

# VEREINBARUNG ZUR AUFTRAGSDATENVERARBEITUNG GEMÄß Art. 28 DSGVO

07. Dezember 2020

*zwischen*

DevStorage, Inh. Thomas Michaelis  
Lerchenweg 8  
73072 Donzdorf  
Deutschland

- im Folgenden Auftragnehmer -

*und*



- im Folgenden Auftraggeber-

*– Auftragnehmer und Auftraggeber werden nachstehend auch als Vertragsparteien  
bezeichnet. –*

---

## Anlagen

- Anhang 1 "Sicherheitskonzept"
  - Anhang 2 "Unterauftragsverhältnisse"
-

## **§1 Gegenstand des Auftrags, Datenkategorien, Betroffene, Art, Umfang und Zwecksetzung der Verarbeitung (Art. 28 Abs. 3, 30 Abs. 2 DSGVO)**

### **§ 1.1 GEGENSTAND**

Der Gegenstand des AV-Vertrages, die im Rahmen des Auftrags verarbeiteten personenbezogenen Daten (Art, 4 Nr. 1 DSGVO; nachfolgend kurz „Daten“), die von der Verarbeitung betroffene Personen (nachfolgend kurz „Betroffene“) sowie Art, Umfang und Zwecke der Verarbeitung, werden durch die folgenden Rechtsbeziehung(en) zwischen den Vertragsparteien bestimmt (nachstehend bezeichnet als Hauptvertrag):

Der Auftragnehmer bietet Produkte und Leistungen aus den Bereichen Domains, DNS, Webhosting, Managed Server, virtuelle Server, SSL-Zertifikate und Housing von Servern im Rechenzentrum an. Der konkrete Gegenstand und die Dauer des Auftrags sowie der Umfang und die Art der Datenerhebung, -verarbeitung und -nutzung ergibt sich aus dem mit dem Auftraggeber geschlossenen Rahmenvertrag sowie eventuellen Zusatzvereinbarungen.

### **§ 1.2 ART DER DATEN**

Gegenstand der Verarbeitung personenbezogener Daten sind sämtliche Datenarten / -kategorien, zu denen der Auftraggeber Informationen an den Auftragnehmer zur Erfüllung der in den Vereinbarungen (Rahmenvertrag und Zusatzvereinbarungen) definierten Leistungen an die Schnittstellen des Auftragnehmers überträgt.

## **§2 Verantwortlichkeit und Weisungsrecht**

**§ 2.1** Der Auftraggeber ist als Verantwortlicher gem. Art. 4 Nr. 7 DSGVO für die Einhaltung der datenschutzrechtlichen Vorgaben, insbesondere für die Auswahl des Auftragnehmers, die an diesen übermittelten Daten sowie erteilte Weisungen verantwortlich (Art. 28 Abs. 3 lit. a, 29 u. 32 Abs. 4 DSGVO).

**§ 2.2** Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrages sowie der Weisungen des Auftraggebers verarbeiten (was insbesondere auch für deren Berichtigung, Löschung oder Einschränkung der Verarbeitung gilt) und nur insoweit die Verarbeitung hierzu erforderlich ist, außer wenn der Auftragnehmer zu der Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 S. 2 lit. a DSGVO).

§ 2.3 Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen im Hinblick auf die Verarbeitung der Daten und die Sicherheitsmaßnahmen zu erteilen.

§ 2.4 Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen geltendes Datenschutzrecht verstößt, wird er den Auftraggeber unverzüglich darauf hinweisen. In diesem Fall ist der Auftragnehmer berechtigt, die Ausführung der Weisung bis zur Bestätigung der Weisung durch den Auftraggeber auszusetzen und im Fall offensichtlich rechtswidriger Weisungen abzulehnen.

