



## ANLAGE 1

# Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 DSGVO

### Präambel

Diese Vereinbarung zur Auftragsverarbeitung (nachfolgend auch „Vereinbarung“) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der hierin sowie im Agenturvertrag in ihren Einzelheiten beschriebenen Auftragsdatenverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit der beauftragten Datenverarbeitung in Zusammenhang stehen und bei denen arvatis („Auftragnehmer“), dessen Mitarbeiter oder durch den Auftragnehmer beauftragte Dritte personenbezogenen Daten des Auftraggebers erheben, verarbeiten oder nutzen oder sonst auf personenbezogene Daten des Auftraggebers zugreifen können. Diese Vereinbarung regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung vorrangig vor allen sonstigen Vereinbarungen.

### 1. Gegenstand und Dauer des Auftrags

#### (1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus dem Agenturvertrag, auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

#### (2) Dauer

Diese Vereinbarung gilt mit Wirkung zum 25. Mai 2018 und ersetzt ab diesem Zeitpunkt alle zuvor ggf. zwischen den Parteien geschlossenen Vereinbarungen zur Auftragsverarbeitung. Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

### 2. Konkretisierung des Auftragsinhalts

#### (1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung.

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. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.

#### (2) Art der Daten

Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben.

#### (3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben.

### 3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO 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 DS-GVO zu berücksichtigen [Einzelheiten in Anhang 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. 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 weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

#### 5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

- a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt. Als Datenschutzbeauftragter ist beim Auftragnehmer Herr David Detjen, Tel: +49 (0)211 - 63 55 31 66, Mail: detjen@arvatis.com, bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
- b) Die Wahrung der Vertraulichkeit gemäß Artt. 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 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.
- c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anhang 1].
- d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, 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.
- f) 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 nach besten Kräften zu unterstützen. Dem Auftragnehmer steht dafür ein angemessenes Entgelt zu.
- g) 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.
- h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.



## 6. Unterauftragsverhältnisse

(1) 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.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) beauftragen und Wechsel der bestehenden Unterauftragnehmer vornehmen, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

Bereits mit Abschluss der Vereinbarung erteilt der Auftraggeber die Zustimmung für folgende Unterauftragnehmer:

- Neue Medien Münnich GmbH (NMM), Hauptstraße 68, D-02742 Friedersdorf (Domainverwaltung Hinterlegung von Auftraggeberdaten zur Domainregistrierung und Hosting von Shopware-Webshops sowie Wordpress-Redaktionssystemen)
- Domain Factory, Oskar-Messler-Strasse 33, 85737 Ismaning (Domainverwaltung Hinterlegung von Auftraggeberdaten zur Domainregistrierung)
- Host Europe GmbH, Welsersstraße 14, 51149 Köln (Domainverwaltung Hinterlegung von Auftraggeberdaten zur Domainregistrierung)
- Timme Hosting GmbH & Co. KG, Ovelgönner Weg 43, 21335 Lüneburg (Domainverwaltung und Hosting von Shopware-Webshops (Quellcode und Datenbanken) sowie Wordpress-Redaktionssystemen (Quellcode und Datenbanken) sowie Hosting von Tideways als Performance-Analysetool)
- 

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

## 7. Kontrollrechte des Auftraggebers

(1) 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.

(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 Umsetzung 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;



- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

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

## 8. 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 Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
- b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- c) 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
- d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
- e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Dem Auftragnehmer steht dafür ein angemessenes Entgelt zu.

## 9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung 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. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten 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. Dem Auftragnehmer steht dafür ein angemessenes Entgelt zu.

(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.

## 12. Haftung und Freistellung



- (1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer alleine der Auftraggeber gegenüber dem Betroffenen verantwortlich.
- (2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.
- (3) Die in der Leistungsvereinbarung vereinbarten Haftungsausschlüsse und Haftungsbegrenzungen finden auf alle Schadensersatz-, Aufwendungsersatz und Freistellungsansprüche aus oder im Zusammenhang mit diesem Vertrag Anwendung.

### 13. Sonstiges

- (1) Es gilt deutsches Recht.
- (2) Erfüllungsort und ausschließlicher Gerichtsstand ist Düsseldorf, Deutschland.
- (3) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. Anstelle der unwirksamen Bestimmung soll vielmehr eine solche wirksame Regelung gelten, die dem wirtschaftlichen Willen der Vertragsparteien bei Vertragsabschluss am nächsten kommt.
- (4) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf das Formerfordernis.



