

Auftragsverarbeitungsvertrag

zwischen

Stiftung Innovation in der Hochschullehre
Treuhandstiftung in Trägerschaft der Toepfer Stiftung gGmbH
Raboisen 30
20095 Hamburg
Deutschland

– im Folgenden auch „**Auftraggeber**“ genannt –

und

[Wird nach Zuschlagserteilung ergänzt]

– im Folgenden auch „**Auftragsverarbeiter**“ genannt –

vertreten durch

[Wird nach Zuschlagserteilung ergänzt]

– im Folgenden werden Auftraggeber und Auftragsverarbeiter
gemeinsam auch **Parteien** genannt –

1. **Gegenstand des Auftrags** (Art. 28 Abs. 3 DS-GVO)

1.1 Der Auftragsverarbeiter erhebt und verarbeitet personenbezogene Daten im Auftrag des Auftraggebers.

1.2 Näheres zum Gegenstand des Auftrages ergibt sich aus dem EVB-IT Systemvertrag (im Folgenden „Hauptvertrag“) vom [Wird nach Zuschlagserteilung ergänzt]

2. **Dauer des Auftrags** (Art. 28 Abs. 3 DS-GVO)

2.1 Die Laufzeit dieses Vertrages entspricht der des in Ziff. 1 genannten Hauptvertrages. Die Regelungen zur Beendigung oder Kündigung des Hauptvertrages gelten entsprechend.

Dieser Auftragsverarbeitungsvertrag gilt jedoch insofern über die Laufzeit des Hauptvertrages hinaus, sofern der Auftragsverarbeiter dann noch personenbezogene Daten, die ihm zur Auftragserfüllung übermittelt wurden, speichert.

- 2.2 Der Auftraggeber kann diesen Vertrag jederzeit aus wichtigem Grund ohne Einhaltung einer Frist kündigen. Ein wichtiger Grund liegt u. a. vor, wenn der Auftragsverarbeiter in besonders schwerem Maße gegen die Bestimmung dieses Vertrages verstößt, der Auftragsverarbeiter beharrlich eine Weisung des Auftraggebers zur rechtmäßigen Datenverarbeitung nicht ausführen kann oder will oder der Auftragsverarbeiter den Zutritt des Auftraggebers zu Kontrollzwecken beharrlich vertragswidrig verweigert.

3. Umfang, Art und Zweck der vorgesehenen Datenverarbeitung; Übermittlungen in Drittländer (Art. 28 Abs. 3 DS-GVO)

- 3.1 Umfang, Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter für den Auftraggeber sind konkret in dem in Ziff. 1.2 genannten Vertrag und/oder in der Leistungsbeschreibung der Parteien beschrieben.

- 3.2 Die Verarbeitung und Nutzung der Daten finden ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, der Niederlande oder in anderen einem Mitgliedsstaat der Europäischen Union statt. Jede Verlagerung in ein Drittland und jeder Zugriff aus einem Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

4. Art der personenbezogenen Daten (Art. 28 Abs. 3 DS-GVO)

Gegenstand der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter sind insbesondere folgende Daten bzw. Datenkategorien:

- Name
- Adresse (Straße und Hausnummer, Wohnort)
- Telefonnummer
- E-Mail-Adresse
- Geburtsdatum
- Geschlecht
- Beruf, Position, Arbeitsbereich
- Newsletter-Einwilligung

5. Kategorien betroffener Personen (Art. 28 Abs. 3 DS-GVO)

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags betroffenen Personen umfasst:

- Personen, die einen Förderantrag bei der Stiftung Innovation in der Hochschullehre gestellt haben.

6. Technische und organisatorische Maßnahmen/Sicherheit der Datenverarbeitung (Art. 28 Abs. 3 lit. c DS-GVO)

6.1 Der Auftragsverarbeiter gestaltet seine innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Zu diesem Zweck werden zu den Regelungstatbeständen des Art. 32 DS-GVO die in **Anhang A** genannten technischen und organisatorischen Maßnahmen **als Mindeststandard** verbindlich festgelegt. Weitergehende Pflichten, die nach Art. 32 DS-GVO in seiner jeweiligen Fassung für den Auftragsverarbeiter gelten, bleiben unberührt.