§ 2.5 Gehen ergänzende Weisungen des Auftraggebers über die Leistungspflicht des Auftragnehmers nach dem Hauptvertrag hinaus und beruhen sie nicht auf einem Fehlverhalten des Auftragnehmers, dann hat der Auftraggeber dem Auftragnehmer den dadurch entstehenden Mehraufwand gesondert zu vergüten.

§ 2.6 Die Vertragsparteien können zum Erteilen und Empfangen von Weisungen berechtigte Personen benennen (insbesondere, wenn diese sich nicht bereits aus dem Hauptvertrag ergeben) und sind verpflichtet deren Änderung unverzüglich mitzuteilen.

### **§3 Sicherheitskonzept und diesbezügliche Pflichten**

§ 3.1 Der Auftragnehmer wird die innerbetriebliche Organisation in seinem Verantwortungsbereich entsprechend den gesetzlichen Anforderungen gestalten und wird insbesondere technische und organisatorische Maßnahmen (nachfolgend bezeichnet als „TOMs“) zur angemessenen Sicherung, insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit von Daten des Auftraggebers, unter Beachtung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen treffen sowie deren Aufrechterhaltung sicherstellen (Art. 28 Abs. 3 u. 32 - 39 i.V.m. Art 5 DSGVO). Zu den TOMs gehören insbesondere die Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, Trennungskontrolle und die Sicherung der Betroffenenrechte.

§ 3.2 Die diesem AV-Vertrag zugrundeliegenden TOMs ergeben sich aus dem Anhang 1 „Sicherheitskonzept“. Sie dürfen entsprechend dem technischen Fortschritt weiterentwickelt und durch adäquate Schutzmaßnahmen ersetzt werden, sofern sie das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschreiten und wesentliche Änderungen dem Auftraggeber mitgeteilt werden.

§ 3.3 Der Auftragnehmer stellt sicher, dass die zur Verarbeitung der Daten des Auftraggebers befugten Personen auf Vertraulichkeit und Verschwiegenheit (Art. 28 Abs. 3 S. 2 lit. b und 29, 32 Abs. 4 DSGVO) verpflichtet und in die Schutzbestimmungen der

DSGVO eingewiesen worden sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

**§ 3.4** Die im Rahmen des AV-Vertrages überlassene Daten sowie Datenträger und sämtliche hiervon gefertigten Kopien verbleiben im Eigentum des Auftraggebers, sind durch den Auftragnehmer sorgfältig zu verwahren, vor Zugang durch unberechtigte Dritte zu schützen und dürfen nur mit Zustimmung des Auftraggebers, und dann nur datenschutzgerecht, vernichtet werden. Kopien von Daten dürfen nur erstellt werden, wenn sie zur Erfüllung der Leistungshaupt- und Nebenpflichten des Auftragnehmers gegenüber dem Auftraggeber erforderlich sind (z.B. Backups).

**§ 3.5** Sofern durch die DSGVO oder ergänzende, insbesondere nationale Vorschriften, vorgegeben, benennt der Auftragnehmer eine/n den gesetzlichen Vorgaben entsprechende/n Datenschutzbeauftragte/n und informiert den Auftraggeber entsprechend (Art. 37 bis 39 DSGVO).

## **§ 4 Informationspflichten und Mitwirkungspflichten**

**§ 4.1** Betroffenenrechte sind gegenüber dem Auftraggeber wahrzunehmen, wobei der Auftragnehmer den Auftraggeber hierbei gem. Art. 28 Abs. 3 S. 2 lit. e. DSGVO unterstützt und ihn insbesondere über die bei ihm eingehenden Anfragen Betroffener informiert.

**§ 4.2** Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er im Hinblick auf die Verarbeitung der Daten Fehler oder Unregelmäßigkeiten im Hinblick auf die Einhaltung der Bestimmungen dieses AV-Vertrages oder einschlägiger Datenschutzvorschriften feststellt.

