# Bundesmuster Auftragsverarbeitung

02. August 2019



bitkom

# Zusammenfassung

Vor Geltungsbeginn der Datenschutzgrundverordnung (DS-GVO) am 25. Mai 2018 hat der Datenschutzbeauftragte des BMI ein neues Vertragsmuster zur Auftragsverarbeitung entwickelt, welches mit Empfehlungen des BfDI als Bundemuster kommuniziert wurde (Anlage 1). Es wurde die Verwendung dieser Mustervereinbarung für die gesamte Bundesverwaltung empfohlen.

Für die Bitkom Arbeitskreise Datenschutz und Digitale Verwaltung ist das Muster von größter Relevanz und großem Interesse. Im Bitkom Arbeitskreis Datenschutz befassen sich die Mitglieder bereits seit vielen Jahren intensiv mit Auftragsverarbeitungsverhältnissen, deren Abschluss und Umsetzung. Die Auslagerung von Datenverarbeitungsprozessen oder deren Übertragung auf einen Dienstleister, eine unternehmensfremde Stelle, ist für viele Unternehmen eine wichtige Möglichkeit, externes Spezialwissen zu nutzen, höhere Sicherheitsstandards zu erreichen und effektiver und flexibler zu wirtschaften. Die DS-GVO erkennt an, dass in der Realität viele Prozesse arbeitsteilig verlaufen, und eröffnet dafür mit Art.28 DS-GVO die Auftragsverarbeitung sowie mit Art.26 DS-GVO die gemeinsame Verantwortung. Im Rahmen der Befassung mit dem Thema der Auftragsverarbeitung entstanden im Bitkom die als Anlage 2 und 3 beigefügten Muster und der Leitfaden.

Bitkom möchte in Anbetracht eines möglichst einheitlichen Verständnisses der Datenschutz-Grundverordnung und einer praxisgerechten Auslegung diese Gelegenheit nutzen und das vom BfDI vorgeschlagene Bundesmuster zur Auftragsverarbeitung zu kommentieren. Neben einigen grundsätzlichen Anmerkungen finden sich unsere Vorschläge zur Ergänzung bzw. möglichen Anpassung des Musters als kommentierte Fassung im nachfolgenden Abschnitt.

## Anlagen

1. BfDI Bundesmuster zur Auftragsverarbeitung
2. Bitkom Mustervertragsanlage Auftragsverarbeitung
3. Bitkom Leitfaden zur Auftragsverarbeitung nach der DS-GVO

# Inhaltsverzeichnis

# 1 Definition für ein einheitliches Verständnis

Für ein einheitliches Verständnis möchten wir vorangestellt auf einige Begrifflichkeiten näher eingehen, deren genaue Bedeutung im Rahmen der Auftragsverarbeitungsverträge von Relevanz ist.

## Datenverarbeitung im Auftrag

Es gibt keine Legaldefinition des Begriffs der Auftragsverarbeitung in der DS-GVO. Art.28 DS-GVO legt lediglich die Anforderungen fest, bei dieser Art der arbeitsteiligen Datenverarbeitungen bestehen. Demnach ist eine Datenverarbeitung im Auftrag die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter (Auftragnehmer) nach Weisung und im Auftrag des Verantwortlichen (Auftraggeber).

## Weisung

Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt; der Auftraggeber hat ein Weisungsrecht im Rahmen dieser vereinbarten Leistung.

## Subunternehmer

Als Auftragnehmer des Auftragsverarbeiters im Sinne der DS-GVO ist der Subunternehmer ein »weiterer Auftragsverarbeiter«, vgl. Art.28 Abs.4 DS-GVO. Zur Vermeidung von Missverständnissen aufgrund der Erinnerung an § 11 Abs. 5 BDSG alt, sollte eine weitere Auftragsverarbeiter nur bei der Teil- oder vollständigen Übernahme der Hauptleistung definiert werden.

## Dritter

Der Ausdruck »Dritter« bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten (Art. 4 Nr. 10 DS-GVO).

## Datenübermittlung

Phase der Datenverarbeitung, in der personenbezogenen Daten von dem Verantwortlichen an andere Personen oder Stellen (Dritte) bekannt oder weitergegeben gegeben werden; im BDSG definiert in § 3 Abs. 4 Nr. 3. Die Bekanntgabe kann durch aktive Weitergabe, gleich in welcher Form, oder durch Einsicht eines Dritten oder Abruf der Daten durch einen Dritten erfolgen. Demgegenüber verwendet die DS-GVO eine umfassendere, weniger differenzierte Begriffsbestimmung der Verarbeitung (Art. 4 Nr. 2 DS-GVO), der die Übermittlung umfasst.

## »Funktionsübertragung«

Übertragung einer ganzen Funktion zur eigenverantwortlichen Wahrnehmung durch den Auftragnehmer (in Abgrenzung zur Datenverarbeitung im Auftrag). Mit diesem Begriff, der weder im BDSG, der RL 95/46 EG noch in der DS-GVO definiert wird, wird seit seiner Erwähnung in einer Gesetzesbegründung zum BDSG im Jahr 1989 eine weisungsabhängige, primär technische Dienstleistung (Auftragsverarbeitung) von einer (weitgehend) weisungsfreien, dabei eigene Aufgaben erfüllende Leistungserbringung abgegrenzt. Der Dienstleister wird dabei auch wegen der eigenen verfolgten Zwecke damit zu einem Verantwortlichen (Beispiele: Rechtsanwalt, Steuerberater Wirtschaftsprüfer oder auch Gutachter). Die Rechtmäßigkeitsgrundlage für die Übermittlung (Verarbeitung) der personenbezogenen Daten an solche Funktionsübernehmer ist meistens das überwiegende berechtigte Interesse (bisher nach § 28 Abs.1 Nr. 2 BDSG). Dieses Konstrukt ermöglicht auch die DS-GVO in Art.6 Abs.1 lit. f DS-GVO.

# 2 Grundsätzliche Anmerkungen zum Mustervertrag

## 2.1 Rahmenvertrag

Bitkom regt an, dass neben dem Mustervertrag zur Auftragsverarbeitung auch ein Muster »Rahmenvereinbarung AV« erstellt wird. In Ausschreibungen von Rahmenverträgen hat sich gezeigt, dass die Abwicklung und Bewerbung einfacher und transparenter für Bieter und ausschreibende Stelle ist, wenn bereits durch Rahmenverträge alle erforderlichen (Kern) Informationen über den Inhalt einer AVV vorliegen. Bieterfragen könnten so auch vor Angebotsabgabe einfacher beantwortet werden und dann im Zuschlagsfall beim späteren Abschluss von Einzelverträgen im Bedarfsfall »nur« noch die Anlagen zur Konkretisierung vereinbart werden. Diese Anlagen sollten dabei aus unserer Sicht folgende Aspekte umfassen:

- Konkretisierung des Auftragsinhalts mit
  - Gegenstand, Dauer und Zweck der Verarbeitung
  - Art(en) der personenbezogenen Daten
  - Kategorien betroffener Personen
- TOMs
- Subunternehmer

## 2.2 Grenzüberschreitende Datentransfers

Hinsichtlich grenzüberschreitender Datentransfers weisen wir darauf hin, dass Diskrepanzen zwischen Standardvertragsklauseln und den notwendigen Regelungen in der AVV bestehen (können).