6.2 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Der Auftragsverarbeiter hat auf Anforderung die Angaben nach Art. 30 DS-GVO dem Auftraggeber zur Verfügung zu stellen.

7. Berichtigung, Löschung und Sperrung von Daten (Art. 28 Abs. 3 lit. a DS-GVO)

7.1 Der Auftragsverarbeiter hat nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder die Datenverarbeitung einzuschränken. Dokumentationen, die dem Nachweis der auftrags- oder ordnungsgemäßen Datenverarbeitung durch den Auftragsverarbeiter und etwaige Unterauftragsverarbeiter dienen, können unter Berücksichtigung des Art. 17 DS-GVO ggf. aufbewahrt und verarbeitet werden. Gesetzliche Aufbewahrungsfristen des Auftragsverarbeiters und etwaiger Unterauftragsverarbeiter bleiben unberührt.

7.2 Soweit eine betroffene Person sich unmittelbar an den Auftragsverarbeiter zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

8. Pflichten des Auftragsverarbeiters, insbesondere die von ihm vorzunehmenden Kontrollen (Art. 28 Abs. 1 und Abs. 3 lit. d DS-GVO)

8.1 Der Auftragsverarbeiter wird hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet (Art. 28 Abs. 1 DS-GVO).

- 8.2 Der Auftragsverarbeiter hat sicherzustellen, dass bei ihm stets ein betrieblicher Datenschutzbeauftragter, der die erforderliche Fachkunde und Zuverlässigkeit besitzt, bestellt ist.
- 8.3 Der Auftragsverarbeiter stellt sicher, dass alle zur Verarbeitung der personenbezogenen Daten befugten Personen sich ihm gegenüber schriftlich zur Einhaltung datenschutzrechtlicher Bestimmungen und zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DS-GVO). Der Auftragsverarbeiter wird die von ihm bei der Verarbeitung von personenbezogenen Daten eingesetzten Personen ausreichend in allen relevanten Fragen des Datenschutzrechts und der Datensicherheit schulen.
- 8.4 Der Auftragsverarbeiter führt auch bezüglich dieses Auftrags regelmäßig im Hinblick auf die Vertragsausführungen bzw. -erfüllung die Auftragskontrolle durch, insbesondere bzgl. der Einhaltung und bzgl. ggf. notwendiger Anpassungen von Regelungen und Maßnahmen zur Durchführung des Auftrages.
- 8.5 Der Auftragsverarbeiter sichert die Umsetzung, Einhaltung und Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber zu. Hierzu kann der Auftragsverarbeiter aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragte, IT-Sicherheitsabteilung, Datenschutzauditors, Qualitätsauditors) oder geeignete Zertifizierungen durch IT-Sicherheits- oder Datenschutzaudits (z.B. nach BSI-Grundschutz) vorlegen.
- 8.6 Der Auftragsverarbeiter wird angesichts der Art der Verarbeitung den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DS-GVO genannten Rechte der betroffenen Personen nachzukommen (Art. 28 Abs. 3 lit. e DS-GVO).
- 8.7 Der Auftragsverarbeiter wird unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Art. 32 bis 36 genannten Pflichten unterstützen (Art. 28 Abs. 3 lit. f DS-GVO).
- 8.8 Der Auftragsverarbeiter wird dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DS-GVO in seiner jeweiligen Fassung niedergelegten Pflichten zur Verfügung stellen und Überprüfungen – einschließlich Inspektionen –, die von dem Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und dazu beitragen (Art. 28 Abs. 3 lit. h DS-GVO).

- 8.9 Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden und die personenbezogene Daten enthalten, werden besonders gekennzeichnet.

