Datenschutzvereinbarung
zur Verarbeitung personenbezogener Daten
im Auftrag

gemäß Art. 28 DS-GVO

zwischen dem Verantwortlichen:

_____

_____

_____
*(nachstehend **Auftraggeber** genannt)*

und dem Auftragsverarbeiter:

strait GmbH
48691 Vreden
Stadtlohner Strasse 23 – 25
Tel.: 02564-82950
Fax: 02564-8295200
info@strait.de
www.strait.de
*(nachstehend **Auftragnehmer** genannt)*

Bitte diesen Vertrag ausfüllen

- Seite 1: Auftraggeber
- Seite 3+4: §3 Auftragsumfang

Und unterschrieben an uns zurückübermitteln.

Präambel

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der in dieser Vereinbarung und der in **§3** beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit der Dienstleistung in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

Den Parteien ist bekannt, dass ab dem 25.05.2018 die EU Datenschutz-Grundverordnung (DS-GVO: EU-Verordnung 2016/679) gilt und sich die Vorgaben der Auftragsverarbeitung grundsätzlich nach Art. 28 DS-GVO richten.

Einzelvereinbarungen in dieser Datenschutzvereinbarung gehen den Allgemeinen Geschäftsbedingungen (AGB) des Auftragnehmers vor.

§ 1 Definitionen

1. **Personenbezogene Daten**
   Nach Art. 4 Abs. 1 DS-GVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden **"betroffene Person"**) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

2. **Auftragsverarbeiter**
   Nach Art. 4 Abs. 8 DS-GVO ist ein **Auftragsverarbeiter** eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

3. **Weisung**
   Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Speicherung, Pseudonymisierung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete, in der Regel schriftliche Anordnung des Auftraggebers. Die Weisungen werden vom Auftraggeber erteilt und können durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Die Weisungen des Auftraggebers sind schriftlich oder per E-Mail zu erteilen.

§ 2 Anwendungsbereich und Verantwortlichkeit

1. Der Auftragnehmer verarbeitet im Auftrag des Auftraggebers personenbezogene Daten oder es kann im Zusammenhang mit der Dienstleistungserbringung nicht ausgeschlossen werden, dass der Auftragnehmer Zugriff auf personenbezogenen Daten bekommt bzw. Kenntnis von diesen

erlangt. Nach Art 28 DS-GVO ist daher der Abschluss einer Vereinbarung zur Verarbeitung im Auftrag erforderlich.

2. Der Auftraggeber hat den Auftragnehmer im Rahmen der Sorgfaltspflichten des Art. 28 DS-GVO als Dienstleister ausgewählt. Voraussetzung für die Zulässigkeit einer Datenverarbeitung im Auftrag ist, dass der Auftraggeber dem Auftragnehmer den Auftrag schriftlich bzw. auch elektronisch erteilt. Dieser Vertrag enthält nach dem Willen der Parteien und insbesondere des Auftraggebers den Auftrag zur Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 DS-GVO und regelt die Rechte und Pflichten der Parteien zum Datenschutz im Zusammenhang mit der Erbringung der Dienstleistung.

3. Das Eigentum an den personenbezogenen Daten liegt ausschließlich beim Auftraggeber als „Verantwortlichem" im Sinne der DS-GVO. Aufgrund dieser Verantwortlichkeit kann der Auftraggeber auch während der Laufzeit des Vertrages und nach Beendigung des Vertrages die Berichtigung, Löschung, Sperrung und Herausgabe von personenbezogenen Daten verlangen.

§ 3 Gegenstand und Dauer des Auftrages

1. Der Gegenstand des Auftrages ist wie folgt definiert:

Bitte kreuzen Sie die Datenbereiche an.
Bitte berücksichtigen Sie hierbei die Tatsache, dass z.B. in Shops Plugins zur Zahlungsabwicklung genutzt werden, deren Daten technisch direkt zwischen der Website/Shop und dem Plugin-Anbieter ausgetauscht und von uns weder verarbeitet noch gespeichert werden.

