenbank-Containern mit Zugriffkontrollen gespeichert.
- Alle Dateien werden in separaten logischen Zugriffsstrukturen mit Zugriffskontrollen gespeichert.

2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)

Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine

Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Datenerhebungen und -behandlung werden gemäß den maßgebenden Verfahren und Weisungen durchgeführt.
- Verschlüsselungsmethoden werden eingesetzt, um die Vertraulichkeit der Informationen bei der Übermittlung zu schützen.
- Der Zugriff auf Informationen wird durch Festlegung von Verfahren zum Handhaben, zur Kennung, zum Kopieren, Verteilen, Speichern, Transportieren, Entsorgen und Drucken von Informationen als Hartkopie beschränkt.
- Hartkopie-Datenträger werden kontrolliert verteilt.
- Speichergeräte, die Informationen enthalten, werden physisch zerstört oder sicher über-schrieben und nicht vor Entsorgung oder Wiederverwendung mit einer Löschfunktion behandelt.
- Geräte, Informationen oder Software werden nicht ohne Genehmigung und/oder Protokollierung aus den Räumlichkeiten der Auftragnehmerin (und/oder des Unterauftragnehmers) entfernt.
- Wenn Datenträger wegen Wartungsarbeiten die Räumlichkeiten verlassen sollen, in denen die Dateien sich befinden, sind Verfahren eingerichtet worden, um die unzulässige Wiedergewinnung der auf ihnen gespeicherten Informationen zu verhindern.
- Die Auftragsnehmerin (und/oder der Unterauftragnehmer) hat Antiviren- und Malwareschutz installiert, um die Sicherheit und Verfügbarkeit der Systeme zu unterstützen.
- Autorisierte Verbindungswege zwischen Nutzern und Diensten werden geleitet und sind beschränkt.
- Ein Einbruchserkennungssystem ist installiert, um Sicherheitsvorfälle zu überwachen und zu protokollieren.
- Der Fernzugriff auf Systeme und Daten erfordert eine Zweistufenzugriffsberechtigungs-prüfung.
- Protokollierungsmechanismen sind eingesetzt, um sicherzustellen, dass die Person und die Zeit des Datenzugriffs sich später nachvollziehen lassen.
- Sichere Datenübertragungsmethoden sind eingerichtet.
- Verschlüsselungsmethoden werden eingesetzt, um die Vertraulichkeit der Informationen bei der Übermittlung zu schützen.
- Geräte, Informationen oder Software werden nicht ohne Genehmigung und/oder Protokollierung aus den Räumlichkeiten der Auftragnehmerin (und/oder des Unterauftragnehmers) entfernt.

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können:

- Protokollierungsmechanismen sind eingesetzt, um sicherzustellen, dass die Person und die Zeit des Datenzugriffs sich später nachvollziehen lassen.
- Prüfprotokolle sind gegen Änderung gesichert und werden unabhängig geprüft.
- Autorisierte Verbindungswege zwischen Nutzern und Diensten werden geleitet und sind beschränkt.
- Wenn Datenträger entsorgt oder wiederverwendet werden sollen, sind Verfahren eingerichtet worden, um die anschließende Wiedergewinnung der auf ihnen gespeicherten Informationen zu verhindern.
- Wenn Datenträger wegen Wartungsarbeiten die Räumlichkeiten verlassen sollen, in denen die Dateien sich befinden, sind Verfahren eingerichtet worden, um die unzulässige Wiedergewinnung der auf ihnen gespeicherten Informationen zu verhindern.
- Die Auftragnehmerin (und/oder der Unterauftragnehmer) hat interne Verfahren eingerichtet, die dafür sorgen, dass die Verarbeitung weisungsgemäß erfolgt.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DSGVO), rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c) DSGVO

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (die Angaben beziehen sich auf eigene IT-Systeme des Auftragnehmers):

- Die Auftragnehmerin (und/oder der Unterauftragnehmer) hat geeignete Pläne zur Katastrophen-Behebung und Wiederaufnahme der Geschäftstätigkeit erstellt. TTE (und/oder der Subunternehmer) prüfen regelmäßig sowohl den Plan zur Kontinuität der Geschäftstätigkeit als auch die Risikobewertung. Pläne zur Kontinuität der Geschäftstätigkeit werden getestet und regelmäßig aktualisiert, um zu gewährleisten, dass sie auf dem neuesten Stand und wirksam sind.