9. Berechtigung zur Begründung von Unterauftragsverhältnissen mit weiteren Auftragsverarbeitern (Art. 28 Abs. 2 DS-GVO)

- 9.1 Die Beauftragung von weiteren Auftragsverarbeitern im Rahmen einer Auftragsdatenverarbeitung (Unterauftragsverarbeiter) ist dem Auftragsverarbeiter nur unter Einhaltung der nachfolgenden Regelungen gestattet.

- 9.2 Die Beauftragung von Unterauftragsverarbeitern ist nur mit vorheriger schriftlicher Zustimmung des Auftraggebers zulässig.

- 9.3 Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Auftraggeber über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters. In diesem Fall hat der Auftraggeber das Recht gegen die Hinzuziehung des neuen Unterauftragsverarbeiters Einspruch zu erheben.

Erhebt der Auftraggeber Einspruch, ist die Hinzuziehung eines Unterauftragsverarbeiters unzulässig.

- 9.4 Der Auftragsverarbeiter wird die in Art. 28 Abs. 2 und 4 DS-GVO genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhalten.

- 9.5 Der Auftragsverarbeiter muss den Unterauftragsverarbeiter sorgfältig auswählen.

- 9.6 Der Vertrag mit etwaigen Unterauftragsverarbeitern muss Art. 28 DS-GVO entsprechen und dabei die für das zwischen den Parteien bestehende Auftragsverhältnis in diesem Vertrag vorhandenen Regelungen entsprechend gegenüber dem Unterauftragsverarbeiter umsetzen. Der Auftragsverarbeiter ist verpflichtet, die für den Datenschutz relevanten vertraglichen Vereinbarungen mit dem Unterauftragsverarbeiter dem Auftraggeber auf Verlangen zur Kenntnis zu bringen. Insofern ist ein Zurückbehaltungsrecht ausgeschlossen.

- 9.7 Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Weisungsrechte entsprechend diesem Vertrag und Art. 28 Abs. 3 DS-GVO beim Unterauftragsverarbeiter einzuräumen. Dies umfasst auch das Recht des Auftraggebers, von dem Unterauftragsverarbeiter auf schriftliche Anforderung Auskunft über den datenschutzrelevanten Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, auf Verlangen durch Übermittlung von Kopien der relevanten Vertragsunterlagen, zu erhalten.

- 9.8 Der Auftragsverarbeiter hat die Einhaltung der Pflichten des Unterauftragsverarbeiters vor der ersten Übermittlung personenbezogener Daten und danach regelmäßig zu prüfen.
- 9.9 Die Weiterleitung von Daten an einen Unterauftragsverarbeiter ist erst zulässig, wenn dieser die oben genannten technischen und organisatorischen Maßnahmen zur Datensicherheit angemessenen umgesetzt hat.
- 9.10 Erbringt der Unterauftragsverarbeiter die vereinbarte Leistung im Einklang mit diesem Vertrag und dem Unterauftragsverarbeitungsvertrag außerhalb der Europäischen Union und außerhalb der Mitgliedstaaten des Abkommen über den Europäischen Wirtschaftsraum, stellt der Auftragsverarbeiter die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne der vorstehenden Absätze eingesetzt werden sollen.
- 9.11 Eine weitere Auslagerung der Datenverarbeitung durch den Unterauftragsverarbeiter bedarf der ausdrücklichen Zustimmung des Auftraggebers (Hauptauftraggeber) Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragsverarbeiter aufzuerlegen.
- 10. Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragsverarbeiters (Art. 28 Abs. 3 lit. h DS-GVO)**
- 10.1 Der Auftragsverarbeiter erklärt sich damit einverstanden, dass der Auftraggeber jederzeit berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und die Einhaltung der vertraglichen Pflichten zu kontrollieren. Der Auftragsverarbeiter ist verpflichtet, jegliche für diese Kontrolle erforderlichen Auskünfte zu geben und die erforderliche Einsichtnahme in gespeicherte Daten, Datenverarbeitungsprogramme und Unterlagen sowie Zugang zu allen relevanten betrieblichen Einrichtungen zu gewähren.
- 10.2 Sofern nicht ein wichtiger Grund für eine aktuelle Kontrollmaßnahme vorliegt, ist die Kontrollmaßnahme mit einer Frist von einer Woche anzukündigen. Ein wichtiger Grund für eine unverzügliche Kontrollmaßnahme liegt u. a. in den Fällen der Art. 33 und 34 DS-GVO vor, sofern die Verletzung des Schutzes personenbezogener Daten in der Sphäre des Auftragsverarbeiters erfolgt ist.
- 10.3 Der Auftragsverarbeiter ist damit einverstanden, dass Kontrollen auch von Dritten durchgeführt werden, für die der Auftraggeber als Unterauftragsverarbeiter die Datenverarbeitungsleistungen erbringt, die Gegenstand dieses Vertrages sind.