- ☒ Protokolldaten (z. B. Logfiles über Nutzungsvorgänge für statistische Auswertungen)
- ☐ Emailtransport
- ☐ CMS-Nutzerdaten (Name, Anschrift, Telefon, E-Mail)
- ☐ Verbindungsdaten (Datum und Zeit der Verbindung, Verbindungsteilnehmer)
- ☐ Abrechnungsdaten (z. B. Verbrauchs- und Leistungswerte)
- ☐ Arbeitszeitdaten (Arbeits- und Fehlzeiten, Soll-Arbeitszeit, Pausen, Urlaub, Sonderurlaub, Krankheitstage, Überstunden)
- ☐ Bewerberdaten (Angaben zur Person, Kontaktdaten, Lebenslauf, Foto, Zeugnisse)
- ☐ Biometrische Daten (Biometrische Angaben zur betroffenen Person wie z. B. Fingerabdruck, Stimme, Gesichtsmerkmale)
- ☐ Bonitätsdaten (Scoringwerte, Zahlungshistorie)
- ☐ Fahrzeugdaten (z. B. Halter-, Fahrer-, GPS-Daten)
- ☐ Gehaltsdaten (Entgelt, Bonus und Prämien, steuerliche Angaben, Zuschläge)
- ☐ Genetischen Daten (Informationen über Genomdaten der betroffenen Person)
- ☐ Gesundheitsdaten (z. B. Krankmeldungen, Patientendaten)
- ☐ Internetnutzungsdaten (IP-Adresse, Besuchszeit und Datum)
- ☐ Kontaktdaten (Name, Telefon, Fax, E-Mail)
- ☐ Kundendaten (Kundennummer, Firma, Ansprechpartner, Anschrift, Webseite, Kommunikationsdaten)

☐ Mitarbeiterdaten (Personalstammdaten, Kontaktdaten, Notfalldaten)

☐ Schadensdaten (Angaben zur Person, Kontaktdaten, Schadensverlauf, Unfallbericht, Zeugen)

☐ Verhaltensdaten (z. B. Verhaltensbeobachtungen, Bewegungsprofil)

☐ Versicherungsdaten (Angaben zur Person, Kontaktdaten, Vertragsdaten, Gesundheitsangaben, Kontoverbindungen)

☐ Vertragsdaten (Anschrift, Kontaktdaten, Vertragsinhalte)

☐ Zahlungsdaten (Kontoinformationen, Kreditkartendaten)

2. Diese Vereinbarung tritt mit ihrer Unterzeichnung durch beide Parteien in Kraft und endet im Regelfall mit Kündigung des zugrundeliegenden Hauptvertrages laut AGB. Das Recht zur außerordentlichen Kündigung bleibt unberührt.

§ 4 Beschreibung der Verarbeitung, Daten und betroffener Personen

Umfang, Art und Zweck der Verarbeitung sind ebenso wie die Art der Daten und der Kreis der betroffenen Personen in §3 beschrieben.

§ 5 Technische und organisatorische Maßnahmen

Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Wahrung der anzuwendenden Datenschutzvorschriften angemessen und erforderlich sind.

1. Da der Auftragnehmer die Dienstleistungen für den Auftraggeber auch außerhalb der Geschäftsräume des Auftraggebers durchführt, sind vom Auftragnehmer zwingend die von ihm getroffenen technischen und organisatorischen Maßnahmen i.S.d. Art. 28 Abs. 3 lit. C DS-GVO, Art. 32 DS-GVO i.V.m. Art. 5 Abs. 1 und Abs. 2 DS-GVO hierzu zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben.
2. Die Maßnahmen dienen der Datensicherheit und der Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der mit diesem Auftrag in Zusammenhang stehenden 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 DS-GVO zu berücksichtigen.
3. Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 1 „Technische und organisatorische Maßnahmen zum Datenschutz“** dieser Vereinbarung beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Vorwege mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können

vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

§ 6 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 der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber zur Erledigung durch diesen weiterleiten.
2. Die Umsetzung der Rechte auf Löschung, Berichtigung, Datenübertragbarkeit und Auskunft sind nur nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.
3. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten oder aufgrund gerichtlicher oder behördlicher Anordnung erforderlich sind.
4. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens jedoch mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer dem Auftraggeber die Möglichkeit zum Zugriff und zur Sicherung sämtlicher in seinen Besitz gelangter Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, einzuräumen. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
5. 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.

