Vereinbarung zur Auftragsverarbeitung zum Vertrag

zwischen dem/der

_____
Verantwortlicher, nachfolgend Auftraggeber genannt

und dem/der

SHEROES UG, Überseeboulevard 2, 20457 Hamburg

_____
Auftragsverarbeiter, nachfolgend Auftragnehmer genannt

Präambel

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien im Auftragsverhältnis gemäß Art. 28 DSGVO. Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Vertrages.

Sie findet Anwendung auf alle Tätigkeiten des Auftragnehmers, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten des Auftraggebers verarbeiten.

§ 1 Gegenstand und Dauer des Auftrags

1. Gegenstand

Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung **Webtracking, Datenbank-Systeme, Schnittstellenentwicklung und Beratung in den Bereichen Data-Warehouse (DWH) und Business Intelligence** vom _____, auf die ausdrücklich verwiesen wird.

2. Dauer

Die Dauer dieses Auftrags entspricht der Laufzeit der Leistungsvereinbarung.

Das Recht zur fristlosen außerordentlichen Kündigung bleibt hiervon unberührt. Die fristlose Kündigung ist insbesondere möglich, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften, oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will, oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

§ 2 Inhaltskonkretisierung

1. Art der personenbezogenen Daten (Art. 4 Nr. 1, 13, 14 und 15 DSGVO)

Folgende Arten (Kategorien) von personenbezogenen Daten werden verarbeitet:

- **Personenstammdaten (Vorname, Nachname, Geburtsdatum)**
- **Adressdaten**
- **Kommunikationsdaten (Telefon, E-Mail, Fax)**
- **Nutzerdaten**
- **Logfiles**
- **User Tracking der eigenen Websites**
- **User Tracking auf fremden Websites**

2. Art und Zweck der Verarbeitung (Art. 4 Nr. 2 DSGVO):

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind im **§1** der Leistungsvereinbarung vom _____ beschrieben.

Konkrete Beschreibung des Auftragsgegenstandes hinsichtlich Art und Zweck der Verarbeitung durch den Auftragnehmer:

- **Der Auftragnehmer stellt dem Auftraggeber die Technologie opentrack zum User-Tracking auf eigenen Websites zur Verfügung.**
- **In diesem Zusammenhang unterstützt der Auftragnehmer beim Entladen, Transformieren und Bereitstellen (ETL) der Daten.**
- **Betrieb und Hosting der Technologie opentrack**

3. Kategorien betroffener Personen (Definition Art. 4 Nr. 1 DSGVO)

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Besucher
- Bewerber
- Beschäftigte
- Kunden
- Mitarbeiter
- Dritte
- Abonnenten
- Ansprechpartner
- Handelsvertreter
- Interessenten
- Lieferanten

4. Verarbeitung innerhalb EU/ EWR oder Drittland mit angemessenem Schutzniveau

Jede Übermittlung von personenbezogenen Daten in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

§ 3 Technisch-organisatorische Maßnahmen

1. Der Auftragnehme**r** hat die Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber vorab bekannt zu machen. Der Auftraggeber trägt die Verantwortung dafür, dass die Maßnahmen für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Zu den vereinbarten technischen und organisatorischen Maßnahmen, siehe Anlage 1.

2. Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der 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 unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen (siehe auch Anlage 1).

3. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Für die auftragsgemäße Verarbeitung personenbezogener Daten wird eine geeignete Methodik zur Risikobewertung nach Wahl des Auftragnehmers verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt.

5. Der Auftragnehmer verpflichtet sich die getroffenen technischen und organisatorischen Maßnahmen (siehe Anlage 1) gegenüber dem Auftraggeber im Rahmen von dessen Kontrollbefugnissen nach § 7 dieses Vertrages nachzuweisen.

§ 4 Betroffenenrechte; Berichtigung, Einschränkung und Löschung von Daten

1. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird dieser das Ersuchen unverzüglich an den Auftraggeber weiterleiten.

2. Soweit vom Leistungsumfang umfasst, sind Auskunft, Löschung bzw. „Vergessenwerden“, Berichtigung und Datenportabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

3. Der Auftraggeber trägt die hierdurch beim Auftragnehmer entstehenden Mehrkosten.

§ 5 sonstige Pflichten des Auftragnehmers, insbesondere Qualitätssicherung

1. Der Auftragnehmer verpflichtet sich, die gesetzlichen Pflichten gemäß der Art. 28 bis 33 DSGVO einzuhalten, insbesondere jedoch zur Einhaltung folgender Vorgaben:

Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr/Frau
Andre Karjoth
Lohkoppelstrasse 20B
22083 Hamburg
bestellt.