## 2.3 Unterstützungsleistungen und Vergütung

Sofern die Vergütung für datenschutzrechtliche Unterstützungsleistungen bereits im Hauptvertrag geregelt werden soll, ist dies in den Fällen problematisch, in denen ein Pauschalpreis oder Aufwandsvergütung mit Obergrenze vereinbart werden soll. Eine Unterstützungsleistung ist aufgrund des derzeit nicht vorhersehbaren Umfangs nur als Vergütung nach Aufwand ohne Obergrenze möglich ohne den Auftragnehmer/ Auftragsverarbeiter unbillig zu belasten.
Bitkom schlägt daher einen gesonderten Punkt zur »Vergütung datenschutzrechtliche Unterstützungsleistung – Vergütung nach Aufwand ohne Obergrenze« im Hauptvertrag oder im AV-Muster vor. Am sinnvollsten ist es, wenn die Vergütung direkt im AVV geregelt wird und die entsprechenden Aspekte hierzu gesondert und übersichtlich in einem separaten Paragraphen aufgeführt werden.

Im Rahmen dieser Sonderregelung sollte dann auch konkretisiert werden, was genau unter »Unterstützungsleistungen« fällt und dass z.B. die Gewährleistung von TOMs nicht als Unterstützungsleistung bewertet wird. Im weiteren AVV kann dann auf die Regelungen zur Unterstützungsleistung und zur Vergütung Bezug genommen werden. Hierdurch würde auch vermieden, dass wie bisher in verschiedensten Paragraphen im Vertrag Aspekte zur Unterstützung und Vergütung aufgenommen werden müssen.

**Inhalt des Paragraphen:**
Soweit in der Leistungsvereinbarung Vereinbarungen zu Leistungsänderungen getroffen wurden, gehen diese den Regelungen in diesem Absatz vor. Soweit keine Vereinbarung zu Leistungsänderungen in der Leistungsvereinbarung getroffen wurden, werden Weisungen und Maßnahmen, die eine Abweichung zu den in dieser Auftragsvereinbarung oder in der Leistungsvereinbarung festgelegten Leistungen darstellen, als Antrag auf Leistungsänderung behandelt. Zusätzliche Weisungen und Maßnahmen, die über die vertraglich vereinbarten Leistungen hinausgehen, sind – soweit nicht ausdrücklich anders vereinbart – bei Mehraufwand für den Auftragsverarbeiter gesondert zu vergüten. Die Vertragsparteien werden sich in diesem Fall über eine angemessene Vergütung gesondert verständigen.

[...]

## 2.4 Auditrechte

Die Auditrechte sollten im Sinne einer einheitlichen und kohärenten Regelungsrahmens in einem separaten Abschnitt in dem AVV beschrieben werden.

# 3 Kommentierte Vertragsfassung

Nachfolgend möchten wir im Rahmen von Kommentaren auf die jeweiligen Einzelabschnitte des Vertragsmusters eingehen. Die Anmerkungen und Ergänzungen sollen vor allem den konstruktiven Dialog und Austausch über das Muster begünstigen.

## Vereinbarung zur Auftragsverarbeitung

Als Anlage zum Vertrag / zur Leistungsbeschreibung vom [Datum]
- nachfolgend »Leistungsvereinbarung« -

zwischen der

Bundesrepublik Deutschland (XXXX XXX), vertreten durch XXXXXX XXXX
- nachfolgend »Verantwortlicher« -

und

[Vertragspartner]
- nachfolgend »Auftragsverarbeiter« -

- beide nachfolgend gemeinsam »Vertragsparteien« -

wird die folgende Vereinbarung zur Auftragsverarbeitung geschlossen:

**Inhalt**

# 4 Stellungnahme

**Präambel**

Die Vertragsparteien sind mit der Leistungsvereinbarung ein Auftragsverarbeitungsverhältnis eingegangen. Um die sich hieraus ergebenden Rechte und Pflichten gemäß den Vorgaben der europäischen Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG – DSGVO), und des Bundesdatenschutzgesetzes (BDSG) zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

**§ 1 Anwendungsbereich**

Die Vereinbarung findet Anwendung auf die Erhebung, Verarbeitung und Löschung (im Folgenden: Verarbeitung) aller personenbezogener Daten (im Folgenden: Daten), die Gegenstand der Leistungsvereinbarung sind oder im Rahmen von deren Durchführung anfallen oder dem Auftragsverarbeiter bekannt werden und im Auftrag des Verantwortlichen verarbeitet werden (Art. 28 DS-GVO).

**Vorschlag:** Es sollten ausschließlich die Begrifflichkeiten der DS-GVO verwendet werden, d.h. »Verarbeitung«. Andernfalls wird eine europaweite und einheitliche Anwendung erschwert.

**Anmerkung:** Diese Formulierung trifft die Auftragssituation nicht und muss daher angepasst werden. Unter diesen Anwendungsbereich würden auch personenbezogene Daten fallen, die zum Beispiel im Rahmen von Professional Services unter einem NDA ausgetauscht werden. Hierbei handelt es sich aber nicht zwingend um eine Auftragsverarbeitung. Daher sollte hier aufgenommen werden, dass die Vereinbarung Anwendung findet, wenn (i) die Leistungsvereinbarung die Verarbeitung von personenbezogenen Daten im Auftrag zum Gegenstand hat oder (ii) der Auftragsverarbeiter tatsächlich personenbezogene Daten im Auftrag verarbeitet.

**Vorschlag einer Ergänzung:** Die Vereinbarung soll nur für den relevanten Leistungsbereich Anwendung finden. Der Gegenstand der Leistungsvereinbarung könnte nämlich auch Leistungen enthalten, die nicht dem Art. 28 DSGVO unterliegen.

**Anmerkung:** Wichtig ist in diesem Zusammenhang auch der Kontext des früheren § 11(5) BDSG, dessen Wertung nach Geltung der DS-GVO und dem neuen BDSG nicht mehr fortgilt. Es ist daher äußerst relevant, die Auslegung zur Frage, wann eine Auftragsverarbeitung vorliegt an die derzeitige Rechtslage anzupassen. Dies betrifft vor allem die Tatsache, dass es keine Auftragsverarbeitung darstellt, wenn eine Person lediglich rein technisch und quasi zufällig bei der Erfüllung ihrer anderen Tätigkeit Zugriff auf Daten hat.

**§ 2 Konkretisierung des Auftragsinhalts**

1. Gegenstand und Dauer der Auftragsverarbeitung sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung von Daten bestimmen sich nach der Leistungsvereinbarung.

2. Folgende Datenarten oder -kategorien sind Gegenstand der Verarbeitung durch den Auftragsverarbeiter: [Aufzählung oder Beschreibung der Datenarten oder -kategorien, z.B. Personaldaten, Kommunikationsdaten etc.].

3. Der Kreis der durch den Umgang mit ihren Daten betroffenen Personen ist [...][1] konkret beschrieben.

**Gelöscht:** Nicht unter den Anwendungsbereich fallen Daten von Mitarbeitern des Auftragsverarbeiters, soweit sie ausschließlich das Beschäftigungsverhältnis mit dem Auftragsverarbeiter betreffen.

**Vorschlag:** Streichung dieses Satzes, da der Gegenstand des Vertrages die Auftragsverarbeitung ist und die Mitarbeiterdaten hierzu nicht gehören.

