

# Auftragsverarbeitungsvertrag (AVV)

|                    |  |
|--------------------|--|
| Version:           | 1.1 Auftraggeber Kunde – MSM Auftragsverarbeiter |
| Datum der Version: | 01.08.2024                                       |

# Standardvertragsklauseln

## ABSCHNITT I

### Klausel 1

#### Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von [zutreffende Option auswählen]:

OPTION 1: Artikel 28 Absätze 3 und 4 der 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 (Datenschutz-Grundverordnung)] oder

OPTION 2: Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG] sichergestellt werden.

b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.

c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.

d) Die Anhänge I bis IV sind Bestandteil der Klauseln.

e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

## **Klausel 2**

### **Unabänderbarkeit der Klauseln**

- a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.
- b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

## **Klausel 3**

### **Auslegung**

- a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.
- b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.
- c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

## **Klausel 4**

### **Vorrang**

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

## **Klausel 5 – fakultativ**

### **Kopplungsklausel**

- a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.

- b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.
- c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

## **ABSCHNITT II**

### **PFLICHTEN DER PARTEIEN**

#### **Klausel 6**

##### **Beschreibung der Verarbeitung**

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

#### **Klausel 7**

##### **Pflichten der Parteien**

##### **7.1. Weisungen**

- a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.
- b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

##### **7.2. Zweckbindung**

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

##### **7.3. Dauer der Verarbeitung personenbezogener Daten**

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

#### **7.4. Sicherheit der Verarbeitung**

- a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.
- b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

#### **7.5. Sensible Daten**

Falls die Verarbeitung personenbezogener Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

#### **7.6. Dokumentation und Einhaltung der Klauseln**

- a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.
- b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.
- c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine

Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

- d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.
- e) Die Parteien stellen der / den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

## 7.7. Einsatz von Unterauftragsverarbeitern

a)

OPTION 1: VORHERIGE GESONDERTE GENEHMIGUNG:

Der Auftragsverarbeiter darf keinen seiner Verarbeitungsvorgänge, die er im Auftrag des Verantwortlichen gemäß diesen Klauseln durchführt, ohne vorherige gesonderte schriftliche Genehmigung des Verantwortlichen an einen Unterauftragsverarbeiter untervergeben. Der Auftragsverarbeiter reicht den Antrag auf die gesonderte Genehmigung mindestens

[ZEITRAUM ANGEBEN]

vor der Beauftragung des betreffenden Unterauftragsverarbeiters zusammen mit den Informationen ein, die der Verantwortliche benötigt, um über die Genehmigung zu entscheiden. Die Liste der vom Verantwortlichen genehmigten Unterauftragsverarbeiter findet sich in Anhang IV. Die Parteien halten Anhang IV jeweils auf dem neuesten Stand.

OPTION 2: ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG:

Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens

4 Wochen

im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.



- c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.
- d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.
- e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

## **7.8. Internationale Datenübermittlungen**

- a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.
- b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

## **Klausel 8**

### **Unterstützung des Verantwortlichen**

- a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden

Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

- b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.
- c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:
- 1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;
  - 2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz- Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;
  - 3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;
  - 4) Verpflichtungen gemäß
    - OPTION 1: Artikel 32 der Verordnung (EU) 2016/679 oder
    - OPTION 2: Artikel 33 und Artikel 36 bis 38 der Verordnung (EU) 2018/1725.
- d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

## Klausel 9

### Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU)

2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

### 9.1. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b) bei der Einholung der folgenden Informationen, die gemäß

OPTION 1: Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 oder

OPTION 2: Artikel 34 Absatz 3 der Verordnung (EU) 2018/1725

in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

c) bei der Einhaltung der Pflicht gemäß

OPTION 1: Artikel 34 der Verordnung (EU) 2016/679 oder

OPTION 2: Artikel 35 der Verordnung (EU) 2018/1725,

die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

## 9.2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

- a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);
- b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;
- c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß

OPTION 1: Artikel 33 und 34 der Verordnung (EU) 2016/679 oder

OPTION 2: Artikel 34 und 35 der Verordnung (EU) 2018/1725

zu unterstützen.

