

Anlage 2 - Auftragsverarbeitungsvertrag

Standardvertragsklauseln

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

- a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von 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) 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

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) 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 vier 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 gem. Art. 32 der Verordnung (EU) 2016/679.

- 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 Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 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 Artikel 34 der Verordnung (EU) 2016/679, 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 Artikel 33 und 34 der Verordnung (EU) 2016/679 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:	
Anschrift:	
Name, Funktion und Kontaktdaten der Kontaktperson:	
Name, Funktion und Kontaktdaten des Datenschutzbeauftragten:	
Unterschrift und Beitrittsdatum:	

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

Name:	SimplyDelivery GmbH
Anschrift:	Wilhelm-Kabus-Str. 70, Haus 34.3 10829 Berlin
Name, Funktion und Kontaktdaten der Kontaktperson:	Geschäftsführer: Björn Wisnewski Ronny Rohland André Wenzel Tel.: +49 (0) 3378.5100622206 E-Mail: info@simplydelivery.de
Name, Funktion und Kontaktdaten des Datenschutzbeauftragten:	DataSolution LUD GmbH Kay Kühnel

gten:	Tel.: +49 (0) 3378.829107 E-Mail: mail@ds-lud.de
Unterschrift und Beitrittsdatum:	

ANHANG II

Beschreibung der Verarbeitung

Bitte kreuzen Sie an, wo es zutrifft!

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

- Kunden des Auftraggebers
- Auftraggeber (Ansprechpartner, Mitarbeiter)
- Geschäftspartner, Lieferanten (Ansprechpartner)
- Interessierte Parteien

Kategorien personenbezogener Daten, die verarbeitet werden

- Bestelldaten: Tag, Uhrzeit, Art der Bestellung, Zahlungsarten, Produkte, Ort, Gerät oder Kanal, über den die Bestellung getätigt wurde, Daten zur Bestellhistorie, Sonderwünsche, kundenbezogene Gutscheindaten, personalisierte Bonusdaten (Bonuspunkte).
- Personenbezogene Daten (Kunden): Vorname, Nachname, Lieferadressen, Telefonnummer, Kundennummer, Daten zur Bestellhistorie, ggf. E-Mail-Adresse, ggf. Geburtsdatum.
- Mitarbeiterverwaltung: Vorname, Nachname, Adresse, Personalnummer, Arbeitszeiten, An- und Abwesenheitszeiten, Urlaubsdaten, Abrechnungsdaten, Position, Beruf, Qualifikation, Lohn- und Gehaltsdaten, Steuerdaten, Sozialversicherungsdaten, Konfessionsdaten, Gesundheitsdaten, Bank- und Kreditkartendaten, Arbeitsmittel- und Arbeitskleidungsdaten, Systemzugangsdaten, Endgerätedaten, Standortdaten, Geofence-Daten
- Bestandsverwaltung: Firma, Adresse, Kontaktdaten, Ansprechpartner, Kundennummer, Rechnungsdaten, Auftragsdaten, Vertragsdaten
- Websites/App: Metadaten, Server-Logfile-Daten, Benutzerdaten, Anmeldedaten

Sensible Daten, die verarbeitet werden (falls zutreffend), und angewandte Beschränkungen

oder Garantien, die der Art der Daten und den damit verbundenen Risiken in vollem Umfang Rechnung tragen, wie z. B. strikte Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnung des Zugangs zu den Daten, Beschränkungen für die Weitergabe oder zusätzliche Sicherheitsmaßnahmen.

Daten aus der Mitarbeiterverwaltung und der Dokumentenablage

Art der Verarbeitung

- SimplyCrew - Personalverwaltung (digitale Mitarbeiterakte)
- SimplyCall - Callcenter (Entgegennahme von Kundenaufträgen und Weiterverarbeitung)
- SimplyDrive - DriverApp (automatische Routenplanung für Fahrer und Filialen)
- SimplyGoods - Warenwirtschaft (Buchung aller Warenverbräuche in Echtzeit)
- SimplyKiosk - Selbstbedienungsterminal (Bestell- und Bezahlmöglichkeit vor Ort)
- SimplyKitchen - Küchenmanager (Planung, Erfassung und Auswertung von Arbeitsabläufen im Küchenbereich)
- SimplyManager - Store Management (zentraler Zugriff und Verwaltung von Restaurants und Lieferdiensten)
- SimplyPOS - Kassensystem (Buchhaltungssystem mit Schnittstellen zum Finanzamt)
- SimplyShop - Webshop & App (Verkaufsplattform für Kundenbestellungen)
- SimplyLoyalty - Bonusprogramm (Kundenbindungsprogramm)