**Vorschlag:** Es sollte eine alternative Regelung geben, die Betroffenen auch in dieser Vereinbarung zu benennen.

**NEU:** § 2 Absatz 2 und 3 sollten in einer Anlage spezifiziert werden.

**Vorschlag:** Die Konkretisierung des Auftragsinhalts (Datenarten, Datenkategorien, betroffener Personenkreis) sollte in einer entsprechenden Anlage bzw. im Hauptvertrag abgebildet werden.

1 in der Leistungsbeschreibung mit Verweis auf dortige Fundstelle oder durch Bezugnahme auf einen gesonderten Anhang mit genauer Bezeichnung (Aufzählung oder Beschreibung der betroffenen Personenkategorien, z.B. Beschäftigte etc.)

**§ 3 Verantwortlichkeit und Weisungsbefugnis**

1. Die Vertragsparteien sind für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich. Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist der Verantwortliche verantwortlich. Der Verantwortliche wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z.B. durch Einholung von Einwilligungserklärungen) geschaffen werden, damit der Auftragsverarbeiter die vereinbarten Leistungen auch insoweit rechtsverletzungsfrei erbringen kann. Der Verantwortliche kann jederzeit die Herausgabe, Berichtigung, Anpassung, Löschung und Einschränkung der Verarbeitung der Daten verlangen.

**Vorschlag:** Hier sollte präzisiert werden, da »die Vertragsparteien« zu allgemein gefasst ist und der speziellen Situation zwischen Verantwortlichem und Auftragsverarbeiter nicht gerecht wird. Schließlich obliegt dem Verantwortlichen die Beurteilung der Zulässigkeit der Datenverarbeitung.

Gem. Art. 4 Nr. 7 DS-GVO ist der Auftraggeber der (Allein-)Verantwortliche, nicht die Vertragsparteien gemeinsam, wie es hier gegebenenfalls verstanden werden könnte. Insbesondere in klarer Abgrenzung zum Joint Controllership nach Art. 26 DS-GVO sollte eine deutlichere Regelung getroffen werden. Der Auftragnehmer ist wie in § 3 (4) auch geregelt, von den Weisungen des Auftraggebers abhängig.

**Formulierungsvorschlag:** Der Auftraggeber als Verantwortlicher ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragsverarbeiter sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich. Der Auftragsverarbeiter hat die ihm aufgrund der Auftragsverarbeitung obliegenden Pflichten, insbesondere die Sicherheit der Verarbeitung nach Maßgabe des Art. 32 DS-GVO zu gewährleisten.

Alternativ könnte durch Ergänzung von »in ihrem Aufgaben- und Zuständigkeitsbereich verantwortlich« eine Klarstellung erfolgen.

2. Zur Gewährleistung des Schutzes der Rechte der betroffenen Personen unterstützt der Auftragsverarbeiter den Verantwortlichen angemessen, insbesondere durch die Gewährleistung geeigneter technischer und organisatorischer Maßnahmen. Die Vertragsparteien werden/können sich in diesem Fall über Art und Umfang der Unterstützung und eine angemessene Vergütung gesondert verständigen.

**Ergänzung:** Hier sollte ein Verweis auf „angesichts der Art der Verarbeitung“ erfolgen. Andernfalls wäre die Regelung deutlich strenger als Art. 28 DS-GVO, der gerade die Einbeziehung der Datenverarbeitung in diese Beurteilung zulässt.

**Anmerkung und Ergänzung:** Sofern die Vergütung für datenschutzrechtliche Unterstützungsleistungen bereits im Hauptvertrag geregelt werden soll, ist dies in den Fällen problematisch, in denen ein Pauschalpreis oder Aufwandsvergütung mit Obergrenze vereinbart werden soll. Eine Unterstützungsleistung ist aufgrund des derzeit nicht vorhersehbaren Umfangs nur als Vergütung nach Aufwand ohne Obergrenze möglich ohne den Auftragnehmer/ Auftragsverarbeiter unbillig zu belasten. Bitkom schlägt daher einen gesonderten Punkt zur „Vergütung datenschutzrechtliche Unterstützungsleistung – Vergütung nach Aufwand ohne Obergrenze“ im Hauptvertrag oder im AV-Muster vor. Am sinnvollsten ist es, wenn die Vergütung direkt im AVV geregelt wird und die entsprechenden Aspekte hierzu gesondert und übersichtlich in einem separaten Paragraphen aufgeführt werden.

Im Rahmen dieser Sonderregelung sollte dann auch konkretisiert werden, was genau unter "Unterstützungsleistungen" fällt und dass z.B. die Gewährleistung von TOMs nicht hinzugezählt wird. Im weiteren Vertragsmuster könnte dann jeweils eine Bezugnahme erfolgen. Dies würde auch vermeiden, dass an verschiedensten Stellen auf Unterstützungleistungen und die Vergütung eingegangen werden muss.

3. Soweit sich eine betroffene Person zwecks Geltendmachung eines Betroffenenrechts unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

4. Der Auftragsverarbeiter darf Daten ausschließlich im Rahmen der Weisungen des Verantwortlichen verarbeiten, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder des Mitgliedstaates, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen 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 Satz 2 lit. a DSGVO). Eine Weisung ist die auf einen bestimmten Umgang des Auftragsverarbeiters mit Daten gerichtete schriftliche oder elektronische Anordnung des Verantwortlichen.
Die Anordnungen sind zu dokumentieren. Die Weisungen werden zunächst durch die Leistungsvereinbarung definiert und können von dem Verantwortlichen danach in dokumentierter Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.

**Anmerkung und Änderungsvorschlag:** Da die DS-GVO von dokumentierten Weisungen ausgeht, sollte die Weisung eher in Textform erfolgen. Abweichende Vereinbarungen sind weiterhin möglich, aus Dokumentationsgründen bedarf es für die mündliche Weisung dann jedoch dennoch einer Bestätigung.

**Gelöscht:** Mündlich erteilte Anordnungen sind unverzüglich schriftlich oder elektronisch zu bestätigen.

5. Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie von Seiten des Verantwortlichen bestätigt oder geändert wird.

**Gelöscht:** [Die weisungsberechtigten Personen auf Seiten des Verantwortlichen sowie die zum Empfang der Weisungen berechtigten Personen auf Seiten des Auftragsverarbeiters sowie die vorgesehenen Informationswege sind in Anlage xxx festgelegt].

**Anmerkung und Änderungsvorschlag:** In der Praxis werden die Ansprechpartner meist erst im Kick-Off Protokoll festgelegt und stehen bei Zuschlagserteilung noch nicht fest. D. h. zugleich, dass die jeweiligen Ansprechpartner bei Zuschlag nicht immer schon in der Anlage benannt werden können. Zudem ist die Beschränkung auf individuelle Personen wegen Urlaub, Krankheit, Abteilungswechsel etc. eher schwierig. Bitkom schlägt vor, den Inhalt der eckigen Klammer zu streichen und hier stattdessen eher auf Rollenbeschreibungen abzustellen.

6. Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Weisungen, die im Vertrag gem. § 2 (1) nicht vorgesehen sind, werden als Antrag auf Leistungsänderung (CR) behandelt. Auskünfte an Dritte oder die betroffene Person darf der Auftragsverarbeiter nur nach vorheriger ausdrücklicher schriftlicher oder elektronischer Zustimmung durch den Verantwortlichen erteilen, sofern er nicht gesetzlich oder behördlich dazu verpflichtet ist. Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an unberechtigte Dritte weiterzugeben. Kopien und Duplikate werden, mit Ausnahme von Sicherheitskopien zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung ohne Wissen des Verantwortlichen nicht erstellt.