## ANLAGE 2

# Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die og. Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

### 1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

#### 1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

#### Technische Maßnahmen

1. Chipkarten / Transpondersysteme
2. Manuelles Schließsystem
3. Sicherheitsschlösser
4. Absicherung der Gebäudeschächte
5. Türen mit Knauf Außenseite
6. Klingelanlage mit Kamera

#### Organisatorische Maßnahmen

1. Schlüsselregelung / Liste
2. Besucher in Begleitung durch Mitarbeiter
3. Sorgfalt bei Auswahl Reinigungsdienste

#### 1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpassword, Benutzererkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

#### Technische Maßnahmen

1. Login mit Benutzername + Passwort
2. Firewall
3. Einsatz VPN bei Remote-Zugriffen



4. Verschlüsselung von Datenträgern
5. Verschlüsselung Smartphones
6. Automatische Desktopsperre
7. Verschlüsselung von Notebooks / Tablet

#### Organisatorische Maßnahmen

1. Verwalten von Benutzerberechtigungen
2. Erstellen von Benutzerprofilen
3. Richtlinie „Sicheres Passwort“
4. Richtlinie „Löschen / Vernichten“
5. Allg. Richtlinie Datenschutz und / oder Sicherheit
6. Anleitung „Manuelle Desktopsperre“

#### 1.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

#### Technische Maßnahmen

1. Aktenschredder (mind. Stufe 3, cross cut)

#### Organisatorische Maßnahmen

1. Minimale Anzahl an Administratoren

#### 1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

#### Technische Maßnahmen

1. Trennung von Produktiv- und Testumgebung
2. Mandantenfähigkeit relevanter Anwendungen

#### Organisatorische Maßnahmen

1. Steuerung über Berechtigungskonzept
2. Festlegung von Datenbankrechten



### 1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

#### Organisatorische Maßnahmen

1. Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

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

### 2.1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

#### Technische Maßnahmen

1. Einsatz von VPN
2. Protokollierung der Zugriffe und Abrufe
3. Bereitstellung über verschlüsselte Verbindungen wie sftp, https

#### Organisatorische Maßnahmen

1. Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen

### 2.2. 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. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

#### Technische Maßnahmen

1. Manuelle oder automatisierte Kontrolle der Protokolle

#### Organisatorische Maßnahmen

1. Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)



2. Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

### 3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

#### 3.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlage, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidssysteme, Plattenspiegelungen etc.

#### Technische Maßnahmen

1. Feuer- und Rauchmeldeanlagen
2. Serverraum klimatisiert
3. RAID System / Festplattenspiegelung

#### Organisatorische Maßnahmen

1. Backup & Recovery-Konzept (ausformuliert)
2. Keine sanitären Anschlüsse im oder oberhalb des Serverraums
3. Getrennte Partitionen für Betriebssysteme und Daten

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

#### 4.1. Datenschutz-Management

#### Organisatorische Maßnahmen

1. Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
2. Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich
3. Interner / externer Informationssicherheits-Beauftragter Name / Firma Kontakt
4. Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
5. Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
6. Formalisierter Prozess zur Bearbeitung von
7. Auskunftsanfragen seitens Betroffener ist vorhanden



## 4.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen

1. Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
2. Einsatz von Spamfilter und regelmäßige Aktualisierung
3. Einsatz von Virens Scanner und regelmäßige Aktualisierung

Organisatorische Maßnahmen

1. Dokumentierter Prozess zur Erkennung und
2. Meldung von Sicherheitsvorfällen / Daten-Pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
3. Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem

## 4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

Privacy by design / Privacy by default

Technische Maßnahmen

1. Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
2. Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen

## 4.4. Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Organisatorische Maßnahmen

1. Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
2. Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
3. Schriftliche Weisungen an den Auftragnehmer
4. Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis



## ANLAGE 3

# Datenschutzhinweise für Kunden/Vertragspartner gemäß der Europäischen Datenschutzgrundverordnung (DSGVO)

Die nachfolgende Information gibt Ihnen einen Überblick über die Verarbeitung Ihrer personenbezogenen Daten durch unser Unternehmen sowie die sich aus der DSGVO ergebenden Rechte für Sie.

### 1. Verantwortliche Stelle der Datenverarbeitung und Datenschutzbeauftragter

Verantwortlicher für die Datenverarbeitung ist („Unternehmen“, „wir“):  
arvatis media GmbH  
Kopernikusstr. 28  
40223 Düsseldorf  
Deutschland  
Tel.: +49 211 / 63 55 31 60  
E-Mail: info@arvatis.com

Unseren Datenschutzbeauftragten erreichen Sie unter:

arvatis media GmbH  
Datenschutzbeauftragter  
Kopernikusstr. 28  
40223 Düsseldorf  
Deutschland  
Tel.: +49 211 / 63 55 31 66  
E-Mail: detjen@arvatis.com

