# Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

**Vereinbarung**

zwischen der

Freiheit Gruppe GmbH.

- Verantwortlicher - nachstehend Auftraggeber genannt - und der

Björn Knetter

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

## Gegenstand und Dauer des Auftrags

1. Gegenstand

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:   
Programmierung von Webseiten plus Content Management System Morpheus.  
Mailings.

1. Dauer

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien jederzeit gekündigt werden.

## Konkretisierung des Auftragsinhalts

1. Art und Zweck der vorgesehenen Verarbeitung von Daten

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:  
Programmierung von Webseiten plus Content Management System Morpheus.   
Mailings versenden. Mailings aufbauen.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mit- gliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zu- stimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau in wird hergestellt durch sonstige Maßnahmen die Löschung der Daten nach Versand.

Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/- kategorien (Aufzählung/Beschreibung der Datenkategorien)

* + - Personalstammdaten.

1. Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

* + Kunden
  + Interessenten

## Technisch-organisatorische Maßnahmen

1. Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und er- forderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbeson- dere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnah- men Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbe- darf ergibt, ist dieser einvernehmlich umzusetzen.
2. Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Ver- bindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffen- den 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 Eintrittswahrschein- lichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].
3. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maß- nahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unter- schritten werden. Wesentliche Änderungen sind zu dokumentieren.

## Berichtigung, Einschränkung und Löschung von Daten

1. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig son- dern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbei- tung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftrag- nehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiter- leiten.
2. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichti- gung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

## Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung fol- gender Vorgaben:

* 1. Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr Björn Knetter, Telefon: 0176 66855208, E-Mail: post@pixel-dusche.de benannt.
  2. Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer 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. Der Auftragnehmer und jede dem Auftragneh- mer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Da- ten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließ- lich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
  3. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].
  4. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
  5. Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maß- nahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Straf- verfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsver- arbeitung beim Auftragnehmer ermittelt.
  6. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ord- nungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auf- tragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
  7. 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. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen ge- genüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

## Unterauftragsverhältnisse

1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verste- hen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Ne- benleistungen, 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 Be- lastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftrag- nehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskon- forme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

1. Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Eine Unterbeauftragung ist unzulässig.

1. Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragneh- mer aufzuerlegen.

## Kontrollrechte des Auftraggebers

1. Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzu- führen 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.
2. 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 Umset- zung der technischen und organisatorischen Maßnahmen nachzuweisen.
3. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
4. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Ver- gütungsanspruch geltend machen.

## Mitteilung bei Verstößen des Auftragnehmers

1. 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 Da- tenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.
   1. 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 er- möglichen

* 1. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
  2. die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informa- tionen unverzüglich zur Verfügung zu stellen
  3. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
  4. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Auf- sichtsbehörde

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

## Weisungsbefugnis des Auftraggebers

1. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).
2. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durch- führung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

## Löschung und Rückgabe von personenbezogenen Daten

1. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Da- tenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Auf- bewahrungspflichten erforderlich sind.
2. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens 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. Das Protokoll der Löschung ist auf Anforderung 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 Auftrag- geber übergeben.

# Anlage – Technisch-organisatorische Maßnahmen

## Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

### Zutrittskontrolle

* + - Alarmanlage
    - Zugangskontrollsystem
    - Schließsystem mit Codesperre
    - Sicherheitsschlösser
    - Schlüsselregelung (Schlüsselausgabe etc.)
    - Sorgfältige Auswahl von Reinigungspersonal

### Zugangskontrolle

* + - Zuordnung von Benutzerrechten
    - Erstellen von Benutzerprofilen
    - Passwortvergabe
    - Authentifikation mit Benutzername / Passwort
    - Schlüsselregelung (Schlüsselausgabe etc.)
    - Sorgfältige Auswahl von Reinigungspersonal
    - Einsatz von Anti-Viren-Software
    - Einsatz einer Hardware-Firewall
    - Einsatz einer Software-Firewall bei allen mobilen Arbeitsplätzen

### Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Be- rechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;

* + - Erstellen eines Berechtigungskonzepts
    - Verwaltung der Rechte durch Systemadministrator
    - Anzahl der Administratoren auf das „Notwendigste“ reduziert
    - Protokollierung bei der Eingabe, Änderung und Löschung von Daten der Seitenverwaltung im CMS
    - Sichere Aufbewahrung von Datenträgern
    - physische Löschung von Datenträgern vor Wiederverwendung
    - ordnungsgemäße Vernichtung von Datenträgern

### Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;

* + Festlegung von Datenbankrechten
  + Trennung von Produktiv- und Testsystem, sofern vorhanden
* **Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)** Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuzie- hung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeord- net werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

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

### Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen insbesondere bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN),

* + - Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Über- lassung bzw. vereinbarter Löschfristen
    - Beim physischen Transport: sichere Transportbehälter/-verpackungen
    - Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und - fahrzeugen

### Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme ein- gegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanage- ment;

* + - Protokollierung der Eingabe, Änderung und Löschung von Daten
    - Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Da- ten eingegeben, geändert und gelöscht werden können.
    - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individu- elle Benutzernamen (nicht Benutzergruppen)
    - Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
    - Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

## Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

### Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (onli- ne/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Fire- wall, Meldewege und Notfallpläne; Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS- GVO);

Björn Knetter bietet diesen Service nicht an.

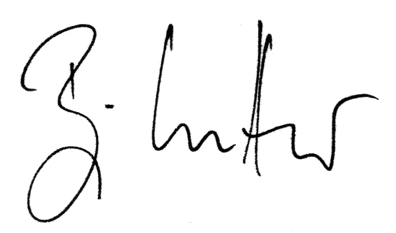
## Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

* + **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);**
  + **Auftragskontrolle**

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

* + - Löschbarkeit von Daten

Auftraggeber Auftragnehmer



09.05.2018 Frankfurt Main

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Datum, Ort, Unterschrift Datum, Ort, Unterschrift