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

2. Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO:

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften bekannt sind; er setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.

Bei den eingesetzten Beschäftigten handelt es sich daher ausschließlich um Berufsgeheimnisträger oder solche, die aufgrund gesetzlicher oder vertraglicher Verpflichtungen die bestehenden Schweige- und Geheimhaltungspflichten wahren.

Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind (z.B. durch Herausgabeverlangen von Ermittlungsbehörden).

3. Auf Anfrage arbeiten sowohl der Auftraggeber als auch der Auftragnehmer mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

4. Der Auftraggeber ist unverzügliche über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde zu informieren, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
5. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer bestmöglich zu unterstützen.

Die hierdurch bei dem Auftragnehmer entstehenden Kosten sind vom Auftraggeber zu tragen.

6. Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.

7. Der Auftragnehmer hat die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber sicherzustellen.

§ 6 Unterauftragsverhältnisse mit Subunternehmern

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

§ 7 Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

§ 8 Mitteilung bei Datenschutzverletzungen

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherigen Konsultationen der Aufsichtsbehörde. U.a. zählen hierzu

- Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.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

- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

- die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

- Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

§ 9 Weisungen des Auftraggebers

1. Weisungen oder Hinweise des Auftraggebers an den Auftragnehmer sind an einen der in Anhang 3 genannten berechtigten Kontaktpersonen zu richten. Jede Partei kann die genannten berechtigten Personen durch Erklärung in Schrift- oder Textform (im einfachen elektronischen Format) gegenüber der anderen Partei ändern.

2. Der Auftraggeber erteilt alle Einzelanweisungen möglichst in Text- oder Schriftform. Mündlich ergangene Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

3. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn eine Weisung möglicherweise gegen Datenschutzvorschriften oder gegen Regelungen dieses Vertrages verstößt. In diesem Fall ist der Auftragnehmer berechtigt, die Durchführung der entsprechenden Weisungen solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

§ 10 Löschung und Rückgabe von personenbezogenen Daten

1. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, und gesetzliche Aufbewahrungsfristen bleiben hiervon unberührt.

2. Nach Abschluss der vertraglich vereinbarten Leistungserbringung oder zuvor nach Aufforderung durch den Auftraggeber – spätestens jedoch mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Ein Löschprotokoll ist anzulegen und nach Aufforderung dem Auftraggeber vorzulegen.

3. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 11 Haftung und Vertragsstrafe

Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der Regelungen gemäß Art. 82 DSGVO. Der Auftragnehmer haftet dabei gemäß Art. 82 Abs. 2 S. 2 DSGVO nur für den durch die Verarbeitung verursachten Schaden, wenn er seinen speziell als Auftragsverarbeiter auferlegten Pflichte nicht nachgekommen ist, oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.

Bei Verstößen gegen diese Vereinbarung, insbesondere zur Einhaltung des Datenschutzes, verpflichtet sich der Auftragnehmer dem Auftraggeber eine Vertragsstrafe in Höhe von 4 % der letzten Monatsrate (lt. Leistungsvereinbarung) zu zahlen.

§ 12 Schlussbestimmungen

1. Ergänzungen und Änderungen dieser Anlage und des Leistungsvertrages bedürfen der

Schriftform oder Textform im einfachen elektronischen Format i.S.v. Art. 28 Abs. 9 DSGVO. Dies gilt auch für einen etwaigen Verzicht auf dieses Formerfordernis.

2. Sollte eine Bestimmung dieser Anlage oder des Leistungsvertrages unwirksam oder undurchführbar sein, so lässt dies die Wirksamkeit der anderen Bestimmungen unberührt. Die Parteien verpflichten sich in einem solchen Fall die unwirksame Bestimmung durch eine andere rechtswirksame zu ersetzen, die den Zweck der weggefallenen Bestimmung erfüllt.

3. Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter, etwa durch Pfändung, durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich und vor Eintritt dieser Maßnahmen zu informieren.

4. Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

5. Bei inhaltlichen Widersprüchen zwischen dieser Anlage und dem Leistungsvertrag haben die Regelungen dieser Anlage Vorrang.