- 11. Mitwirkungspflichten des Auftragsverarbeiters; mitzuteilende Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen (Art. 28 Abs. 3 f) DS-GVO)**
- 11.1 Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten und stellt alle für den Auftraggeber zur Erstellung des Verzeichnisses der Verarbeitungstätigkeiten nach Art. 30 DS-GVO relevanten Informationen, die seine Tätigkeit betreffen, zur Verfügung.
- 11.2 Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, wenn er oder eine bei ihm beschäftigte Person gegen Vorschriften zum Schutz personenbezogener Daten, gegen Bestimmungen nach diesem Vertrag zur Auftragsverarbeitung oder gegen eine vom Auftraggeber erteilte sonstige Weisung verstoßen hat, insbesondere wenn Anhaltspunkte dafür bestehen, dass ein Dritter – egal aus welchem Grund – unrechtmäßig Kenntnis von Auftraggeberdaten erlangt haben könnte oder wenn in sonstiger Weise eine Gefährdung für die Integrität oder Vertraulichkeit der Auftraggeberdaten eingetreten ist. Die Information hat unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntniserlangung seitens des Auftragsverarbeiters zu erfolgen. Dabei sind gegenüber dem Auftraggeber Angaben über den Zeitpunkt und die Art des Vorfalls (einschließlich einer Information, welche Auftraggeberdaten wie betroffen sind), das betroffene EDV-System, die betroffenen Personen, den Zeitpunkt der Entdeckung, alle denkbaren nachteiligen Folgen des Datensicherheitsvorfalls sowie die von dem Auftragsverarbeiter daraufhin ergriffenen Maßnahmen zu machen. Der Auftragsverarbeiter ist verpflichtet, den Auftraggeber auf erstes Anfordern unverzüglich im Rahmen des Zumutbaren zu unterstützen, um etwaige nachteilige Folgen für den Auftraggeber oder betroffene Personen zu verhindern.
- 11.3 Dies gilt insbesondere in den Fällen, in denen gemäß Art. 33 oder 34 DS-GVO eine Meldepflicht gegenüber der Aufsichtsbehörde oder eine Benachrichtigungspflicht gegenüber der betroffenen Person bestehen könnte. In diesen Fällen hat die Information unverzüglich zu erfolgen.
- 11.4 In Fälle des Art. 33 oder 34 DS-GVO übermittelt der Auftragsverarbeiter unverzüglich die für die Erfüllung von Melde- und Nachweispflichten des Auftraggebers notwendigen Informationen einschließlich der Informationen nach Art. 33 Abs. 3 DS-GVO.