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden

Gegenstand dieser Vereinbarung ist die Erbringung von Dienstleistungen gemäß dem zwischen dem Auftraggeber und dem Auftragnehmer geschlossenen Hauptvertrag. Er betrifft insbesondere die Erfassung und Verarbeitung von Lieferaufträgen und der damit verbundenen personenbezogenen Daten.

Dauer der Verarbeitung

Die Dauer des Vertrages richtet sich nach der im Hauptvertrag vereinbarten Laufzeit und endet mit dem Ablauf des Hauptvertrages. Soweit gesetzliche Aufbewahrungsfristen eine darüber hinausgehende Datenverarbeitung erfordern, endet sie erst mit Ablauf dieser Aufbewahrungsfristen.

Im Falle der Verarbeitung durch (Unter-)Auftragsverarbeiter müssen auch der Gegenstand, die Art und die Dauer der Verarbeitung angegeben werden. Bitte beachten Sie Anhang IV.

ANHANG III

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

Vorgabe	erfüllt
Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)	
1. Zutrittskontrolle (Bürogebäude, Büroräume, ...)	
1.1. Betriebsgelände / Bürogebäude	
1.1.1. Wachpersonal	zT
1.1.2. Bewegungsmelder	X
1.1.3. Alarmanlage	-
1.1.4. Videoüberwachung	-
1.2. Überwachung innerhalb des Gebäudes	
1.2.1. Wachpersonal	-
1.2.2. Bewegungsmelder	-
1.2.3. Alarmanlage	-
1.2.4. Videoüberwachung	-
1.3. Absicherung Zutritt	
1.3.1. sichere verschließbare Türen, Türschlösser	X
1.3.2. Sicherheitsschlösser	X
1.3.3. Generalschlüsselanlage	X
1.3.4. Notausgang (nur von innen zu öffnen)	X
1.3.5. Stark eingeschränkte Zutrittsrechte Serverraum	nR
1.3.6. Serverräume abgegrenzt (Sperrbereich)	nR
1.3.7. Server in abschließbaren Serverschränken	nR
1.4. Schriftliche Festlegungen zur Zutrittsberechtigung	
1.4.1. Ausweisregelung	X
1.4.2. Besucherregelungen	-
1.4.3. Trennung von Bearbeitungs- und Publikumszonen	X
1.4.4. Schlüsselregelung	X
1.4.5. Quittierung der Schlüsselausgabe	X

2. Zugangskontrolle (Netzwerkanmeldung)	
2.1. Passwortverfahren	
2.1.1. Authentifikation mit Benutzer + Passwörter	x
2.1.2. Biometrische Authentifikation	-
2.1.3. Zwei-Faktoren-Authentifikation	-
2.1.4. Forderung eines Zeichen-Mixes (Groß- und Kleinbuchstaben, Zahl, Sonderzeichen)	x
2.1.5. Mindestlänge 8 Zeichen	x
2.1.6. Erstanmeldeprozedur (Änderung Startpasswort erzwungen)	x
2.1.7. Bildschirmschoner bei Pausen mit Passwort-Aktivierung	X
2.1.8. Zugangssperre nach festgelegter Anzahl von Fehlversuchen	-
2.1.9. Passwortgenerationen mind. 5	-
2.1.10. Erstellen und Verwalten von Benutzerberechtigungen	x
2.1.11. Keine „Gruppen-Passwörter“	x
2.2. Protokollierung des Zugangs (An-/Abmeldung)	x
2.3. Verschlüsselung von Netzwerken/Dateiverzeichnissen	x