6. Die Anhänge sind Bestandteil dieser Anlage und damit auch Bestandteile des Leistungsvertrages:

- Anhang 1: Checkliste Technische und Organisatorische Maßnahmen
- Anhang 2: Genehmigte Subunternehmer des Auftragnehmers
- Anhang 3: Berechtigte Kontaktpersonen

_____, den _____ Hamburg, den _____

SHEROES UG, Überseeboulevard 2, 20457 Hamburg

_____ _____

Auftraggeber Auftragnehmer

Anlage 1

Checkliste Technische und Organisatorische Maßnahmen (TOM)

Zur Gewährleistung des Auftragnehmers zur gesetzesmäßigen Verarbeitung von personenbezogenen Daten im Auftrag, werden folgende technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO eingehalten:

1. Vertraulichkeit

Zutrittskontrolle (z.B. für Gebäude und Räume, aber auch Schränke)

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

Das Hosting erfolgt über Hetzner Online GmbH, Gunzenhausen.
Die Server befinden sich in den Datacenterparks Nürnberg und Falkenstein

x elektronisches Zutrittskontrollsystem mit Protokollierung
x Hochsicherheitszaun um den gesamten Datacenterpark
x dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation- Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
x Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
x 24/7 personelle Besetzung der Rechenzentren
x Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräume
x Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt
x beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters •

Verwaltung
x elektronisches Zutrittskontrollsystem mit Protokollierung
x Videoüberwachung an den Ein- und Ausgängen

Zugangskontrolle (keine unbefugte Systembenutzung, z.B. unerlaubtes Hochfahren oder unbefugte Anmeldung in Systemen)

Mindestmaßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert wird:

X Passwortmechanismus (sichere Passwörter)
X Automatisches Sperren des Computers/ Abmeldung des Benutzers bei längerem Nicht-Gebrauch/ Abwesenheit des Mitarbeiters vom Arbeitsplatz
□ Zwei-Faktor-Authentifizierung im System
X Einsatz von Virenschutz-Software auf dem Arbeitsplatzsystem
X Verwendung einer zentralen und individuell konfigurierten Firewall
X Regelmäßige, professionell durchgeführt Updates von Software
□ Nach Stand der Technik sichere Verschlüsselung von Datenträgern mit anerkanntem Verschlüsselungsverfahren.
X Verzicht auf freigegebene externe Steckplätze (USB etc.) oder Laufwerke, wo diese nicht zwingend benötigt werden.

Zugriffskontrolle (Anwendungen ausführen, unerlaubte Tätigkeiten in IT-Systemen und Zugriffe auf Daten, Applikationen und Schnittstellen verhindern)

Mindestmaßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt, gelesen, kopiert, verändert oder entfernt werden können:

- x Differenzierte Berechtigungen der Benutzer für das Lesen/ Kopieren/ Verändern/ Löschen von Daten mittels bedarfsorientiertem Berechtigungskonzept (Datenträger- und Speicherkontrolle)
- x Differenzierte Berechtigungen für die Nutzung von Anwendungen und Betriebssysteme
- x Rechteverwaltung zentral durch Systemadministrator(-en), Anzahl dieser auf das Notwendige reduziert
- x Regelmäßige Überprüfung und Aktualisierung der Berechtigungen einschließlich Sperrung von z.B. ausgeschiedenen Mitarbeitern
- x Zugriffsprotokollierung und Auswertung mindestens jährlich findet statt
- x Überprüfung und Dokumentation, an welche Stellen personenbezogene Daten übermittelt wurden (Übertragungskontrolle)
- □ Verfahren zur Erkennung ungewünschter Datenabflüsse
- x Inventarisierung, sichere Aufbewahrung und Kontrolle der Datenträger
- x Vollständige und ordnungsgemäße Löschung/ Vernichtung von Datenträgern vor einer anderweitigen Verwendung oder Weitergabe (Hetzner Online GmbH)
- x Einsatz von Aktenvernichtern einer angemessen hohen Sicherheitsstufe oder Einsatz eines zertifizierten Dienstleisters, einschließlich Protokollierung der Vernichtung und wenigstens stichprobenartiger Kontrollen.
- x Verbot von BYOD oder restriktive, sichere Bring-Your-Own-Device-Regelungen
- x Sorgfältige Auswahl von Auftragsverarbeitern (auch Unterauftragnehmer) nach festgelegten, geeigneten Kriterien unter Abschluss der Auftragsvereinbarungen; einschließlich einer Kontrolle der Unterauftragnehmer

Trennungskontrolle

Mindestmaßnahmen, die gewährleisten, dass personenbezogene Daten, die zu unterschiedlichen Zwecken und für verschiedene Auftraggeber erhobene Daten wurden, getrennt verarbeitet werden:

- x Logische Speicherung der Daten nach Kunden/ Zwecken separiert auf Datenbanksystem mit Kundenzugriff.
- x Verarbeitung von Test und Produktionsdaten in getrennten Systemen (Sandbox)

Pseudonymisierung

Eine Pseudonymisierung obliegt dem Auftraggeber.