12. Umfang der Weisungsbefugnisse des Auftraggebers (Art. 28 Abs. 3 a) DS-GVO)

- 12.1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – ausschließlich nach Weisung des Auftraggebers, sofern nicht ein Ausnahmefall im Sinne des Art. 28 Abs. 3 lit. a DS-GVO vorliegt. Der Auftraggeber hat das Recht, die im Rahmen der oben genannten Aufgabenbeschreibung erfolgende Datenverarbeitung in Bezug auf Art, Umfang und Verfahren im Einzelfall zu konkretisieren. Auskünfte an Dritte oder die betroffenen Personen darf der Auftragsverarbeiter nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen, sofern der dazu nicht rechtlich verpflichtet ist.
- 12.2 Weisungen sollen grundsätzlich schriftlich oder in Textform (z. B. per E-Mail) erteilt werden. Mündliche Weisungen wird der Auftraggeber ab diesem Zeitpunkt schriftlich oder per E-Mail (in Textform) bestätigen. Die Bestätigung ist keine Voraussetzung für die Verbindlichkeit der Weisung. Der Auftragsverarbeiter ist verpflichtet, die Weisungen zu dokumentieren und die Dokumentation ggf. dem Auftraggeber auf Anfrage zur Verfügung zu stellen.
- 12.3 Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte im eigenen Interesse weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hier-von ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung oder zur Erfüllung gesetzlicher Aufbewahrungspflichten erforderlich sind.
- 12.4 Der Auftragsverarbeiter hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragsverarbeiter ist in diesen Fällen berechtigt, die Durchführung der Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

13. Rückgabe überlassener Datenträger, Löschung beim Auftragsverarbeiter gespeicherter Daten nach Beendigung des Auftrags (Art. 28 Abs. 3 g) DS-GVO)

Nach Beendigung des Auftrags – auf Aufforderung durch den Auftraggeber unverzüglich – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, Dateien und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Vertragsverhältnis stehen und personenbezogene Daten enthalten, dem Auftraggeber auszuhändigen bzw. verfügbar zu machen oder nach vorheriger Zustimmung oder Weisung des Auftraggebers datenschutzgerecht zu

vernichten. Dokumentationen, die dem Nachweis der auftrags- oder ordnungsgemäßen Datenverarbeitung durch den Auftragsverarbeiter und etwaige Unterauftragsverarbeiter dienen, können unter Berücksichtigung des Art. 17 DS-GVO ggf. aufbewahrt und verarbeitet werden.

14. Kosten

In Bezug auf die Erfüllung der nach diesem Vertrag und der DS-GVO bestehenden Pflichten, einschließlich der Pflichten nach Ziff. 6, 7, 8, 9, 10, 11 und 13, besteht kein Anspruch auf Vergütung oder Aufwendungsersatz des Auftragsverarbeiters gegenüber dem Auftraggeber.

15. Haftung/Freistellung

15.1 Wenn Dritte gegenüber dem Auftraggeber einen Anspruch wegen einer gegen Datenschutzbestimmungen verstoßenden Verarbeitung des Auftragsverarbeiters geltend machen, wird der Auftragsverarbeiter den Auftraggeber von allen solchen Ansprüchen gemäß den nachfolgenden Regelungen vollumfänglich freistellen.

15.1.1 Für den Fall, dass Dritte gegenüber dem Auftraggeber Ansprüche nach der vorstehenden Regelung geltend machen, wird der Auftraggeber den Auftragsverarbeiter unverzüglich darüber zumindest in Textform gemäß § 126b BGB informieren und dem Auftragsverarbeiter die gerichtliche und außergerichtliche Abwehr dieser Ansprüche überlassen. Sofern der Auftragsverarbeiter nicht innerhalb von dreißig Kalendertagen nach vorstehender Anzeige mit der Abwehr solcher Ansprüche beginnt, kann der Auftraggeber die Abwehr selbst vornehmen. Der Auftragsverarbeiter wird den Auftraggeber von allen angemessenen Aufwendungen und Kosten, die aus solchen Verfahren herrühren, freistellen, einschließlich angemessener Anwaltsgebühren.

15.1.2 Sofern der Auftraggeber selbst die Ansprüche abwehrt oder durch Vergleich beendet, wird sich der Auftraggeber nicht zu Lasten des Auftragnehmers äußern. Der Auftraggeber wird keinen Vergleich abschließen, ohne vorher die Einwilligung des Auftragsverarbeiters eingeholt zu haben. Für den Fall, dass dem Auftragsverarbeiter bzw. dem Auftraggeber die erfolgreiche Abwehr von Ansprüchen innerhalb eines Rechtsstreits oder anderen Verfahrens ganz oder teilweise nicht gelingt, wird der Auftragnehmer den Auftraggeber von allen Schäden und/oder Kosten freistellen, die dem Dritten durch endgültige Gerichtsentscheidung, Schiedsgerichtsentscheidung oder durch Vergleich zugesprochen werden.