**Anmerkung:** z.B. beim EVB-IT Erstellungsvertrag gem. Muster 3 Änderungsverfahren

**Vorschlag einer Ergänzung:** Hier könnte ergänzt werden, dass dies dann nicht gilt, wenn auf Basis einer gesetzlichen Regelung / staatlichen Anordnung (z.B. durch das BKA) Daten herausgegeben werden sollen.

**Vorschlag einer klarstellenden Ergänzung**

**Eingefügt:** unberechtigte

**Eingefügt:** mit Ausnahme von Sicherheitskopien zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung ohne Wissen

**Gelöscht:** Der Verantwortliche führt

7. das Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 DSGVO. Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Wunsch Informationen zur Aufnahme in das Verzeichnis zur Verfügung.

**Vorschlag einer Ergänzung:** Hier sollte aufgenommen werden, dass es nur solche Informationen handelt, die der Verantwortliche nicht eh schon hat oder mit angemessenem Aufwand beschaffen kann.

**Gelöscht:** Der Auftragsverarbeiter führt entsprechend den Vorgaben des Art. 30 Abs. 2 DSGVO ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung

**Anmerkung und Vorschlag zur Streichung:** Das ist bereits gesetzliche Pflicht des Auftragsverarbeiters und sollte nicht zu einem vertraglichen Anspruch des Verantwortlichen umfunktioniert werden. Die Pflicht ist darüber nicht in Art. 28 DS-GVO enthalten.

8. Die Verarbeitung der Daten im Auftrag des Verantwortlichen findet ausschließlich auf dem Gebiet / der Europäischen Union / des Europäischen Wirtschaftsraums [nicht zutreffende Alternative bitte streichen] statt.

**Gelöscht:** der Bundesrepublik Deutschland

**Eingefügt:** des Europäischen Wirtschaftsraums

**Anmerkung:** Datenlokalisationspflichten sollten als absolute Ausnahme gelten. Sinn und Zweck der DSGVO ist u. a. ein einheitliches grenzüberschreitendes Datenschutzniveau, das durch die Möglichkeit der Begrenzung der Verarbeitung rein auf das Gebiet der Bundesrepublik Deutschland – ohne triftigen Grund – widersprüchlich zum Grundgedanken der DS-GVO steht. U. E. müsste diese Wahlmöglichkeit gestrichen werden. D. h. die Verarbeitung in der Europäischen Union ist grundsätzlich zulässig, es sei denn es liegt ein Fall gem. Art. 78 Abs. 2 DS-GVO vor.

Der Text sollte daher standardmäßig auf die EU/ den EWR abzielen und nur in Sonderfällen die Verarbeitung ausschließlich auf dem Gebiet der BRD vorsehen.

Eine Beschränkung auf BRD ist zudem auch aufgrund der Vergabebedingungen kritisch zu bewerten, da die Ausschreibungsbedingungen diskriminierungsfrei sein müssen. Bei einer Beschränkung auf die BRD kommt es daher (sofern nicht die wenigen Ausnahmetatbestände einschlägig sind) mit hoher Warscheinlichkeit zu Verstößen.

Eine Verarbeitung in einem Staat außerhalb der EU ist nur zulässig wenn gewährleistet ist, dass unter Berücksichtigung der Voraussetzungen des Kapitels V der DSGVO das durch die DSGVO gewährleistete Schutzniveau nicht unterlaufen wird . Die grundlegenden Voraussetzungen für die Rechtmäßigkeit der Verarbeitung bleiben unberührt.

9. Der Auftragsverarbeiter gewährleistet dass ihm unterstellte natürliche Personen, die Zugang zu Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten. Eine Verarbeitung von Daten außerhalb der Betriebsräume des Auftragsverarbeiters (z.B. Telearbeit, Heimarbeit, Home Office, mobiles Arbeiten) bedarf der vorherigen ausdrücklichen schriftlichen Zustimmung des Verantwortlichen, die erst nach Festlegung angemessener technischer und organisatorischer Maßnahmen für die Verarbeitungssituation erteilt werden kann.

**§ 4 Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter**

1. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und weist dies dem Verantwortlichen auf Wunsch nach. Dies umfasst auch die Belehrung über die in diesem Auftragsverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.

2. Die Vertragsparteien unterstützen sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht im Hinblick auf die Grundsätze ordnungsgemäßer Datenverarbeitung einschließlich der Umsetzung der notwendigen technischen und organisatorischen Maßnahmen (Art. 5 Abs. 2, Art. 24 Abs. 1, Art. 30 Abs.2 DSGVO). Die Vertragsparteien stellen sich hierzu bei Bedarf entsprechende Informationen zur Verfügung.

**Gelöscht:** sichergestellt

**Vorschlag einer Änderung:** Begriffe, die auf eine Garantie im Rechtssinne mit der Folge einer unbeschränkten und verschuldensunabhängigen Haftung im Sinne von § 276 BGB hindeuten könnten, sollten vermieden werden.

**Gelöscht:** und bedarf der vorherigen ausdrücklichen schriftlichen Zustimmung des Verantwortlichen

**Anmerkung und Vorschlag zur Streichung:** In Satz 2 müsste u.E. der letzte Halbsatz gestrichen werden. Art. 45 Abs. 1 DS-GVO regelt deutlich, dass eine Übermittlung in ein Drittland oder eine internationale Organisation vorgenommen werden darf, wenn diese ein angemessenes Schutzniveau bieten. Gem. Art. 45 Abs. 1 S. 2 DS-GVO ist dann gerade keine besondere Genehmigung erforderlich. Woraus soll sich das Recht »der vorherigen ausdrücklichen schriftlichen Zustimmung« ergeben und widerspricht dies nicht gerade der Idee der Vereinheitlichung des grenzüberschreitenden

In der Praxis wird z. B. in einer Ausschreibung der Einsatz einer Software gefordert, die bestimmte Funktionalitäten erfüllen soll. Der Bieter entscheidet sich aus technischen und preislichen Gründen für eine Software, deren Hersteller Privacy Shield gelistet ist. Derzeit wäre dies ohne Zustimmung nicht möglich.

Unter Beachtung des Art. 28 Abs. 2 lit a könnte die Formulierung »und findet auf Basis einer dokumentierten Anweisung statt« oder »Diese Verarbeitung findet im Rahmen der dokumentierten Weisung nach art. 28 Absatz 3 lit. a DS-GVO statt«. eingefügt werden.

**Gelöscht:** stellt sicher

**Vorschlag einer Änderung:** Begriffe, die auf eine Garantie im Rechtssinne mit der Folge einer unbeschränkten und verschuldensunabhängigen Haftung im Sinne von § 276 BGB hindeuten könnten, sollten vermieden werden.

**Anmerkung:** Eine gesonderte Zustimmung widerspricht der proklamierten Erleichterung von Vereinbarkeit und Familie. Vgl. BMFSFJ ↗**https://www.erfolgsfaktor-familie.de/arbeitszeiten/familienbewusste-arbeitszeitmodelle-und-was-dahinter-steckt/home-office.html** U. E. sollte der Abschluss eines Home-Office-Vertrages, der die datenschutzrechtlichen Grundvorgaben berücksichtigt, zwischen Arbeitgeber und Mitarbeiter ausreichend sein. Aus besonderen sachlichen Gründen könnten zusätzlich Sonderregelungen vereinbart werden.