**§ 4.3** Für den Fall, dass der Auftragnehmer Tatsachen feststellt, welche die Annahme begründen, dass der Schutz der für den Auftraggeber verarbeiteten Daten verletzt worden ist, hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig zu informieren, unverzüglich erforderliche Schutzmaßnahmen zu ergreifen, und bei der Erfüllung der dem Auftraggeber obliegenden Pflichten gem. Art. 33 und 34 DSGVO zu unterstützen.

**§ 4.4** Sollte die Sicherheit der Daten des Auftraggebers durch Maßnahmen Dritter (z.B. Gläubiger, Behörden, Gerichte, etc.) gefährdet sein (Pfändung, Beschlagnahme, Insolvenzverfahren, etc.) wird der Auftragnehmer die Dritten unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich bei dem Auftraggeber liegen und nach Rücksprache mit dem Auftraggeber, sofern erforderlich, entsprechende Schutzmaßnahmen ergreifen (z.B. Widersprüche, Anträge, etc. stellen).

**§ 4.5** Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde gegenüber dem Auftragnehmer tätig wird und deren Tätigkeit die für den Auftragnehmer verarbeiteten Daten betreffen kann. Der Auftragnehmer unterstützt den Auftraggeber bei der Wahrnehmung seiner Pflichten (insbesondere zur Auskunft- und Duldung von Kontrollen) gegenüber Aufsichtsbehörden (Art. 31 DSGVO).

**§ 4.6** Der Auftragnehmer stellt dem Auftraggeber Informationen betreffend die Verarbeitung von Daten im Rahmen dieses AV-Vertrages, die für dessen Erfüllung von gesetzlichen Pflichten (zu denen insbesondere Anfragen Betroffener oder Behörden und die Einhaltung seiner Rechenschaftspflichten gem. Art. 5 Abs. 2 DSGVO, als auch die Durchführung einer Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO gehören können) notwendig sind, zur Verfügung, sofern der Auftraggeber diese Informationen nicht selbst beschaffen kann. Die Informationen müssen dem Auftragnehmer zur Verfügung stehen und müssen nicht von Dritten beschafft werden, wobei Mitarbeiter, Beauftragte und Subunternehmer des Auftraggebers nicht als Dritte gelten.

**§ 4.7** Gehen die Zurverfügungstellung der notwendigen Informationen und die Mitwirkung über die Leistungspflicht des Auftragnehmers nach dem Hauptvertrag hinaus und beruht nicht auf einem Fehlverhalten des Auftragnehmers, hat der Auftraggeber dem Auftragnehmer den dadurch entstehenden Mehraufwand gesondert zu vergüten.

## **§ 5 Kontrollbefugnisse**

**§ 5.1** Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorgaben und der Regelungen dieses AV-Vertrages, insbesondere der TOMs beim Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren (Art. 28 Abs. 3 lit. h DSGVO).

**§ 5.2** Die Kontrollen sind auf den erforderlichen Rahmen beschränkt und müssen auf Betriebs- und Geschäftsgeheimnisse des Auftragnehmers sowie den Schutz von personenbezogenen Daten Dritter (z.B. anderer Kunden oder Mitarbeiter des Auftragnehmers) Rücksicht nehmen. Zur Durchführung der Kontrolle sind nur fachkundige Personen zugelassen, die sich legitimieren können und im Hinblick auf die Betriebs- und Geschäftsgeheimnisse sowie Prozesse des Auftragnehmers und personenbezogene Daten Dritter zur Verschwiegenheit verpflichtet sind.

**§ 5.3** Statt der Einsichtnahmen und der Vor-Ort-Kontrollen, darf der Auftragnehmer den Auftraggeber auf eine gleichwertige Kontrolle durch unabhängige Dritte (z.B. neutrale Datenschutzauditoren), Einhaltung genehmigter Verhaltensregeln (Art. 40 DSGVO) oder geeignete Datenschutz- oder IT-Sicherheitszertifizierungen gem. Art. 42 DSGVO verweisen. Dies gilt insbesondere dann, wenn Betriebs- und Geschäftsgeheimnisse des Auftragnehmers oder personenbezogene Daten Dritter durch die Kontrollen gefährdet wären.