- Die Auftragnehmerin (und/oder der Unterauftragnehmer) hat Datensicherungspläne aufgestellt und setzt automatische Datensicherungssysteme zur Datenverwaltung ein. Datensicherungskopien werden sicher aufbewahrt.
- Die Rechenzentrumsanlagen der Auftragnehmerin (und/oder des Unterauftragnehmers) unterhalten zusätzliche Strom- und Netzwerksysteme und vernünftige Umgebungskontrollen, um die Kontinuität der Systemverfügbarkeit zu gewährleisten.
- Die Auftragnehmerin (und/oder der Unterauftragnehmer) hat Antiviren- und Malwareschutz installiert, um die Sicherheit und Verfügbarkeit der Systeme zu unterstützen

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO, Art. 25 Abs. 1 DSGVO)

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftragsgebers verarbeitet werden können:

- Personenbezogene Daten werden für interne Zwecke genutzt und nur soweit dies zur Erbringung der in der Vereinbarung (und etwaigen Änderungen) genannten Leistungen und dieser Anlage gemäß § 11 Bundesdatenschutzgesetz vom April 2015 erforderlich ist.
- Die Auftragnehmerin (und/oder der Unterauftragnehmer) handelt in Übereinstimmung mit den Bedingungen hinsichtlich Verarbeitung wie in der Vereinbarung und dieser Anlage aufgeführt.
- Die Auftragnehmerin (und/oder der Unterauftragnehmer) hat interne Verfahren eingerichtet, die dafür sorgen, dass die Verarbeitung weisungsgemäß erfolgt.

Datenschutz-Management

Maßnahmen, die eine Steuerung der Datenschutzprozesse ermöglichen und die Einhaltung der datenschutzrechtlichen Vorgaben nachweisbar sicherstellen:

- Die Auftragnehmerin (und/oder der Unterauftragnehmer) hat einen Beauftragten für den Datenschutz bestimmt und Persönlichkeitsschutzregeln aufgestellt.
- Überwachungssysteme werden eingesetzt, um die Systemkapazität und Nutzung zu verwalten.
- Alle Vorfälle personenbezogener Datensicherheit werden gemäß den entsprechenden Vorfalls-reaktionsverfahren behandelt.
- Die Auftragnehmerin (und/oder der Unterauftragnehmer) hat Datensicherungspläne aufgestellt und setzt automatische Datensicherungssysteme zur Datenverwaltung ein. Datensicherungskopien werden sicher aufbewahrt.
- Die Rechenzentrumsanlagen der Auftragnehmerin (und/oder des Unterauftragnehmers) unterhalten zusätzliche Strom- und Netzwerksysteme und vernünftige Umgebungskontrollen, um die Kontinuität der Systemverfügbarkeit zu gewährleisten.
- Die Auftragnehmerin (und/oder der Unterauftragsnehmer) hat Antiviren- und Malwareschutz installiert, um die Sicherheit und Verfügbarkeit der Systeme zu unterstützen
- Die Auftragnehmerin (und/oder der Unterauftragnehmer) hat interne Verfahren eingerichtet, die dafür sorgen, dass die Verarbeitung weisungsgemäß erfolgt.
- Ein Passwortverwaltungssystem ist eingerichtet worden, um die Nutzerberechtigung zum Zugriff auf die Informationsressourcen zu prüfen.
- Die Systeme führen Konfigurationen durch, um Klangpasswörter zu fördern und die Möglichkeit unbefugter Nutzung der Konten zu minimieren.
- Es werden periodische Prüfungen von Nutzerkonten durchgeführt, um sicherzustellen, dass die angemessenen Mindestrechte gewährt sind und Konten unbefugter Nutzer entfernt worden sind.
- Die Auftragnehmerin (und/oder der Unterauftragnehmer) hat die Verantwortung für die Compliance-Verwaltung und unterstützende Funktionen bestimmt und zugewiesen.
- Die Auftragnehmerin (und/oder der Unterauftragnehmer) erwägt die Aufgabentrennung bei der Gestaltung der organisatorischen Strukturen und die Zuweisung von dienstlichen Pflichten.
- Die Auftragnehmerin (und/oder der Unterauftragnehmer) hat Richtlinien für die Handhabung von Softwareentwicklung und -änderung aufgestellt
- Die Auftragnehmerin (und/oder der Unterauftragnehmer) hat die Leitung für den Einkauf von Hardware und Software zentralisiert.
- Es wurde ein dokumentiertes Datenschutz-Management-System eingeführt, um die Vorgaben der DSGVO zu steuern.

Anlage 3: Unterauftragnehmer

Name, Anschrift/Land, Auftragsinhalt

Mittwald CM Service GmbH & Co. KG / Deutschland, Speicherung von Daten (Hosting)
Artur Heinze (Agentejo) / Deutschland, IT Entwicklung und Support
Usersnap GmbH / Österreich, Kunden-Feedback Tool