Eine vorherige ausdrückliche Zustimmung widerspricht zudem der angestrebten Förderung flexibler Arbeitsorte und Heimarbeit.

**Gelöscht:** stellt sicher

**Vorschlag einer Änderung:** Begriffe, die auf eine Garantie im Rechtssinne mit der Folge einer unbeschränkten und verschuldensunabhängigen Haftung im Sinne von § 276 BGB hindeuten könnten, sollten vermieden werden.

**Anmerkung:** »Gegenseitig« ist in Bezug auf die in § 4 Absatz 2 des Musters angesprochenen Pflichten eine eher unklare Terminologie und sollte präzisiert werden.

**Anmerkung:** Art. 5 Abs. 2 und Art. 24 Abs. 1 DS-GVO regeln nur die Rechenschaftspflicht des Verantwortlichen, also des Auftraggebers. Es ist aber von gegenseitiger Unterstützung der ihnen obliegenden Rechenschaftspflicht die Rede. Müsste dann nicht für den Auftragsverarbeiter noch Art. 30 Abs. 2 DS-GVO ergänzt werden und im Folgesatz auch der Verantwortliche verpflichtet werden, entspr. Informationen dem Auftragsverarbeiter zur Verfügung stellen (wenn z. B. zusätzliche personenbezogene Daten als Folge eines CR zu verarbeiten sind oder ein neues Ticketsystem eingeführt wird)?

3. Der Auftragsverarbeiter hat eine/n Datenschutzbeauftragte/n zu benennen, die/der ihre/seine Tätigkeit entsprechend den gesetzlichen Vorschriften ausübt. Die Kontaktdaten der/des Datenschutzbeauftragten sind dem Verantwortlichen zum Zwecke der direkten Kontaktaufnahme mitzuteilen. Änderungen an den Kontaktdaten oder in der Person des Datenschutzbeauftragten sind stets der Webseite des Auftragsverarbeiters zu entnehmen.

**Anmerkung:** Das sollte nur dann gelten, soweit eine gesetzliche Pflicht zur Bestellung besteht. Ist der AG also nicht zur Benennung eines DSB verpflichtet genügt die Mitteilung einer Datenschutzkontaktperson.

Begründung: Diskriminierungsfreiheit gegenüber europäischen Mitbewerbern; die DSB-Bestellung beruht ganz maßgeblich auf der deutschen, strengen Sonderregelung.

**Eingefügt:** Änderungen an den Kontaktdaten oder in der Person des Datenschutzbeauftragten sind stets der Webseite des Auftragsverarbeiters zu entnehmen.

4. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde im Rahmen ihrer Zuständigkeit bei dem Auftragsverarbeiter anfragt, ermittelt oder sonstige Erkundigungen einzieht.

**Anmerkung und Vorschlag einer Anpassung:** Diese Informationspflicht sollte auf Fälle beschränkt werden, bei denen der Verantwortliche im Rahmen der Verarbeitung personenbezogenen Daten von der Kontrolle betroffen ist.

**§ 5 Technisch-organisatorische Maßnahmen und deren Kontrolle**

1. Die Vertragsparteien vereinbaren die in dem Anhang »Technisch-organisatorische Maßnahmen« zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen. Der Anhang ist Gegenstand dieser Vereinbarung. Der Verantwortliche trägt die Verantwortung für die Bewertung der TOMs.

**Eingefügt:** Die Vertragsparteien vereinbaren die in dem

**Eingefügt:** Der Verantwortliche trägt die Verantwortung für die Bewertung der TOMs.

2. Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dem Anhang »Technisch-organisatorische Maßnahmen« festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

3. Der Auftragsverarbeiter wird dem Verantwortlichen alle sich aus dem vertraglich vereinbarten Leistungsumfang und innerhalb seines Verantwortungsbereichs als Auftragsverarbeiter ergebenden erforderlichen Informationen zur Verfügung stellen, die zum Nachweis der Einhaltung der in dieser Vereinbarung getroffenen und der gesetzlichen Vorgaben erforderlich sind. Er wird insbesondere Überprüfungen/Inspektionen, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und deren Durchführung unterstützen. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann dabei auch durch

**Eingefügt:** sich aus dem vertraglich vereinbarten Leistungsumfang und innerhalb seines Verantwortungsbereichs als Auftragsverarbeiter ergebenden

**Vorschlag einer Ergänzung:** zur Eingrenzung der Verantwortung des Auftragsverarbeiters auf seine Sphäre der Verantwortung

Vorlage eines aktuellen Testats, von Berichten hinreichend qualifizierter und unabhängiger Instanzen (z.B. Wirtschaftsprüfer, unabhängige Datenschutzauditoren), durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO, einer Zertifizierung nach Art. 42 DSGVO oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden. Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen über den Ausschluss von genehmigten Verhaltensregeln gemäß Art. 41 Abs. 4 DSGVO, den Widerruf einer Zertifizierung gemäß Art. 42 Abs. 7 und jede andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise unverzüglich zu unterrichten.

Hier sollte, auch nicht nur in beispielhafter Aufzählung, nur auf den BSI Grundschutz abgestellt werden, sondern auch auf ISO und SOC abgestellt werden.

4. Der Verantwortliche kann sich zu Prüfzwecken in den Betriebsstätten des Auftragsverarbeiters zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der gesetzlichen Vorgaben oder der zur Durchführung dieses Vertrages erforderlichen technischen und organisatorischen Erfordernisse überzeugen. Der Verantwortliche wird Kontrollen mit einer angemessenen Frist ankündigen und bei deren Durchführung auf den Geschäftsbetrieb und Betriebsablauf Rücksicht nehmen.

**Gelöscht:** jederzeit

**Vorschlag einer Anpassung:** Statt »jederzeit« sollte hier auf „nach vorheriger Abstimmung“ abgestellt werden. Vom Auditrecht kann der Verantwortliche natürlich jederzeit Gebrauch machen. Dabei muss es sich jedoch nicht stets um ein Vor-Ort-Audit handeln. Dies sollte hier präzisiert und abgestuft werden: Zunächst kann z.B. die Vorlage von Unterlagen und Prüfberichten erfolgen, dann der Einsatz eines unabhängigen von beiden Parteien bestimmten Prüfers, dann ein Vor-Ort-Audit. Das vorgesehene weite Auditrecht gefährdet die IT-Sicherheit für alle Kunden des Auftragsverarbeiters, weswegen eine Anpassung dringend erforderlich ist.

**Vorschlag einer Formulierung:** »Der Verantwortliche kann sich regelmäßig zu Prüfzwecken in den Betriebsstätten des Auftragsverarbeiters zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der gesetzlichen Vorgaben oder der zur Durchführung dieses Vertrages erforderlichen technischen und organisatorischen Erfordernisse überzeugen.«

**Vorschlag einer Ergänzung:** Der Verantwortliche wird Kontrollen mit einer angemessenen Frist ankündigen und bei deren Durchführung auf den Geschäftsbetrieb und Betriebsablauf Rücksicht nehmen.

5. Der Auftragsverarbeiter stellt dem Verantwortlichen darüber hinaus alle sich aus dem vertraglich vereinbarten Leistungsumfang und innerhalb seines Verantwortungsbereichs als Auftragsverarbeiter erforderlichen Informationen zur Verfügung, die er für die Prüfungen nach Absatz 4 sowie für eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der Daten (Datenschutz-Folgenabschätzung i.S.d. Art. 35 DSGVO) benötigt.