**§ 5.4** Geht die Duldung und Mitwirkung bei den Kontrollen, bzw. adäquaten Alternativmaßnahmen des Auftraggebers über die Leistungspflicht des Auftragnehmers nach dem Hauptvertrag hinaus und beruhen sie nicht auf einem Fehlverhalten des Auftragnehmers, dann hat der Auftraggeber dem Auftragnehmer den dadurch entstehenden Mehraufwand gesondert zu vergüten.

## § 6 Unterauftragsverhältnisse

**§ 6.1** Nimmt der Auftragnehmer die Dienste eines Unterauftragsverarbeiters (d.h. Unterauftragnehmer oder Subunternehmer) in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, dann muss er dem Unterauftragsverarbeiter im Wege eines Vertrags oder eines nach der DSGVO zulässigen anderen Rechtsinstruments dieselben Datenschutzpflichten zu denen sich der Auftragnehmer in diesem AV-Vertrag verpflichtet hat, auferlegen (insbesondere im Hinblick auf die Befolgung von Weisungen, Einhaltung der TOMs, Erteilung von Informationen und Duldung von Kontrollen). Ferner hat der Auftragnehmer den Unterauftragsverarbeiter sorgfältig auszuwählen, auf dessen Zuverlässigkeit zu prüfen und diese, als auch dessen Einhaltung der vertraglichen und gesetzlichen Vorgaben zu überwachen (Art. 28 Abs. 2 u. 4 DSGVO).

Der Auftraggeber erklärt sich unbeschadet etwaiger Einschränkungen durch den Hauptvertrag ausdrücklich damit einverstanden, dass der Auftragnehmer im Rahmen der Auftragsverarbeitung Unterauftragsverarbeiter einsetzen darf.

**§ 6.2** Die bereits zum Abschluss dieses AV-Vertrages bestehenden Unterauftragsverhältnisse, werden vom Auftragnehmer im Anhang 2 „Unterauftragsverhältnisse“ angegeben und gelten vom Auftragnehmer als genehmigt.

**§ 6.3** Der Auftragnehmer informiert den Auftraggeber im Hinblick auf Änderungen bei den Unterauftragsverarbeitern, die für die Auftragsverarbeitung maßgeblich sind. Der Auftraggeber macht von seinem Recht auf Einspruch im Hinblick auf die Änderungen oder neue Unterauftragsverarbeiter nur unter Beachtung der Grundsätze von Treu und Glauben sowie der Angemessenheit und Billigkeit Gebrauch.

**§ 6.4** Vertragsverhältnisse, bei denen der Auftragnehmer die Leistungen Dritter als reine Nebenleistung in Anspruch nimmt, um seine geschäftliche Tätigkeit auszuüben (z.B. Reinigungs-, Bewachungs- oder Transportleistungen) stellen keine Unterauftragsverarbeitung im Sinne der vorstehenden Regelungen dieses AV-Vertrages dar. Gleichwohl hat der Auftragsverarbeiter sicher zu stellen, z.B. durch vertragliche Vereinbarungen oder Hinweise und Instruktionen, dass hierbei die Sicherheit der Daten nicht gefährdet wird und die Vorgaben dieses AV-Vertrages und der Datenschutzvorschriften eingehalten werden.

## § 7 Verarbeitung in Drittländern

**§ 7.1** 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 (EWR) statt.

**§ 7.2** Die Auftragsverarbeitung in einem Drittland, auch durch Unterauftragsverarbeiter, bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, außer wenn der Auftragnehmer zu der Verarbeitung im Drittland durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 S. 2 lit. a DSGVO).

**§ 7.3** Die Zustimmung des Auftraggebers zur Verarbeitung im Drittland, gilt im Hinblick auf die im Anhang 2 „Unterauftragsverhältnisse“ genannten Verarbeitungen als erteilt.