2. Integrität

Weitergabekontrolle

Mindestmaßnahmen, die gewährleisten, dass personenbezogene Date bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

x Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.

x Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.
X Verschlüsselte Übertragung auf Kundensysteme nach Stand der Technik
X Abruf von Daten durch Kunden mittels Passwort gesicherten Zugriff
□ Legitimationskonzept für Empfänger
X Dokumentation der Übertragungswege
□ VPN, VPN-Tunnel
□ Weitergabe von Daten nur in anonymisierter (nur hilfsweise in anonymisierter) Form
X Monitoring und Log-Management
X Keine oder stark eingeschränkte Nutzung von mobilen Datenträgern außerhalb des Unternehmens

Eingabekontrolle (Nachvollziehbarkeit, Dokumentation)

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

X Protokolle zur Überprüfung und Dokumentation, wann von wem auf welche personenbezogenen Daten zugegriffen wurde, so dass diese eingegeben oder verändert worden sind
X Berechtigungsregelungen
X Dokumentenmanagment

3. Verfügbarkeit

Verfügbarkeitskontrolle

Mindestmaßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust, gegen technische Störungen durch das Versagen der Betriebs-/Anwendungssoftware, vor fahrlässigen/vorsätzlichen Handlungen, vor schadenstiftender Software geschützt sind:

X regelmäßige Sicherheitskopien, Backup-Konzept
□ Wiederherstellungskonzept (Recovery) einschließlich regelmäßiger Tests
X Logische Trennungen von Daten
X Unabhängig voneinander funktionierende Systeme, einschließlich redundanter Server
X Unterbrechungsfreie Stromversorgung zu gewährleisten
X Automatisierte Meldungen bei Fehlern
X Überwachungsgeräte im Serverraum (Temperatur und Luftfeuchtigkeit)
X Feuer- und Rauchmelder sowie Feuerlöscher in allen relevanten Räumen
x Dauerhaft aktiver DDoS-Schutz.

4. Kontrolle (Sonstige, Überprüfung, Bewertung und Evaluierung)

Mindestmaßnahmen, die sicherstellen, dass die Maßnahmen geeignet sind, die Sicherheit zu gewährleisten und den Belastungen standhalten, möglichst mit festen Mindestzeitintervallen

x IT-Sicherheits-Richtlinie vorhanden.
□ Einhaltung von anerkannten Standards, ggf. konkret: _____
x Regelmäßige Überprüfungen, dass personenbezogene Daten, die im (Unter-) Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden (können) (Auftragskontrolle)
□ Vorhandene Revision mit regelmäßiger Auswertung und Überprüfung
□ Umfassende Gefahrenanalyse findet statt, ggf. konkret:
_____
□ Bewertung der Systeme durch regelmäßige Audits
x Belastungstests (Penetrationstests) erfolgen regelmäßig
x Regelmäßige, risikobezogene Anpassungen und Erneuerungen der Maßnahmen
□ Notfallplan zur Wiederherstellung der personenbezogenen Daten verarbeiteten IT-Systeme

_____, den _____

_____
Auftragnehmer

Anlage 2

Genehmigte Subunternehmer des Auftragsnehmers

Subunternehmer Firma	Anschrift; Land	Leistung
Hetzner Online GmbH	Gunzenhausen, DE	Hosting der Server

Hamburg, den _____

SHEROES UG, Überseeboulevard 2, 20457 Hamburg

_____
Auftragnehmer

Anhang 3

Berechtigte Kontaktpersonen

Weisungsberechtigte Personen des Auftraggebers:

1.
Name:
Abteilung/ Organisationseinheit:
E-Mail:
Telefon:

2. (Vertreter)
Name:
Abteilung/ Organisationseinheit:
E-Mail:
Telefon:

Weisungsberechtigte Empfänger des Auftragnehmers:

1.
Name: Nicolas Danner
Abteilung/ Organisationseinheit: Geschäftsführung
E-Mail: nicolas.danner@sheroes.de
Telefon: 0151 – 700 240 25

_____, den _____

_____
Auftraggeber

Hamburg, den _____

SHEROES UG, Überseeboulevard 2, 20457 Hamburg

_____
Auftragnehmer