6. Der Auftragsverarbeiter hat im Benehmen mit dem Verantwortlichen alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Stands der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

**Anmerkung und Änderungsvorschlag:** Die Durchführung von Backups ist nicht immer Gegenstand des Auftrags, z.B. bei IaaS-Cloud-Services. Daher sollte keine allgemeine Pflicht aufgenommen werden. Alternativ könnte ein Vorbehalt aufgenommen werden „Soweit in der Leistungsvereinbarung vereinbart...“

**§ 6 Mitteilung bei Verstößen durch den Auftragsverarbeiter**

Der Auftragsverarbeiter unterrichtet den Verantwortlichen umgehend über eine Verletzung des Schutzes personenbezogener Daten des Verantwortlichen nachdem ihm diese Verletzung oder Umstände, die eine Verletzung begründen könnten bekannt geworden ist (nachdem ihm diese Verletzung oder Umstände die einen Verdacht begründen können bekannt geworden sind). Dies gilt insbesondere im Hinblick auf die Meldepflicht nach Art. 33 Abs. 2 DSGVO sowie auf korrespondierende Pflichten des Verantwortlichen nach Art. 33 und Art. 34 DSGVO. Der Auftragsverarbeiter wird den Verantwortlichen erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen. Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung gem. § 3 dieses Vertrages durchführen.

**Anmerkung:** Schwerwiegende Störungen des Betriebsablaufs sind zu definieren – wann schlägt dies auf die Verarbeitung durch? U.E. nach nicht, wenn es nur um die theoretische Möglichkeit eines Fernzugriffs geht (ehemals § 11 abs. 5 BDSG).

**Vorschlag einer Änderung:** Wiedergabe des Artikels 33 DS-GVO. U.a. die Meldung eines Verdachts einer Verletzung wäre weitreichender.

**§ 7 Löschung und Rückgabe von Daten**

1. Überlassene Datenträger und Datensätze verbleiben im Eigentum des Verantwortlichen.

**Anmerkung:** Einige Anbieter überlassen Geräte zur Miete, die eine Festplatte verbaut haben. Hier wird diese durch die Hintertür Eigentum des Verantwortlichen. Dies sollte berücksichtigt werden und der Satz angepasst werden (s.o).

**Formulierungvorschlag:** § 3 Pflichten des Auftragnehmers: (6) Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber. In besonderen, vom Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung bzw. Übergabe.

§ 8 Vertragsdauer und -beendigung: (3) Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und / oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest. Dadurch resultierende zusätzliche Kosten durch die Herausgabe oder Löschung der Daten sind vom Auftraggeber zu tragen.

2. Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Verantwortlichen, jedoch spätestens mit Beendigung der Leistungsvereinbarung, hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon im Rahmen der Vertragserfüllung gefertigte Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung des Verantwortlichen datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Ein Löschungsprotokoll ist dem Verantwortlichen auf Anforderung vorzulegen.

**Anmerkung:** Hier ist eine sprachliche Änderung notwendig, um »Datensätze« und »Eigentum« nicht zu vermengen.

**Formulierungsvorschlag:** Es besteht kein Zurückbehaltungsrecht für personenbezogene Daten die im Rahmen des AVV übertragen oder bereitgestellt wurden.

**Anmerkung und Ergänzungsvorschlag:** Dies sollte eine Verweigerungsmöglichkeit bei entgegenstehenden Rechten oder Pflichten des AV ergänzt werden.

**Anmerkung:** Diese Formulierung ist zu weitgehend. Sie sollte sich nur auf die Daten beziehen, die der AV im Rahmen des AVV erhalten hat, nicht zB auch auf die Korrespondenz rund um den Vertrag o.ä.

**Anmerkung:** Hier handelt es sich um unklare Terminologie; es sollte deutlich gemacht werden, dass nicht nur die aktive Zusendung sondern auch die Möglichkeit den Export der Daten auszulösen genügt.

**Formuleriungsvorschlag:** Statt »aushändigen« könnte »zur Verfügung stellen« eingesetzt werden.

3. Der Auftragsverarbeiter kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen bis zu deren Ende auch über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben. Für die nach Satz 1 aufbewahrten Daten gelten nach Ende der Aufbewahrungsfrist die Pflichten nach Absatz 2.

**Anmerkung:** Dies sollte durch »Weisung« ersetzt werden, da der Verantwortliche entscheidet, ob Daten herausgegeben oder gelöscht werden.

**Anmerkung:** Für die Löschung bedarf es mehr Flexibilität. Sofortige Löschung ist in komplexeren Systemen nicht möglich; außerdem können auch Daten betroffen sein, die der AV noch aus rechtlichen Gründen weiterhin speichern muss.

**Vorschlag:** Der Satz sollte ergänzt werden, »soweit nicht ohnehin die Pflicht zur Löschung besteht«. Außerdem sollte aufgrund des zeitlichen Moments eingefügt werden: »Im Zuge der Vertragsbeendigung und im Rahmen der vertraglichen Absprache zu ggf. Löschfristen«

**Anmerkung und Vorschlag:** Dies sollte flexibler gestaltet werden, da nicht jeder AV Löschprotokolle erstellt.

**Vorschlag:** »Bestätigung einer Löschung bzw. Vernichtung« statt »Protokoll«; »Auf Anforderung des Verantwortlichen wird der AV die Löschung bestätigen«

## § 8 Subunternehmen

1. Der Auftragsverarbeiter darf weitere Auftragsverarbeiter (Subunternehmen) nur mit vorheriger ausdrücklicher schriftlicher Zustimmung des Verantwortlichen in Anspruch nehmen. [Die zur Erfüllung dieses Vertrages hinzugezogenen Subunternehmen sind in der Anlage x im Einzelnen bezeichnet. Mit deren Beauftragung erklärt sich der Verantwortliche einverstanden]. Sofern es sich um eine allgemeine schriftliche Genehmigung handelt, informiert der Auftragsverarbeiter den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmen. Der Verantwortliche kann gegen derartige Änderungen Einspruch erheben. Dem Auftragsverarbeiter steht ein außerordentliches Kündigungsrecht des Hauptvertrages nach Maßgabe des Hauptvertrages – oder für den Fall, dass ein solches Kündigungsrecht im Hauptvertrag nicht eingeräumt wurde, ein außerordentliches Kündigungsrecht von 4 Wochen zum Monatsende – zu, wenn nach Auffassung des Auftragsverarbeiters der Verantwortliche die Einbindung des Unterauftragsverarbeiters und/oder Sub-Unterauftragsverarbeiters ohne wichtigen Grund verweigert oder dem Auftragsverarbeiter eine Leistungserbringung ohne den abgelehnten Unterauftragsverarbeiter und/oder Sub-Unterauftragsverarbeiters nicht möglich ist. Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienstleistungen. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

**Anmerkung:** Die verantwortliche Stelle sollte Subunternehmer nicht beliebig ablehnen dürfen. Zudem sollte eine Konsequenz regelt werden, wenn der Subunternehmer abgelehnt wird, aber der Auftragsverarbeiter den Subunternehmer einsetzen muss. Es könnte z.B. ein Kündigugsrecht für beide Parteien vorgesehen werden, dass sich auf den spezifischen Service bezieht. Es muss dabei berücksicht werden, dass im Falle einer Kündigung sonst im Zweifel eine neue ausschreibung erfolgen müsste.