## **ABSCHNITT III**

### **SCHLUSSBESTIMMUNGEN**

#### **Klausel 10**

##### **Verstöße gegen die Klauseln und Beendigung des Vertrags**

- a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.
- b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn
- 1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;
  - 2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;
  - 3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.
- c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.
- d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung

oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

# ANHANG I

## Liste der Parteien

### Verantwortliche(r):

[Name und Kontaktdaten des/der Verantwortlichen und gegebenenfalls des Datenschutzbeauftragten des Verantwortlichen]

Name: [wie in online-Beauftragung übergeben](#)

Anschrift: [wie in online-Beauftragung übergeben](#)

Name, Funktion und Kontaktdaten der Kontaktperson:  
[wie in online-Beauftragung übergeben](#)

### Auftragsverarbeiter:

[Name und Kontaktdaten des/der Auftragsverarbeiter/s und gegebenenfalls des Datenschutzbeauftragten des Auftragsverarbeiters]

Name: Marketing Service Magdeburg KG

Anschrift: Bahnhofstr. 17, 39122 Magdeburg

Name, Funktion und Kontaktdaten der Kontaktperson:  
Herr Lars Preuß, Prokurist; [lars.preuss@biberpost.de](mailto:lars.preuss@biberpost.de) , Tel. 0391 5999 315

## ANHANG II

### Beschreibung der Verarbeitung

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:

[wie in online-Beauftragung übergeben](#)

- Mitarbeiter
- Kunden
- Mitglieder Verantwortlicher
- Interessenten
- Werbekunden
- Hybridbriefempfänger
- Die konkreten Betroffenenkategorien ergeben sich aus dem jeweiligen Auftrag

Kategorien personenbezogener Daten, die verarbeitet werden:

[wie in online-Beauftragung übergeben](#)

- Name
- Anschrift
- elektronische oder telefonische Kontaktdaten
- Rechnungsdaten
- Verbrauchsdaten
- Bankverbindung
- Gesundheitsdaten
- Hybridbriefinhalte
- Die konkreten Arten der personenbezogenen Daten ergeben sich aus dem jeweiligen Auftrag.



Verarbeitete sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen:

Art der Verarbeitung: [wie in online-Beauftragung übergeben](#)

Der Auftragsverarbeiter druckt für den Auftraggeber personalisierte Sendungen im Rahmen von:

OPTION 1: Lettershopdienstleistungen

Daten der Sendungen / Inhalt und Anschrift werden über einen vereinbarten sftp Server durch den Verantwortlichen hochgeladen.

Die Aufbereitung und Druck der Sendungen, Sortierung für den Versand und Kuvertierung, Versandkostenoptimierung, Auflieferung zu Post,

In Einzelfällen werden anderer Übertragungswege, z.B. durch verschlüsselte Dateien per Mail vereinbart.

OPTION 2: Hybridpostdienstleistungen

Daten der Sendungen / Inhalt und Anschrift werden über das Hybridbriefportal durch den Verantwortlichen hochgeladen.

Die Aufbereitung und Druck der Sendungen, Sortierung für den Versand und Kuvertierung, Auflieferung zu Post,

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden: [wie in online-Beauftragung übergeben](#)

Erstellung von Abrechnungen

Erstellung von Werbeschreiben

Erstellung von personalisierten Rundschreiben

Die konkreten Zwecke ergeben sich aus dem jeweiligen Auftrag

Dauer der Verarbeitung: [wie in online-Beauftragung übergeben](#)

- einmalig
- wiederholend
- auftragsbezogen

Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben. [wie in online-Beauftragung übergeben](#)

- wie zuvor
- abweichend gilt:

## ANHANG III

### Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten

#### ERLÄUTERUNG:

Die technischen und organisatorischen Maßnahmen müssen konkret beschrieben werden; eine allgemeine Beschreibung ist nicht ausreichend.

Beschreibung der von dem/den Verantwortlichen ergriffenen technischen und organisatorischen Sicherheitsmaßnahmen (einschließlich aller relevanten Zertifizierungen) zur Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen Beispiele für mögliche Maßnahmen:

Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten

Maßnahmen zur fortdauernden Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung

#### **1. Vertraulichkeit**

Zutrittskontrolle gesichert durch:

- Empfang und Videoüberwachung der Einfahrten
- Schließsystem für Gebäude
- Sicherheitsschlösser
- räumlich abgetrennte Verarbeitung von Druckerzeugnissen mit personenbezogenen Daten
- zusätzliche Zutrittsberechtigung zum geschützten Produktionsbereich
- zentrale Schlüsselregelung (Ausgabekontrolle)
- Aufbewahrung Generalschlüssel bei Geschäftsführer
- Server abgegrenzt / gesichert
- Abschließen der Räume bei Arbeitsende
- Anwesenheitskontrollsystem
  
- Zutrittsregelung für betriebsfremde Personen (Anmeldung am Empfang)
- Begleitung betriebsfremder Personen innerhalb des Hauses

Zugangskontrolle ist realisiert über:

- Userbezogene Passwort Vergabe
- Passwortregel: keine trivial Passwörter, regelmäßiger Passwortwechsel)
- festgelegte Erstanmeldeprozedur
- gesicherte Aufbewahrung Administrator-Passwort

- Firewall (inkl. Aktualität und Administration)
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall

Zugriffskontrolle erfolgt:

- Programmspezifische Berechtigungskonzepte
- Einsatz von Aktenvernichtern bzw. Dienstleistern zur Akten- und Datenträgervernichtung
- Verwaltung der Rechte durch Systemadministrator
- Sichere (verschlossene) Aufbewahrung von Datenträgern für notwendige Datensicherungen
- keine Verwendung von mobilen Datenträgern im Austausch mit Kunden
- differenzierte Zugriffs- und Verarbeitungsmöglichkeiten in Hinsicht auf Lesen, Schreiben, Ändern und Löschen

## **2. Integrität**

Weitergabekontrolle realisiert durch:

- persönliche Datenträgerübergabe falls der Auftraggeber einen Datenträger übergeben möchte (nicht favorisiert; Übergabe über Datenserver hat Vorrang)
- Das unbefugte Lesen, Kopieren, Verändern oder Entfernen von Daten bei der Übertragung wird durch folgende Maßnahmen verhindert:
- Der Austausch der Daten erfolgt vorrangig mit verschlüsselten Verfahren
- Das Mitbringen von privaten Datenträgern und das unautorisierte Speichern und Weitergeben der Daten ist untersagt
- Fernwartung nur bei Anwesenheit Mitarbeiter
- Die Installation von nicht freigegebener Software ist durch technische Maßnahmen unterbunden.

Eingabekontrolle realisiert durch:

- Die Daten werden durch Auftraggeber zur Verfügung gestellt und über sichere Verbindungen (Hybridpostportal – Zugang, SFTP, Cloud) an den Prozessverantwortlichen übergeben.
- die Nachvollziehbarkeit von Eingabe, Freigabe, Änderung, Löschung von Daten wird systemseitig gewährleistet
- grundsätzlich werden nur Eingaben unter dem eigenen Benutzernamen vorgenommen
- schriftliche Auftragsunterlagen werden mit entsprechenden Vermerken
- weitergeleitet und mit Bezug zum Kunden und Auftrag abgelegt

### **3. Verfügbarkeit und Belastbarkeit**

Verfügbarkeitskontrolle realisiert durch:

- Speicherung der angelieferten Daten und Verarbeitungsschritte bis zum Abschluss der Bearbeitung
- anerkannte Maßnahmen zum Brandschutz (Einsatz Brandschutzbeauftragter)
- USV
- Firewall
- Virenschutz

Kurzfristige Wiederherstellbarkeit der Funktionsfähigkeit

- regelmäßige Sicherung von Datenträgern
- Backup-Regeln
- Wartungs- und Pflegeverträge der Anwendungen
- Dokumentation der Installation

Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen:

Realisiert durch:

- regelmäßige Sicherung von Datenträgern
- Backup-Regeln
- Wartungs- und Pflegeverträge der Anwendungen
- Dokumentation der Installation

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Führung, Ausbau und Pflege eines Datenschutz-Management mit regelmäßigen Bewertungen und Überarbeitungen.

Das Unternehmen hat einen Datenschutzbeauftragten bestellt.

## Maßnahmen zur Identifizierung und Autorisierung der Nutzer

- Die Daten werden durch Auftraggeber zur Verfügung gestellt und über sichere Verbindungen (Hybridpostportal – Zugang, SFTP, Cloud) an den Prozessverantwortlichen übergeben.
- die Nachvollziehbarkeit von Eingabe, Freigabe, Änderung, Löschung von Daten wird systemseitig gewährleistet
- grundsätzlich werden nur Eingaben unter dem eigenen Benutzernamen vorgenommen
- schriftliche Auftragsunterlagen werden mit entsprechenden Vermerken weitergeleitet und mit Bezug zum Kunden und Auftrag abgelegt

## Maßnahmen zum Schutz der Daten während der Übermittlung

- Der Austausch der Daten erfolgt vorrangig mit verschlüsselten Verfahren

## Maßnahmen zum Schutz der Daten während der Speicherung durch

### Zutrittskontrolle:

- Empfang und Videoüberwachung der Einfahrten
  - Schließsystem für Gebäude
  - Sicherheitsschlösser
  - räumlich abgetrennte Verarbeitung von Druckerzeugnissen mit personenbezogenen Daten
  - zusätzliche Zutrittsberechtigung zum geschützten Produktionsbereich
  - zentrale Schlüsselregelung (Ausgabekontrolle)
  - Aufbewahrung Generalschlüssel bei Geschäftsführer
  - Server abgegrenzt / gesichert
  - Abschließen der Räume bei Arbeitsende
  - Anwesenheitskontrollsystem
- 
- Zutrittsregelung für betriebsfremde Personen (Anmeldung am Empfang)
  - Begleitung betriebsfremder Personen innerhalb des Hauses