## **§ 8 Dauer des Auftrags, Vertragsbeendigung und Datenlöschung**

**§ 8.1** Dieser AV-Vertrag wird mit dessen Abschluss gültig, wird auf unbestimmte Zeit geschlossen und endet spätestens mit der Laufzeit des Hauptvertrags.

**§ 8.2** Das Recht auf außerordentliche Kündigung bleibt den Vertragsparteien vorbehalten, insbesondere im Fall eines schwerwiegenden Verstoßes gegen die Vorgaben dieses AV-Vertrages und geltendes Datenschutzrecht. Der außerordentlichen Kündigung hat grundsätzlich eine Abmahnung der Verstöße mit angemessener Frist voranzugehen, wobei sie nicht erforderlich ist, wenn nicht damit zu rechnen ist, dass die beanstandeten Verstöße behoben werden oder diese derart schwer wiegen, dass ein Festhalten am AV-Vertrag der kündigenden Vertragspartei nicht zuzumuten ist.

**§ 8.3** Nach Abschluss der Erbringung der Verarbeitungsleistungen im Rahmen dieses AV-Vertrages, wird der Auftragnehmer alle personenbezogenen Daten und deren Kopien (sowie sämtliche im Zusammenhang mit dem Auftragsverhältnis in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände), nach Wahl des Auftraggebers entweder löschen oder zurückgeben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht (Art. 28 Abs. 1 S. 2 lit. g DSGVO). Die Einrede eines Zurückbehaltungsrechts, wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen. Im Hinblick auf die Löschung oder Rückgabe, gelten die Auskunfts-, Nachweis und Kontrollrechte des Auftraggebers entsprechend diesem AV-Vertrag.

**§ 8.4** Im Übrigen bleiben die Verpflichtungen aus diesem AV-Vertrag im Hinblick auf die im Auftrag verarbeiteten Daten auch nach Beendigung des AV-Vertrages bestehen.

**§ 8.5** Gehen die Löschung, bzw. die Rückgabe der Daten über die Leistungspflicht des Auftragnehmers nach dem Hauptvertrag hinaus und beruhen sie nicht auf einem

Fehlverhalten des Auftragnehmers, dann hat der Auftraggeber dem Auftragnehmer den dadurch entstehenden Mehraufwand gesondert zu vergüten.

## **§ 9 Vergütung**

**§ 9.1** Die nach diesem AV-Vertrag vereinbarte Vergütung umfasst auch eine Aufwandsentschädigung für die Arbeitszeit des vom Auftragnehmer beanspruchten Personals sowie erforderliche Auslagen (z.B. Reise- oder Materialkosten). Sofern möglich, absehbar und zumutbar, teilt der Auftragnehmer dem Auftraggeber die Höhe der Vergütung im Wege einer sachgerechten Schätzung mit.

**§ 9.2** Die Höhe der Vergütung bestimmt sich nach dem Hauptvertrag. Sofern im Hauptvertrag keine für den AV-Vertrag maßgeblichen Vergütungsregelungen oder entsprechend anwendbaren Sätze für Serviceleistungen getroffen sind, gelten vorerst keine Vergütungssätze.

## **§ 10 Haftung**

**§ 10.1** 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.

**§ 10.2** Die Vertragsparteien stellen sich jeweils von der Haftung frei, wenn eine der Vertragsparteien nachweist, dass sie für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, in keinerlei Hinsicht verantwortlich ist.

## **§ 11 Schlussbestimmungen, Rangfolge, Änderungen, Kommunikationsform, Rechtswahl, Gerichtsstand**

**§ 11.1** Änderungen, Nebenabreden und Ergänzungen dieses AV-Vertrages und seiner Anhänge bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieses AV-Vertrages handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

**§ 11.2** Dieser AV-Vertrag verpflichtet den Auftragnehmer nur insoweit, als dies zur Erfüllung der gesetzlichen Pflichten, insbesondere nach Art. 28 ff. DSGVO erforderlich ist und legt dem Auftragnehmer darüber hinaus keine weiteren Pflichten auf.