Insbesondere sollte sich hier an Art. 28 DS-GVO orientiert werden.

Im Vergabeverfahren muss der Subunternehmer bereits bei Anmeldung fürs Verfahren benannt werden.

**Vorschlag für Formulierung:** Im Falle eines Widerspruchs des Auftraggebers treten die Parteien in individuelle Verhandlungen über die weitere Durchführung des Vertrages, insbesondere im Hinblick ob die Leistung – evtl. gegen erhöhtes Entgelt - mit dem bestehenden Subunternehmer weitergeführt wird oder ob die betroffenen Vertragsbestandteile aufgekündigt werden.

Wenn nach Absprache keine Einigung erzielt werden kann steht dem AV ein Kündigungsrecht für den Einzelservice zu, wenn die Leistungen nicht trennbar sind, ein Gesamtkündigungsrecht.

**Anmerkung:** Dies ist immer eine Ergänzung zu den EVB-IT Verträgen, dort werden auch jeweils die Regelungen zu Subunternehmern aufgenommen. Hier sollte darauf geachtet werden, dass es nicht zu widersprüchlichen Aussagen kommt bzw. darauf referenziert wird.

In den EVB-IT Verträgen sind die Wechsel von SubU deutlich differenzierter dargestellt. Dies sollte als Ausgangspunkt und Vorlage dienen.

Die Kündigung sollte jedenfalls nicht ohne Begründung abgelehnt werden dürfen; die Gründe für die Kündigung/den Wechsel müssen eine Rolle spielen.

**Gelöscht:** »unverzüglich«; Vorschlag zur Streichung

**Anmerkung:** Der Aufbau der Regelung ist unklar; insb. Bezüge im Absatz zu Situationen, wenn allgemeine Genehmigung zur Einsetzung von SubAV erteilt wird.

**Anmerkung:** Hier ist unklar, ob das Einspruchsrecht nur für Änderungen oder auch für die Hinzuziehung gelten soll. Gerade im Bereich standardisierter Leistungen ist ein Einspruchsrecht nicht umsetzbar, da die Leistungen nur einheitlich erbracht werden können.

**Anmerkung:** Hier bleibt die Rechtsfolge unklar; Die Kündigung des Vertrages sollte eine mögliche Rechtsfolge sein und benannt werden.

**Anmerkung:** Dieser Einspruch darf nicht auf sachfremden Erwägungen beruhen. Die Regelung zur Rechtsfolge fehlt und sollte aufgenommen werden.

**Anmerkung und Vorschlag:** Das Kündigungsrecht sollte sich nicht auf Hauptvertrag sondern auf Einzelservices beziehen.

**Vorschlag einer Ergänzung (siehe Änderungen im Text)**

**Anmerkung und Vorschlag:** Dies sollte ausdifferenziert werden auf Post- ,Transport- und Versandleistungen, Reinigungsleistungen.

**Vorschlag:** Ergänzung dahingehend, dass die mit der Auftragsleistung betrauten Subunternehmer nicht betroffen sein sollen von der Regelung.

**Anmerkung:** Hier werden zusätzlich -auslegbare und schwer abgrenzbare- Tätigkeitsfeder implementiert (u. E. eher praxisfern).

2. Wenn Subunternehmen durch den Auftragsverarbeiter eingeschaltet werden, hat der Auftragsverarbeiter zu gewährleisten, dass seine vertraglichen Vereinbarungen mit dem Subunternehmen so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter entspricht und alle vertraglichen und gesetzlichen Vorgaben beachtet werden; dies gilt insbesondere auch im Hinblick auf den Einsatz geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus der Verarbeitung.

**Vorschlag einer Änderung:** Begriffe, die auf eine Garantie im Rechtssinne mit der Folge einer unbeschränkten und verschuldensunabhängigen Haftung im Sinne von § 276 BGB hindeuten könnten, sollten vermieden werden.

3. Dem Verantwortlichen sind in der vertraglichen Vereinbarung mit dem Subunternehmen Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist der Verantwortlichen berechtigt, auf schriftliche Anforderung vom Auftragsverarbeiter Auskunft über die darin enthaltene Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmens zu erhalten.

**Vorschlag für Ergänzung:** Der Verantwortliche arbeitet ausschließlich mit Auftragsverarbeitern zusammen, welche nachweisbar hinreichende Garantien bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleisten kann. Der Nachweis der hinreichenden Garantien gilt bei Verfügbarkeit einer gültigen Zertifizierung zur Informationssicherheit durch eine akkreditierte Prüfstelle als erbracht, wie z.B. ISO 27001.

Können keine hinreichende Garantien aufgrund fehlender oder nicht mehr gültiger Zertifizierung zur Informationssicherheit erbracht werden, so kann der Verantwortliche sich jederzeit zu Prüfzwecken in den Betriebsstätten des Auftragsverarbeiters zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der gesetzlichen Vorgaben oder der zur Durchführung dieses Vertrages erforderlichen technischen und organisatorischen Erfordernisse überzeugen.

Falls der Auftragsverarbeiter Subunternehmen einsetzt, welche keine hinreichenden Garantien aufgrund fehlender oder nicht mehr gültiger Zertifizierung zur Informationssicherheit nachweisen können, sind dem Verantwortlichen in der vertraglichen Vereinbarung mit dem Subunternehmen Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen.

Hier könnte auch auf den separaten Paragraphen zu den Auditrechten Bezug genommen werden.

**Vorschlag:** Hier sollte der Prüfkatalog aufgenommen werden (z.B. BayLDF Standard Maßnahmenkatalog).

4. Kommt das Subunternehmen seinen datenschutzrechtlichen Verpflichtungen nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Subunternehmens. Der Auftragsverarbeiter hat in diesem Falle auf Verlangen des Verantwortlichen die Beschäftigung des Subunternehmens ganz oder teilweise zu beenden oder das Vertragsverhältnis mit dem Subunternehmen zu lösen, wenn und soweit dies nicht unverhältnismäßig ist.

**Vorschlag:** Der Auftraggeber verpflichtet sich, mit der zuständigen Aufsichtsbehörde des Auftraggebers – und soweit erforderlich – auch mit der zuständigen Aufsichtsbehörde des Auftraggebers im Rahmen der Ausübung der gesetzlichen Aufgaben und Pflichten der jeweiligen Aufsichtsbehörde in der rechtlichen Geboten- und Zulässigkeit zu kooperieren. XXX gilt entsprechend.