§ 7 Pflichten des Auftragnehmers

1. Eine Verarbeitung personenbezogener Daten, die sich nicht auf die Erbringung der beauftragten Leistung bezieht, ist dem Auftragnehmer untersagt. Es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.
2. Der Auftragnehmer bestätigt, dass er – soweit dieser gesetzlich dazu verpflichtet ist – einen betrieblichen Datenschutzbeauftragten i.S.d. Art. 38, 39 DS-GVO bestellt hat. Nähere Angaben hierzu werden vom Auftragnehmer in **Anlage 1 „Technische und organisatorische Maßnahmen zum Datenschutz“** gemacht.
3. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

4. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten des Auftraggebers.
5. Für den Fall, dass der Auftragnehmer feststellt oder Tatsachen die Annahme begründen, dass von ihm für den Auftraggeber verarbeitete personenbezogene Daten einer Verletzung des gesetzlichen Schutzes personenbezogener Daten gem. Art. 33 DS-GVO (Datenschutzverstoß bzw. Datenpanne) unterliegen, z.B. indem diese unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalls bzw. der Vorfälle in Schriftform oder Textform (Fax/E-Mail) zu informieren. Die Meldung an den Auftraggeber muss mindestens folgende Informationen enthalten:

    a. Eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze.
    b. Den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen.
    c. Eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten.
    d. Eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

   Der Auftragnehmer ist darüber hinaus verpflichtet, unverzüglich mitzuteilen, welche Maßnahmen durch den Auftragnehmer getroffen wurden, um die unrechtmäßige Übermittlung bzw. unbefugte Kenntnisnahme durch Dritte künftig zu verhindern.
6. Der Auftragnehmer stellt auf Anforderung dem Auftraggeber die für das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DS-GVO notwendigen Angaben zur Verfügung und führt als Auftragsverarbeiter selbst ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DS-GVO.
7. Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der personenbezogenen Daten des Auftraggebers befassten Mitarbeiter gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO zur Wahrung der Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen des Datenschutzes vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugriff auf personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in dieser Vereinbarung eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Diese Vertraulichkeitsverpflichtung besteht auch nach Beendigung der Tätigkeit fort.
8. Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren und in geeigneter Weise nachzuweisen.
9. Des Weiteren verpflichtet sich der Auftragnehmer den Auftraggeber gemäß Art. 28 Abs. 3 lit. f DS-GVO bei der Einhaltung der in Art. 34 - 36 DS-GVO genannten Pflichten zu unterstützen:

a. Im Rahmen seiner Informationspflicht gegenüber den betroffenen Personen und dem Auftraggeber in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.
b. Bei der Durchführung seiner Datenschutz-Folgenabschätzung.
c. Im Rahmen einer vorherigen Konsultation mit der Aufsichtsbehörde.

10. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
11. Der Auftragnehmer hat den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen, zu informieren. 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. Eine Information erfolgt nicht, soweit dies gerichtlich oder behördlich untersagt ist.
12. 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 durch den Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
13. 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 Person gewährleistet wird.

§ 8 Rechte und Pflichten des Auftraggebers

1. Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren Auftragsverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen können

   a. schriftlich
   b. per Fax
   c. per E-Mail
   d. mündlich

   erfolgen. Der Auftraggeber soll mündliche Weisungen unverzüglich in Textform (z.B. Fax oder E-Mail) gegenüber dem Auftragnehmer bestätigen.
2. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
3. Dem Auftraggeber obliegen die aus Art. 33 Abs. 1 DS-GVO resultierenden Meldepflichten.
4. Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten personenbezogenen Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest.
5. Erteilt der Auftraggeber Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten vom Auftraggeber zu tragen.