15.1.3 Auf schriftliche Anfrage des Auftragsverarbeiters wird der Auftraggeber auf Kosten des Auftragnehmers angemessene Hilfestellung leisten, um den Auftragsverarbeiter bei der Beendigung durch Vergleich und/oder der Abwehr von Ansprüchen in einem Rechtsstreit oder anderen Verfahren zu unterstützen. Für den Fall, dass der Auftraggeber selbst die Abwehr vornimmt, erklärt sich der Auftragsverarbeiter ebenfalls zur angemessenen Unterstützung des Auftragsverarbeiters bereit.

15.2 Wenn Dritte gegenüber dem Auftragsverarbeiter einen Anspruch wegen einer gegen Datenschutzbestimmungen verstoßenden Verarbeitung des Auftraggebers geltend machen, wird der Auftraggeber den Auftragsverarbeiter von allen solchen Ansprüchen freistellen. Die vorstehenden Ziffern Ziff. 15.1.1 bis 15.1.3 gelten entsprechend.

16. Vertragsstrafe

Für jeden Fall der Zuwiderhandlung verpflichtet sich der Auftragsverarbeiter zu Zahlung einer Vertragsstrafe. Die Höhe der Vertragsstrafe ist im Einzelfall nach billigem Ermessen durch den Auftraggeber zu bestimmen (§ 315 BGB). Bei der Bestimmung der Höhe der Vertragsstrafe im Einzelfall hat der Auftraggeber die Schwere und die Dauer der Vertragsverletzung einschließlich der beim Auftraggeber drohenden oder eingetretenen Schadenshöhe, die Schwere des Verschuldens des Auftragsverarbeiters, aber auch die mit der Vertragsstrafe grundsätzlich verbundene Zwecksetzung als Abschreckungs-, Druck- und Sicherungsmittel angemessen zu berücksichtigen. Ist im Einzelfall die Vertragsstrafe zu hoch bemessen, gilt § 343 BGB (Herabsetzung der Strafe). Das Recht des Auftraggebers zur Geltendmachung eines weitergehenden Schadens bleibt unberührt. Die Vertragsstrafe ist auf einen korrespondierenden Schadensersatz anzurechnen.

17. Inkrafttreten, Schriftform, Zurückbehaltungsrecht, Vertragsauslegung, Verweise auf rechtliche Bestimmungen

17.1 Dieser Vertrag tritt mit beidseitiger Unterzeichnung (maßgeblich ist die letzte Unterschrift) in Kraft.

17.2 Mündliche Nebenabsprachen sind nicht getroffen worden. Änderungen, Ergänzungen sowie die Aufhebung dieses Vertrags oder seiner Bestandteile bedürfen mindestens der Textform. Dies gilt auch für eine Änderung dieser Klausel selbst. § 305b BGB bleibt unberührt. Für den Inhalt derartiger Vereinbarungen ist, vorbehaltlich des Gegenbeweises, ein schriftlicher Vertrag bzw. eine schriftliche Bestätigung des Auftraggebers maßgebend.

- 17.3 Die Einrede des Zurückbehaltungsrechtes im Sinne von § 273 BGB wird in Bezug auf die Herausgabe von Daten und Datenträgern an den Auftraggeber ausgeschlossen.
- 17.4 Sollte eine Bestimmung des Vertrages unwirksam oder undurchführbar sein oder werden oder der Vertrag eine Lücke enthalten, wird hierdurch die Wirksamkeit des Vertrages im Übrigen nicht berührt. Die Regelungen dieser Ziff. 17.4 beinhalten keine bloße Beweislastumkehr, sondern schließen die Anwendung des § 139 BGB aus. Im Fall einer Lücke gilt diejenige wirksame und durchführbare Bestimmung als vereinbart, die dem rechtlichen und wirtschaftlichen Ziel dieses Vertrages am nächsten kommt.
- 17.5 Sofern diese Vereinbarung auf rechtliche Bestimmungen verweist, werden diese Bestimmungen in ihrer jeweiligen Fassung in Bezug genommen.