### 2. Art der Nutzung von personenbezogenen Daten

Wir verarbeiten personenbezogene Daten, die wir im Rahmen unserer Geschäftsbeziehung von Ihnen in Ihrer Funktion als Kunde/Vertragspartner bzw. als Vertreter/Bevollmächtigter/Ansprechpartner des Unternehmens erhalten, das unser Kunde/Vertragspartner ist. In der Geschäftsanbahnungsphase und während der Geschäftsbeziehung werden durch uns und Sie personenbezogene Daten erzeugt. Bei Unternehmen betreffen diese Daten im Wesentlichen den bei Ihnen zuständigen Ansprechpartner sowie ggf. die Unternehmensleitung (Geschäftsführer, Vorstand). Die in der Regel erzeugten personenbezogenen Daten sind:

Name, Anrede, Titel, Adresse, Telefonnummer, Telefaxnummer, E-Mail-Adresse, Kontodaten, Ihr Unternehmen / Firma (mit USt-ID), Abteilung, Position, Geburtsdatum, Vertragsgegenstand, Bonitätsbeurteilungen, Anfragen und Korrespondenz zum Abschluss, zur Verwaltung, zur Durchführung und zur Abrechnung des Vertrages.

### 3. Zweck und Rechtsgrundlage der Datenverarbeitung

Ihre personenbezogenen Daten werden gemäß den anwendbaren datenschutzrechtlichen Bestimmungen, insbesondere der DSGVO und dem Bundesdatenschutzgesetz (BDSG), verarbeitet. Im Einzelnen erfolgt dies zu folgenden Zwecken und aufgrund folgender Rechtsgrundlagen:

a) Aufgrund Ihrer Einwilligung gemäß Art. 6 Abs. 1 Satz 1 lit. a DSGVO  
Haben Sie uns eine Einwilligung zu der Verarbeitung für bestimmte Zwecke erteilt, so verarbeiten wir Ihre Daten auf Rechtsgrundlage der Einwilligung. Umfang und Zweck der Datenverarbeitung ist in der entsprechenden, Ihnen gesondert mitgeteilten Einwilligungserklärung beschrieben.



b) Zur Erfüllung von vertraglichen Pflichten gemäß Art. 6 Abs. 1 Satz 1 lit. b DSGVO

Die Verarbeitung von personenbezogenen Daten erfolgt aus Gründen der Abwicklung von Verträgen, namentlich zur Durchführung Ihres Vertrages. Weitere Informationen zu den Zwecken und dem Umfang der vertraglichen Leistungen, für die die Daten verarbeitet werden, können Sie dem jeweiligen mit Ihnen geschlossenen Vertrag und den darin einbezogenen AGB entnehmen.

c) Zur Erfüllung gesetzlicher Vorgaben gemäß dem Art. 6 Abs. 1 Satz 1 lit. c DSGVO

Als Unternehmen unterliegen wir diversen gesetzlichen Anforderungen zur Erfüllung steuerrechtlichen Kontroll- und Meldepflichten. Zur Sicherstellung dieser Anforderungen werden personenbezogene Daten im Rahmen der Geschäftsanbahnung und Abwicklung entsprechend den gesetzlichen Vorgaben verarbeitet.

d) Im Rahmen der Interessenabwägung gemäß Art. 6 Abs. 1 Satz 1 lit. f DSGVO

Wir verarbeiten Ihre Daten über die eigentliche Erfüllung des Vertrages hinaus zur Wahrung berechtigter Interessen von uns oder Dritten:

- Werbung per E-Mail zu ähnlichen Produkten oder per Post, sofern Sie dem nicht widersprochen haben, um Sie auf unsere aktuellen Angebote hinweisen zu können (unser berechtigtes Interesse)

4. Wer erhält meine Daten?

Auf Ihre personenbezogenen Daten erhalten grundsätzlich nur die Stellen Zugriff, die sie zur Erfüllung der vertraglichen und gesetzlichen Pflichten benötigen. Hierzu gehören folgende Stellen:

- plentymarkets GmbH, Bürgermeister-Brunner-Straße 15, 34117 Kassel: Die plentymarkets GmbH fungiert als Partner von arvatis und stellt das System plentymarkets7 (SaaS) bereit. In von Auftraggebern zugestimmten Einzelfällen kommt es zum Datenaustausch zwischen dem plentymarkets-System des Auftraggebers und arvatis, durch Im- und Exporte von Kunden und Bestelldaten welche durch arvatis auf den vom Auftraggeber bereitgestellten Systemen durchgeführt wird. In den besagten Fällen speichert arvatis die zu transferierenden Daten verschlüsselt zwischen, um diese nach Ende des Vorgangs wieder zu vernichten.
- shopware AG, Ebbinghoff 10, 48624 Schöppingen: Nutzung des Shopware Kundencenters zur Verwaltung von Lizenzen und Plugin-Angeboten sowie Zuordnung der Auftraggeber (Lizenzkäufer). Kommunikation mit Auftraggebern oder Interessenten über das Shopware Ticket-Nachrichtensystem.