»Für Kontrollen der Aufsichtsbehörden gilt § 5 Absatz 4 entsprechend«

§ 29 III BDSG-neu einbeziehen:

**Vorschlag einer Ergänzung:** »Bei den Formulierung des § 9 ist der § 29 Abs. 3 BDSG-Neu zu berücksichtigen«

**§ 9 Datenschutzkontrolle**

Der Auftragsverarbeiter verpflichtet sich, der/dem Datenschutzbeauftragten des Verantwortlichen sowie der zuständigen Aufsichtsbehörde zur Erfüllung ihrer jeweiligen gesetzlichen zugewiesenen Aufgaben im Zusammenhang mit diesem Auftrag Zugang zu den üblichen Geschäftszeiten zu gewähren. Der Auftragsverarbeiter unterwirft sich zusätzlich zu der für ihn bestehenden gesetzlichen Datenschutzaufsicht der Kontrolle der für den Verantwortlichen bestehenden Datenschutzaufsicht (hier: die/der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) und der Kontrolle durch die/den Datenschutzbeauftragten des Verantwortlichen mit Ausnahme der Bereiche, die keinerlei Bezug zur Auftragserfüllung haben. Er duldet insbesondere Betretungs-, Einsichts- und Fragerechte der Genannten. Er wird seine Mitarbeiter anweisen, mit den Genannten zu kooperieren, insbesondere deren Fragen wahr-

**Anmerkung:** Die Regelung findet sich bereits in Art. 58 DSGVO.

**Mögliche Ergänzung:** Kann ein Auftragsverarbeiter eine gültige Zertifizierung zur Informationssicherheit, wie z.B. ISO 27001, nachweisen, so gelten die geeigneten Garantien als hinreichend nachgewiesen. Der Auftragsverarbeiter muss dann wiederum sicherstellen, dass seine Sub-Auftragsverarbeiter ebenfalls eine entsprechende Zertifizierung nachweisen können.

**Anmerkung:** Diese Regelung könnte dazu führen, dass eine Behörde ihre gesetzlich zugewiesenen Aufgaben überschreitet. Wir halten die Regelung für sehr fragwürdig.

**Anmerkung:** Dies könnte gestrichen werden (siehe vorstehende Anmerkungen).

**Anmerkung und Vorschlag:** Dieser Bereich muss im Rahmen der Audits in einer separaten Regelung geregelt werden. Auch der DSB der Aufsichtsbehörde kann kein jederzeitiges zusätzliches Auditrecht haben.

**Anmerkung:** Diese Pflichten sollten in dem bereits erwähnten zusätzlichen/separaten Abschnitt zu Vergütungen und Unterstützungsleistungen aufgenommen werden.

**Anmerkung:** Fraglich ob strafrechtliche Regelungen zB § 203, 206 StGB diesem Verlangen nicht entgegenstehen. (hier auch § 29 Abs. 3 BDG-Neu einbeziehen)

heitsgemäß und vollständig zu beantworten. Die nach Gesetz bestehenden Verschwiegenheitspflichten und Zeugnisverweigerungsrechte der Genannten bleiben davon unberührt.

**§ 10 Schlussbestimmungen**

1. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragsverarbeiters – 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.

**Vorschlag einer Ergänzung:** »oder Textform« sollte hier ergänzt werden.

**Vorschlag einer Anpassung:** »Änderung des Formerfordernisses sind nur gültig, wenn sie unter Referenzierung des Vertrages und dieser Vorschrift vereinbart werden.«

2. Sollten einzelne Regelungen dieser Vereinbarung unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

Hier sollte die BGH Rechtsprechung zur Formulierung von salvatorischen Klauseln beachtet werden.

| | |
|---|---|
| _____ | _____ |
| Datum, Ort | Datum, Ort |
| _____ | _____ |
| Unterschrift (Verantwortlicher) | Unterschrift (Auftragsverarbeiter) |
| _____ | _____ |
| Name, Vorname, Funktion | Name, Vorname, Funktion |

## Anhang »Technisch-organisatorische Maßnahmen«

zur Vereinbarung zur Auftragsverarbeitung vom [Datum]
zwischen XXXXX XXXX
und [Vertragspartner]

§ 5 der Vereinbarung zur Auftragsverarbeitung verweist zur Konkretisierung der technisch-organisatorischen Maßnahmen auf diesen Anhang.

**§ 1 Technische und organisatorische Sicherheitsmaßnahmen**
Die Vertragspartner sind verpflichtet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung der Daten im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person in angemessener Form gewährleistet ist.

**§ 2 Innerbehördliche oder innerbetriebliche Organisation des Auftragsverarbeiters**
Der Auftragsverarbeiter wird seine innerbehördliche oder innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Daten oder Datenkategorien geeignet sind.

**§ 3 Konkretisierung der Einzelmaßnahmen**
1. Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 32 DSGVO dienen:

Die untenstehende Tabelle entspricht der alten Anlage zu § 9 BDSG-alt. Hier sollte eine Anpassung erfolgen.

Statt eines Anhangs der sich am alten Muster orientiert schlagen wir vor, dass ein Annex konzipiert wird, der sich europaweit durchsetzen lässt.

| Nr. | Maßnahme | Umsetzung der Maßnahme |
|---|---|---|
| 1 | **Zutrittskontrolle**<br>Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren. | [Ergänzen] z.B. Zutrittskontrollsystem, Ausweisleser, Magnetkarte, Chipkarte, Schlüssel, Schlüsselvergabe, Werkschutz, Pförtner, Überwachungseinrichtung, Alarmanlage, Türsicherung |
| 2 | **Zugangskontrolle**<br>Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. | [Ergänzen] z.B. Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren (Beispiele: Kennwortverfahren, Automatisches Sperren, Einrichtung eines Benutzerstammsatzes pro User, Verschlüsselung von Datenträgern) |
| 3 | **Zugriffskontrolle**<br>Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. | [Ergänzen] z.B. Bedarfsorientierte Aus¬gestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Über¬wachung und Protokollierung, Verwen¬dung von dem Stand der Technik entspre¬chenden Verschlüsselungsverfah¬ren (Beispiele: differenzierte Berechtigungen wie Profile, Rollen etc. Auswertungen, Kenntnisnahme, Veränderung, Löschung) |
| 4 | **Weitergabekontrolle**<br>Es ist zu 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. | [Ergänzung] z.B. Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren, elektronische Signatur |
| 5 | **Eingabekontrolle**<br>Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. | [Ergänzen] z.B. Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung gewährleisten, etwa durch Protokollierungs- und Auswertungssysteme |
| 6 | **Auftragskontrolle**<br>Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können. | [Ergänzen] Abgrenzen der Kompetenz zwischen Verantwortlichem und Auftragsverarbeiter (Beispiel: eindeutige Vertragsgestaltung, Kriterien zur Auswahl des Auftragsverarbeiters, Kontrolle der Vertragsausführung) |

| Nr. | Maßnahme | Umsetzung der Maßnahme |
|---|---|---|
| 7 | **Verfügbarkeitskontrolle**<br>Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. | [Ergänzen] z.B. Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen, Maßnahmen zur Datensicherung (Beispiel: Backup-Verfahren, Spiegeln von Festplatten, unterbrechungsfreie Stromversorgung, Firewall, Notfallplan) |
| 8 | **Trennungskontrolle**<br>Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. | [Ergänzen] z.B. Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten, Mandantenfähigkeit, Funktionstrennung zwischen Produktion / Test |

2. Es ist ein Verfahren zu etablieren, das eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der zum Einsatz kommenden technischen und organisatorischen Maßnahmen durch die Vertragsparteien ermöglicht.

| | |
|---|---|
| _____ | _____ |
| Datum, Ort | Datum, Ort |
| _____ | _____ |
| Unterschrift (Verantwortlicher) | Unterschrift (Auftragsverarbeiter) |
| _____ | _____ |
| Name, Vorname, Funktion | Name, Vorname, Funktion |

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 1.900 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

**Bundesverband Informationswirtschaft,**
**Telekommunikation und neue Medien e.V.**

Albrechtstraße 10
10117 Berlin
**T** 030 27576-0
**F** 030 27576-400
bitkom@bitkom.org
**www.bitkom.org**

bitkom