### Zugangskontrolle:

- Userbezogene Passwort Vergabe
- Passwortregel: keine trivial Passwörter, regelmäßiger Passwortwechsel
- festgelegte Erstanmeldeprozedur
- gesicherte Aufbewahrung Administrator-Passwort
- Firewall (inkl. Aktualität und Administration)
- Einsatz von Anti-Viren-Software

- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall

Zugriffskontrolle:

- Programmspezifische Berechtigungskonzepte
- Einsatz von Aktenvernichtern bzw. Dienstleistern zur Akten- und Datenträgervernichtung
- Verwaltung der Rechte durch Systemadministrator
- Sichere (verschlossene) Aufbewahrung von Datenträgern für notwendige Datensicherungen
- keine Verwendung von mobilen Datenträgern im Austausch mit Kunden
- differenzierte Zugriffs- und Verarbeitungsmöglichkeiten in Hinsicht auf Lesen, Schreiben, Ändern und Löschen

Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden, realisiert durch:

Zutritts, Zugangs- und Zugriffskontrollen

Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen

Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration

- Backup-Regeln
- Wartungs- und Pflegeverträge der Anwendungen
- Dokumentation der Installation

Maßnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit

Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten

- Führung, Ausbau und Pflege eines Datenschutz-Management mit regelmäßigen Bewertungen und Überarbeitungen

Maßnahmen zur Gewährleistung der Datenminimierung

- keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers und die Bekanntgabe der Weisungen des Auftraggebers an das eingesetzte Personal.

#### Maßnahmen zur Gewährleistung der Datenqualität

- keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers und die Bekanntgabe der Weisungen des Auftraggebers an das eingesetzte Personal.

#### Maßnahmen zur Gewährleistung einer begrenzten Vorratsdatenspeicherung

- keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers und die Bekanntgabe der Weisungen des Auftraggebers an das eingesetzte Personal.

#### Maßnahmen zur Gewährleistung der Rechenschaftspflicht

- Führung, Ausbau und Pflege eines Datenschutz-Management mit regelmäßigen Bewertungen und Überarbeitungen
- Führung von Verarbeitungsübersichten

#### Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung

- keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers und die Bekanntgabe der Weisungen des Auftraggebers an das eingesetzte Personal.

Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch die spezifischen technischen und organisatorischen Maßnahmen zu beschreiben, die der (Unter-)Auftragsverarbeiter zur Unterstützung des Verantwortlichen ergreifen muss.

Beschreibung der spezifischen technischen und organisatorischen Maßnahmen, die der Auftragsverarbeiter zur Unterstützung des Verantwortlichen ergreifen muss.

- Sicherstellung der Durchsetzung der vertraglichen Regelungen zwischen Verantwortlichem und Auftragsverarbeiter gegenüber den Unterauftragnehmer(n)
- Datenübermittlungen vorrangig über verschlüsselte Verfahren
- Vorhalten eigener Backup-Systeme
- Einsatz von:  
Firewall (inkl. Aktualität und Administration)  
Einsatz von Anti-Viren-Software



## **ANHANG IV**

### **Liste der Unterauftragsverarbeiter**

#### **ERLÄUTERUNG:**

Dieser Anhang muss im Falle einer gesonderten Genehmigung von Unterauftragsverarbeitern ausgefüllt werden (Klausel 7.7 Buchstabe a, Option 1).

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

P2 Die Zweite Post GmbH & Co. KG,

Hessenring 13

64546 Mörfelden-Walldorf

Ansprechpartner: Geschäftsführer Florian Jungmeier

Kontaktdaten: Telefon 06105-96778-0, Mail: kontakt@die-zweite-post.de

Verarbeitung: Entwicklung und technische Betreuung Hybridbriefportal

KOCH-DRUCK GmbH & Co. KG

Am Sülzegraben 28

38820 Halberstadt

Funktion und Kontaktdaten der Kontaktperson:

Geschäftsführung:

Anja Koch anja.koch@koch-druck.de Tel: 03941/6900-71

Verarbeitungen:

OPTION 1: Lettershopdienstleistungen

Lettershop, Druckdienstleistungen, Kuvertierung, Portooptimierung und Auflieferung Post

Post- und Logistikzentrum GmbH

Delitzscher Straße 65

06112 Halle/Saale

E-Mail: poststelle2.0@mz.de

Telefon: 0345 565-2488

Ansprechpartner: Herr Steffen Dietrich

Verarbeitungen:

OPTION 1: Lettershopdienstleistungen

Lettershop, Druckdienstleistungen, Kuvertierung, Portooptimierung und Auflieferung Post

OPTION 2: Hybridpostdienstleistungen

Ausdruck der Aussendungen über Hybridbriefportal, Auflieferung Post