Außerdem übermitteln wir Ihre Daten an Dienstleister, die wir für folgende Zwecke einsetzen:

- Chat-Software zur internen und externen Abstimmung des Auftrags
- Versand von E-Mail-Newslettern (sofern wir Ihre E-Mail-Adresse dafür nutzen dürfen)
- Visuelles Managementsystem zur Aufgabenverwaltung und Controlling-Auswertung
- Filehosting zur Versionierungsverwaltung
- Steuerberatung

Zu Abrechnungszwecken geben wir die erforderlichen Zahlungsdaten an unsere Hausbank weiter.

Sofern in dem Datenverarbeitungsprozess auch Dienstleister und Erfüllungsgehilfen eingebunden sind, ist dies nur möglich, wenn die dafür in der DSGVO vorgeschriebenen rechtlichen Verpflichtungen, sowie den Vorgaben von uns zum Umgang mit personenbezogenen Daten, verpflichtend gefolgt wird.

5. Findet eine Übermittlung meiner personenbezogenen Daten in ein „Drittland“ statt?

Eine Übermittlung Ihrer personenbezogenen Daten in Länder außerhalb der EU bzw. des EWR findet grundsätzlich nur statt, wenn Sie uns hierfür eine Einwilligung erteilt haben oder dies für die Durchführung eines Vertrages notwendige Bedingung ist.

6. Wie lange werden meine Daten gespeichert?



Ihre personenbezogenen Daten werden solange verarbeitet und gespeichert, wie es zur Erfüllung unserer vertraglichen und gesetzlichen Verpflichtungen notwendig ist. Nach Erfüllung der vertraglichen und gesetzlichen Pflichten, werden die personenbezogenen Daten regelmäßig gelöscht. Ausnahmen hiervon sind:

- Die Erfüllung handels- und steuerrechtlicher Aufbewahrungsfristen. Die Fristen hierfür betragen zwischen zwei bis zehn Jahren.
- Die Erhaltung von Beweismitteln im Rahmen der jeweils anwendbaren Verjährungsvorschriften. Gemäß den §§ 195 ff. des Bürgerlichen Gesetzbuches können diese Verjährungsfristen bis zu dreißig Jahren betragen. Die regelmäßige Verjährungsfrist beträgt hier drei Jahre bis zum Jahresende.

## 7. Welche Datenschutzrechte kann ich wahrnehmen?

Sie haben als „betroffene Person“ gegenüber uns folgende Rechte hinsichtlich der Sie betreffenden personenbezogenen Daten (Art. 15 ff. DSGVO):

Die betroffene Person hat das Recht, von uns eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf die in Art. 15 DSGVO im einzelnen aufgeführten Informationen.

Die betroffene Person hat das Recht, von uns unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten und ggf. die Vervollständigung unvollständiger personenbezogener Daten zu verlangen (Art. 16 DSGVO).

Die betroffene Person hat das Recht, von uns zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, sofern einer der in Art. 17 DSGVO im einzelnen aufgeführten Gründe zutrifft, z.B. wenn die Daten für die verfolgten Zwecke nicht mehr benötigt werden (Recht auf Löschung).

Die betroffene Person hat das Recht, von uns die Einschränkung der Verarbeitung zu verlangen, wenn eine der in Art. 18 DSGVO aufgeführten Voraussetzungen gegeben ist, z.B. wenn die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat, für die Dauer der Prüfung durch den Verantwortlichen.

Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten Widerspruch einzulegen. Wir verarbeiten die personenbezogenen Daten dann nicht mehr, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Art. 21 DSGVO). Der Widerruf wirkt erst in der Zukunft. Verarbeitungen von personenbezogenen Daten vor Ausspruch des Widerrufs sind hiervon nicht betroffen.

Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt (Art. 77 DSGVO). Die betroffene Person kann dieses Recht bei einer Aufsichtsbehörde in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes geltend machen.

Eine von einer betroffenen Person erteilte Einwilligung zur Verarbeitung von personenbezogenen Daten kann jederzeit gegenüber uns widerrufen werden. Dies gilt auch für Einwilligungen, die vor dem 25. Mai 2018 (Geltung der DSGVO) erteilt worden sind. Der Widerruf wirkt erst in der Zukunft. Verarbeitungen von personenbezogenen Daten vor Ausspruch des Widerrufs sind hiervon nicht betroffen.

## 8. Pflicht zur Bereitstellung von Daten

Die von uns im jeweiligen Vertrag abgefragten Daten (Name, Unternehmen/Firma, Kontakt- und Kontodaten) müssen bereitgestellt werden. Ohne Bereitstellung dieser Daten müssen wir Sie bzw. Ihr Unternehmen als Vertragspartner ablehnen, da wir diese zwingend zur Vertragsabwicklung benötigen.

Stand: 25. Mai 2018