§ 9 Wahrung von Rechten der betroffenen Person

1. Der Auftraggeber ist für die Wahrung der Rechte der betroffenen Person verantwortlich.
2. Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Einschränkung, Datenübertragbarkeit oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen.
3. Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer zwecks Berichtigung, Löschung oder Einschränkung oder Datenübertragbarkeit seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
4. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

§ 10 Kontrollbefugnisse

1. Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen sowie die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.
2. Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Abs. 1 erforderlich ist.
3. Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Abs. 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, sofern die Betriebsabläufe des Auftragnehmers durch die Kontrollen gestört werden.
4. Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DS-GVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen.
5. Der Auftragnehmer erbringt den Nachweis technischer und organisatorischer Maßnahmen, die nicht nur den konkreten Auftrag betreffen. Dabei kann dies erfolgen durch:

    a. die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO.
    b. die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO.
    c. aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsbeauftragter, Datenschutzauditoren.
    d. eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach ISO 27001).

§ 11 Unterauftragsverhältnisse

1. Der Auftragnehmer nimmt für die Verarbeitung personenbezogener Daten im Auftrag des Auftraggebers keine Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten gem. Art. 28 DS-GVO verarbeiten („Unterauftragnehmer“).
2. Die bedarfsweise Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist nur mit schriftlicher Zustimmung des Auftraggebers zulässig.
3. Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen Unternehmen zur Leistungserfüllung heranzieht bzw. mit Leistungen unterbeauftragt. Die zum Zeitpunkt des Abschlusses dieser Vereinbarung eingesetzten Unterauftragnehmer werden in **Anlage 1 „Technische und organisatorische Maßnahmen zum Datenschutz“** dokumentiert.
4. Im Falle einer Beauftragung hat der Auftragnehmer den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 28 Abs. 3 lit. c, 32 DS-GVO i.V.m. Art. 5 Abs. 1, Abs. 2 DS-GVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln. Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten i.S.d. Art. 37-39 DS-GVO bestellt hat, sofern die gesetzliche Pflicht zur Benennung eines Datenschutzbeauftragten besteht.
5. Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten. Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.
6. Die Verpflichtung des Unterauftragnehmers muss schriftlich erfolgen. Dem Auftraggeber ist die schriftliche Verpflichtung auf Anfrage in Kopie zu übermitteln.
7. Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 10 dieser Vereinbarung) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

§ 12 Datengeheimnis und Geheimhaltungspflichten

1. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.
2. Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist.
3. Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieser Vereinbarung erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den oben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

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

§ 13 Haftung

1. Es wird auf die Haftungsregelungen des Art. 82 DS-GVO verwiesen.
2. Weiterhin wird vereinbart, dass der Auftragnehmer verpflichtet ist, dem Auftraggeber sämtliche Schäden und Aufwendungen zu ersetzen, die dem Auftraggeber als Folge einer Verletzung einer Verpflichtung nach dieser Vereinbarung einschließlich seiner Anhänge durch den Auftragnehmer, seinen gesetzlichen Vertreter, Unterauftragnehmer, Mitarbeiter oder sonstigen Erfüllungsgehilfen entstehen.

§ 14 Informationspflichten, Schriftformklausel, Rechtswahl

1. Sollten die personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den personenbezogenen Daten ausschließlich beim Auftraggeber als „Verantwortlichem" im Sinne der DS-GVO liegen.
2. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
3. Bei Unwirksamkeit einer Bestimmung in diesen Vertragsbedingungen bleiben die übrigen Bestimmungen gleichwohl wirksam. Die Vertragsparteien verpflichten sich, eine unwirksame Bestimmung oder eine planwidrig fehlende Bestimmung nach Treu und Glauben durch eine Bestimmung zu ersetzen, die dem gemeinsam verfolgten Zweck der Vertragsparteien am nächsten kommt.

_____, ____.____.2018

Vreden,16.05.2018

C. Küpers

_____

strait GmbH, Christian Küpers, CEO

_____

Anlage 1

Technische und organisatorische Schutzmaßnahmen

1. Organisationskontrolle

Folgende Maßnahmen sind betroffen:

Es gibt Regelungen über

☒ Zutrittsberechtigungen
☒ Zugangsberechtigungen
☒ Zugriffsberechtigungen
☒ Datenübertragung
☒ Verpflichtung der Mitarbeiter auf das Datengeheimnis (§ 5 BDSG)
☒ Einhaltung der Grundsätze zur Funktionstrennung und klare Verantwortungsbereiche