18. Rechtswahl und Gerichtsstand

- 18.1 Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts und unter Ausschluss des deutschen Kollisionsrechts Anwendung. Die gesetzlichen Vorschriften zur Beschränkung der Rechtswahl und zur Anwendbarkeit zwingender Vorschriften bleiben unberührt.
- 18.2 Ausschließlicher Gerichtsstand ist Hamburg, sofern der Auftragsverarbeiter Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist oder im Inland keinen allgemeinen Gerichtsstand hat. Dem Auftraggeber bleibt es jedoch vorbehalten, gerichtliche Schritte auch am allgemeinen Gerichtsstand des Auftragsverarbeiters einzuleiten. Vorrangige gesetzliche Vorschriften, insbesondere zu ausschließlichen Zuständigkeiten, bleiben unberührt.

(Unterschriftenseite folgt)

.....
Ort, Datum

.....
Ort, Datum

.....
Auftraggeber

.....
Auftragsverarbeiter

Anhang A: Technische und organisatorische Maßnahmen / Sicherheit der Datenverarbeitung

Die TOMs des Bieters sind dem Angebot im Vergabeverfahren beizufügen. Untenstehend ein Muster zur Orientierung. Nochmals: Dieses ist keinesfalls verpflichtend.

Anhang A

(Technische und organisatorische Maßnahmen / Sicherheit der Datenverarbeitung)

1. Vertraulichkeit (Art. 32 Abs. 1 b) DS-GVO), Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 a) DS-GVO)

a. Zutrittskontrolle

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

- XX (Bsp. Schlüsselvergabe)
- XX (Bsp. Protokolle)

b. Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Identität und Authentizität von Benutzern wird durch Benutzerkennung und Passworte sichergestellt. Es wird generell eine 2-Faktor-Autorisierung genutzt.
- An den Arbeitsplätzen ist eine zeitabhängige automatische Sperrung zu aktivieren.
- Zugang zu lokalen Serversystemen nur für definierte Personen
- Generelle Verschlüsselung von Datenträgern (Notebooks)
- Logging der Zugänge bei Cloud-Systemen (Logbuch)

c. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zurückgreifen können und dass personenbezogene Daten bei der Verarbeitung und Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Es wird ein Zugriffsberechtigungskonzept installiert, das sicherstellt, dass ein Zugriff auf die personenbezogenen Daten nur den Personen gewährt wird, die den Zugriff auf diese Daten zur Erledigung ihrer Aufgabe benötigen.
- Das Zugriffsberechtigungskonzept wird laufend von ausgewählten Personen aktualisiert. Die Vergabe und Rücknahme von Zugriffsberechtigungen unterliegt einem definierten Verfahren und wird dokumentiert.
- Protokollierung von Zugriffen
- Datenträger werden gesichert aufbewahrt.
- Ordnungsgemäße Vernichtung von Datenträgern entsprechend DIN 66399

d. Trennungskontrolle

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

- Zugriffsberechtigungskonzept, das getrennte Verarbeitungen ermöglicht und unberechtigte Zugriffe ausschließt
- Physikalisch getrennte Speicherung
- Logisch getrennte Speicherung (Mandantenfähigkeit der Systeme)

e. Pseudonymisierung

Daten werden in angemessenem Umfang zur Umsetzung des Grundsatzes der Datenminimierung pseudonymisiert, wodurch sie ohne Hinzuziehen zusätzlicher Informationen nicht mehr einer bestimmten Person zugeordnet

werden können. Die zusätzlichen Informationen sind gesondert aufzubewahren und durch organisatorische und technische Maßnahmen vor dem Zugriff Unberechtigter zu sichern.