**§ 11.3** Vorbehaltlich einer Verpflichtung zur Schriftform in diesem AV-Vertrag und im Hauptvertrag, erfolgt die Kommunikation zwischen dem Auftragnehmer und Auftraggeber im Rahmen dieses AV-Vertrages (insbesondere im Hinblick auf Weisungen und Informationserteilung) zumindest in Textform (z.B. E-Mail). Eine geringere Form (z.B. mündlich) kann den Umständen nach statt der Textform zulässig sein (z.B. in



Notfallsituation), muss jedoch unverzüglich zumindest in Textform bestätigt werden. Sofern die Schriftform verlangt wird, ist die Schriftform im Sinne der DSGVO gemeint.

**§ 11.4** Es gilt das Recht der Bundesrepublik Deutschland. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem AV-Vertrag ist der Sitz des Auftragnehmers, sofern der Auftraggeber Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist oder der Auftraggeber in der Bundesrepublik Deutschland keinen Gerichtsstand hat. Der Auftragnehmer behält sich vor, seine Ansprüche an dem gesetzlichen Gerichtsstand geltend zu machen.

Stand: 07.12.2020

---

Ort, Datum

---

Unterschrift

- Auftraggeber-



---

Ort, Datum

---

Unterschrift

- Auftraggeber-

# Auftrag zur Verarbeitung personenbezogener Daten

## Anhang 1 – Sicherheitskonzept

### Technische und Organisatorische Maßnahmen gem. Art. 32 DSGVO

Grundsätzliche Maßnahmen, die der Wahrung der Betroffenenrechte, unverzüglichen Reaktion in Notfällen, den Vorgaben der Technikgestaltung und dem Datenschutz auf Mitarbeiterebene dienen:

- Es besteht ein betriebsinternes Datenschutz-Management, dessen Einhaltung ständig überwacht wird sowie anlassbezogenen und mindestens halbjährlichen evaluiert wird.
- Es besteht ein Konzept, welches die Wahrung der Rechte der Betroffenen (Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Datentransfer, Widerruf & Widersprüche) innerhalb der gesetzlichen Fristen gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen.
- Es besteht ein Konzept, das eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Verletzungen des Schutzes personenbezogener Daten (Prüfung, Dokumentation, Meldung) gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen
- Der Schutz von personenbezogenen Daten wird unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen bereits bei der Entwicklung, bzw. Auswahl von Hardware, Software sowie Verfahren, entsprechend dem Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigt (Art. 25 DSGVO).
- Die eingesetzte Software wird stets auf dem aktuell verfügbaren Stand gehalten, ebenso wie Virens Scanner und Firewalls.
- Mitarbeiter werden im Hinblick auf den Datenschutz auf Verschwiegenheit verpflichtet, belehrt und instruiert, als auch auf mögliche Haftungsfolgen hingewiesen.
- Die an Mitarbeiter ausgegebene Zugangsdaten oder Codes sowie im Hinblick auf die Verarbeitung personenbezogener Daten erteilte Berechtigungen, werden nach deren Ausscheiden aus dem Unternehmen, bzw. Wechsel der Zuständigkeiten eingezogen, bzw. entzogen.

• Dienstleister, die zur Erfüllung nebensächlicher Aufgaben herangezogen werden, werden sorgfältig ausgesucht und es wird sichergestellt, dass sie den Schutz personenbezogener Daten beachten.