Anweisung und Richtlinien zur Anwendungsentwicklung und Produktion

☒ Entwicklungs-, Ergebnis- und Systemdokumentation
☒ Trennung von Test und Produktion
☒ Regelungen zu Test und Freigabe
☒ Datensicherungskonzept, -plan, -katalog
☒ Dokumentation von IT-Verfahren, Software, IT-Konfiguration
☒ Notfallkonzept

2. Zutrittskontrolle

Folgende Maßnahmen sind betroffen:

☒ Festlegung zutrittsberechtigter Personen
☒ Berechtigungsausweise
☒ Sicherheitsschlösser mit Schlüsselverwaltung und Schließplan
☒ Besucherausweise (für das RZ)
☒ Anwesenheitsaufzeichnungen (An-/Abwesenheitsliste, Besucherbuch, Zeiterfassungseinrichtungen) (für das RZ)
☒ Schaffung von Sicherheitsbereichen und Beschränkung der Zutrittswege (Zutrittskontrollsystem, Verschließung der Räume) (für das RZ)
☒ bauliche Maßnahmen: Gebäudesicherung z. B. durch Einzäunung und Überwachungskameras (für das RZ)
☒ Sicherung durch Alarmanlagen, durch Werksschutz, Wachdienst/-Hund, Einbruchsmelder, Pforte, elektrische Türöffner, Sicherung von Lichtschächten, Spezialverglasung (für das RZ; teilweise für Verwaltung)
☒ gesicherter Eingang für An- und Ablieferung (für das RZ)

3. Zugangskontrolle

Folgende Maßnahmen sind betroffen:

☒ Regelung von Zugangsberechtigungen
☒ Einhaltung der Funktionstrennung bei Vergabe von Zugangsberechtigungen
☒ Sperrung von Zugangsberechtigungen bei längerer Abwesenheit von Benutzern
☒ Abschottung interner Netzwerke gegen ungewollte Zugriffe von draußen (Firewall)
☒ Absicherung der Übertragungsleitungen

4. Zugriffskontrolle

Folgende Maßnahmen sind betroffen:

☒ geregeltes Verfahren über Vergabe, Änderung und Entzug von Zugriffsberechtigungen
☒ Einsatz von Benutzercodes (Passwörtern) für Dateien und System-, Anwendungs- und Dienstprogramme
☒ Passwortregeln bei Konfiguration der IT-Systeme umgesetzt
☒ Beschränkung des Einsatzes freier Abfragemöglichkeiten (SQL-Query) von Datenbanken

5. Weitergabekontrolle

Folgende Maßnahmen sind betroffen:

☒ Auswertungsmöglichkeiten der Übermittlungsprotokolle, um die Empfänger oder Abrufenden gezielt feststellen zu können
☒ gesicherte Datenleitungen
☒ Lokal/Remote, Stand- oder Wählleitung
☒ Fernwartungskonzept
☒ Einsatz kryptographischer Verfahren

6. Eingabekontrolle

Folgende Maßnahmen sind betroffen:

☒ Protokolldateien sind IT-gestützt auswertbar

7. Auftragskontrolle

Folgende Maßnahmen sind betroffen:

☒ sorgfältige Auswahl der Auftragnehmer
☒ Formalisierung der Auftragsverarbeitung
☒ Kontrolle der Arbeitsergebnisse

8. Verfügbarkeitskontrolle

Folgende Maßnahmen sind betroffen:

☒ Funktionstrennung zwischen Fachabteilung und DV-Abteilung
☒ zentrale Beschaffung von Hard- und Software
☒ Erstellen eines Notfallhandbuchs
☒ regelmäßige Durchführung von Datensicherungen
☒ Lagerung der Sicherungskopien an geschützten Orten außerhalb des Rechenzentrums
☒ Brandschutzmaßnahmen

☒ Feuer-/Wasser-Frühwarnsystem
☒ unterbrechungsfreie Stromversorgung (USV)
☒ Recovery-Verfahren
☒ Datenspiegelung (Parallelbetrieb sofern beauftragt)

9. Trennungskontrolle

Folgende Maßnahmen sind betroffen:

☒ logische Trennung der Daten
☒ Benutzerprofile
☒ Berechtigungen