- Es erfolgt keine Pseudonymisierung von Daten auf Auftragnehmer-Seite, in diesem Fall werden die Daten gelöscht.

2. Integrität (Art. 32 Abs. 1 b) DS-GVO)

a. 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 welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtung zur Datenübertragung vorgesehen ist:

- Personenbezogene Daten dürfen grundsätzlich nur über sichere Leitungen (SSL, VPN¹) in verschlüsselter Form und/oder digital signiert übertragen werden.
- Es erfolgt keine Weitergabe von Datenträgern, die personenbezogene Daten beinhalten. Daten werden digital in eigenen digitalen Safes verschlüsselt abgelegt.
- Alle Datenübermittlungen (u.a. Zugangsdaten oder Kennwörter) erfolgen in geeigneter Weise und dokumentiert. Speziell Kennwörter müssen von der betroffenen Person im Einzelfall umgehend geändert werden.

b. Eingabekontrolle

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

- Protokollierung von Dateneingaben oder -veränderungen einschließlich Benutzerkennung und Eingabe- bzw. Änderungsdatum in angemessenem Umfang. XX
- XX kann ausgewertet werden.

¹ Virtual Private Network

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 b) und c) DS-GVO)

a. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Installation eines Datensicherungs-/Back-Up-Verfahrens
- Permanente Überwachung der Funktionsfähigkeit der Datensicherung
- Regelmäßige Tests der Wiederherstellbarkeit der Systeme aus der Datensicherung
- Feuer-/Rauch- und Wasserschutz, Überspannungsschutz und Gewährleistung einer unterbrechungsfreien Stromversorgung
- Sicherheitsrichtlinien sind schriftlich dokumentiert. Es gibt Auftraggeberseitig einen ausgebildeten Datenschutzbeauftragten.

b. Wiederherstellbarkeit

Geeignete Maßnahmen, um den Zugang zu etwaig nicht verfügbaren Daten bei einem technischen und organisatorischen Zwischenfall rasch wieder herzustellen.

- Installation eines Datensicherungs-/Back-Up-Verfahrens
- Redundanz von Systemen und Komponenten
- Monitoring der Systemverfügbarkeit

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 d) DS-GVO; Art. 25 Abs. 1 DS-GVO)

Maßnahmen, die gewährleisten, dass die Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit regelmäßig überprüft, bewertet und evaluiert wird:

- Laufende Verfügbarkeit eines ausgebildeten, zertifizierten Datenschutzbeauftragten
- Routine zur Überprüfung der implementierten Sicherheitsmaßnahmen durch den zertifizierten Datenschutzbeauftragten

- Bereitstellung und Nutzung eines Incident-Response-Management (Vorfall-Reaktions-Plan);
- Laufende Anpassung der Maßnahmen an geänderte/neue Gefahren-Situationen, in Abstimmung mit AG
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Regelmäßige Penetrationstests von Kundenanwendungen, Simulation von Angriffen und Störereignissen
- Auswertung von etwaigen Sicherheitsvorfällen
- Regelmäßige Brandschutz- und Notfallübungen

5. Auftragskontrolle

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

- Überwachung der mit der Auftragsdatenverarbeitung Beschäftigten bzgl. der ausschließlichen Verarbeitung personenbezogener Daten entsprechend den Regelungen des Auftragsdatenverarbeitungsvertrages und der Weisungen des Auftraggebers.
- Verpflichtung der mit der Auftragsdatenverarbeitung Beschäftigten auf Vertraulichkeit und zur Verschwiegenheit.
- Verfügbarkeit eines zertifizierten Datenschutzbeauftragten
- Die Beauftragung von Unterauftragnehmern ist nur mit schriftlicher Genehmigung des Auftraggebers zulässig.
- Unterauftragnehmer sind sorgfältig auszuwählen.
- Die Vereinbarung mit Unterauftragnehmern muss den Regelungen dieses Vertrages, einschließlich den Regelungen über die technischen und organisatorischen Maßnahmen zur Datensicherheit, entsprechen.