- Zugangskontrolle / Zugriffskontrolle
- Firewalls (Hardware / Software).
- Stets aktuelle Softwareversionen.
- Mindestpasswortlängen und Passwortmanager.
- Einsatz von VPN-Technologie.
- Protokollierung von Zugriffen auf Daten.
- Weitergabekontrolle
- Festlegung und Dokumentation der Empfänger.
- Dedizierte Weitergabeberechtigungen.
- Eingabekontrolle
- Protokollierung von Dateneingaben-, Änderungen und Löschungen.
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind.
- Auftragskontrolle
- Verfügbarkeitskontrolle / Integrität
- Gewährleistung des Zweckbindungs- / Trennungsgebotes
- Trennung von Produktiv- und Testsystem.

## **Zugangskontrolle Rechenzentrumsräume**

Der Zutritt zum Rechenzentrum ist über mehrere Türen gesichert, welche sich nur durch das Personal des Rechenzentrums öffnen lassen. Der Zutritt zum Serverraum ist durch ein biometrisches Zutrittssystem geschützt, welches nur Befugten Personen Zutritt gewährt. Zutritt zum Serverraum haben nur die Kunden sowie das Personal des Rechenzentrums. Sämtliche Serversysteme des Auftragnehmers befinden sich in eigenen Schränken, welche separat verschlossen sind. Der gesamte Bereich wird videoüberwacht, die Aufzeichnungen werden durch den Rechenzentrumsbetreiber gesichert. Das Rechenzentrum verfügt über eine Einbruchmeldeanlage.

## **Übermittlung von Daten**

Personenbezogene Daten können entweder über unser Kundenportal unter Verwendung der jeweiligen individuellen Zugangsdaten des Kunden, bei einer Erstkontaktaufnahme über unsere Website oder per E-Mail übertragen werden. Sämtliche Daten werden ausschließlich verschlüsselt übertragen und auf Servern des Auftragnehmers verarbeitet. Die verschiedenen Berechtigungen des Auftragnehmers stellen sich, dass ausschließlich befugte Mitarbeiter des Auftragnehmers diese Daten einsehen, verändern und löschen können. Personenbezogene Daten werden nur für die Dauer der vertraglichen und gesetzlichen Fristen gespeichert und im Anschluss anonymisiert oder gelöscht

## **Zugriffskontrolle auf Serversysteme**

Der Zugriff auf Serversysteme ist nur mit einer Keyfile möglich. Mitarbeiter sind angewiesen, eventuelle Passwörter über eine interne Richtlinie zufällig zu generieren. Ein festgelegter Prozess regelt die Zugriffsberechtigungen bei der Neueinstellung und beim Ausscheiden von Mitarbeitern aus dem Unternehmen. Über sämtliche Änderungen der Zugriffsberechtigungen der Mitarbeiter wird elektronisch Protokoll geführt.

## **Sicherungen und Wiederherstellung**

Alle direkt durch den Auftragnehmer verwendeten Daten werden zentral auf Backupsystemen gesichert. Die Sicherung erfolgt separat nach Teilsystemen. So kann eine Wiederherstellung zeitnah durch Administratoren erfolgen. Die Speicherung der Backups erfolgt unverschlüsselt, der Zugriff auf Backupsysteme ist nur den Administratoren des Auftragnehmers möglich. Die Sicherung der Teilsysteme erfolgt mindestens einmal täglich.

## **Erreichbarkeit, Zuverlässigkeit**

Alle Dienste und Teilsysteme werden mit einer Monitoringsoftware überwacht.

# Auftrag zur Verarbeitung personenbezogener Daten

## Anhang 2 – Unterauftragsverhältnisse

(1) Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor Hinzuziehung weiterer oder Ersetzung der bisherigen Subunternehmer informiert der Auftragnehmer den Auftraggeber. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

(2) Der Auftraggeber kann der Änderung innerhalb einer angemessenen Frist aus wichtigem Grund gegenüber der vom Auftraggeber bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Die Beauftragung von Subunternehmern ist jedoch nur möglich, wenn dem Subunternehmer vertraglich Datenschutzpflichten auferlegt werden, die dem vorliegenden Vertrag vergleichbar sind.

(3) Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. 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.