3. Zugriffskontrolle (Anwendungen)	
3.1. Berechtigungskonzept und Zugriffsrechte	
3.1.1. Authentifikation mit Benutzer + Passwörter	X
3.1.2. Biometrische Authentifikation	-
3.1.3. Zwei-Faktoren-Authentifikation	X
3.1.4. Forderung eines Zeichen-Mixes (Groß- und Kleinbuchstaben, Zahl, Sonderzeichen)	X
3.1.5. Mindestlänge 12 Zeichen	X
3.1.6. Sperrung bei wiederholter Falscheingabe	-
3.1.7. Berechtigungskonzept	X
3.1.8. Rollendefinition	X
3.1.9. Differenzierte Berechtigungen (Daten, Anwendungen)	X
3.1.10. Verwaltung der Benutzerrechte durch Systemadministratoren	X
3.1.11. Begrenzung Anzahl Administratoren auf das „Notwendigste“	X
3.2. Festlegung von Verantwortlichkeiten zum Schutz von Informationen	X
3.3. Inventarisierung sämtlicher Komponenten	X

4. Trennungskontrolle	
4.1. Festlegung von Datenbankrechten	X
4.2. Getrennte Datenbanken	X
4.3. Logische Mandantentrennung (softwareseitig)	X
4.4. Bedarfsgerechte Trennung in Netzwerken	X
4.5. Trennung von Kundendaten (Zugriffsrechte)	X

5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO)	
<p>Wo dies möglich und zweckmäßig ist, erfolgt die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können; dies gilt nicht, sofern eine Einwilligung der spezifischen Person eingeholt wurde. Diese zusätzlichen Informationen werden gesondert aufbewahrt und unterliegen entsprechenden technischen und organisatorischen Maßnahmen.</p>	

Integrität (Art. 32 Abs. 1 lit. b DSGVO)	
6. Weitergabekontrolle	
6.1. Datenleitung über https (Onlinedienste)	X
6.2. Zugriff von außen VPN	zT
6.3. E-Mail-Verschlüsselung (S/MIME, REDDCRYPT, ...)	X
6.4. SSL-Verschlüsselung bei Web-Access	X
6.5. Verschlüsselung von Datenträgern/Notebooks	zT

7. Eingabekontrolle	
7.1.1. Vergabe von Rechten auf Basis Berechtigungskonzept	X
7.1.2. Protokollierung der Eingabe, Änderung und Löschung von Daten	X
7.1.3. Protokollierung An- und Abmeldung	X
7.1.4. Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)	X

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)	
8. Verfügbarkeitskontrolle	
8.1. Brandschutzeinrichtungen	
8.1.1. Feuerlöscher im Serverraum	nR
8.1.2. Rauch- oder Brandmelder	nR
8.1.3. Rauchverbot in Server- und PC-Arbeitsräumen	x
8.2. Stromversorgung	
8.2.1. Unterbrechungsfreie Stromversorgung (USV)	nR
8.2.2. Überspannungsschutzeinrichtungen	
8.3. Klimaversorgung Serverraum	
8.4. Back-up & Recovery-Verfahren	
8.4.1. für Server inkl. Regelung und Umsetzung	x
8.4.2. für Informationen in Netzwerken/Diensten	
8.4.3. Fähigkeit, die Verfügbarkeit der Daten sowie den Zugang rasch wiederherzustellen (Art. 32 Abs. 1 lit. c DSGVO)	x
8.4.4. Spiegeln von Server-Festplatten (z.B. RAID)	x
8.5. Virenschutz	
8.5.1. Virenschutzprogramm im Einsatz	-
8.5.2. Schutzprogramm(e) erkennt bekannte Schadsoftware	x
8.5.3. Schutzprogramm(e) erkennt unbekannte Schadsoftware (Heuristik)	x
8.5.4. Update der Virenschutzprogramme	-
8.6. Firewall	
8.7. Sichere Hinterlegung von Notfallpasswörtern	
8.8. Aufbewahrungsmodalitäten von Back-up's (Safe, getrennter Brandabschnitt)	
8.9. Geeignete Archivierungsmöglichkeiten	

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO, Art. 25 Abs. 1 DSGVO)	
9. Auftragskontrolle	
9.1. Sorgfältige Auswahl der Auftragnehmer sowie regelmäßige Kontrolle	
9.1.1. Sorgfältige Auswahl des Auftragnehmers (insbes. Hinsichtlich Datensicherheit)	x

9.1.2.	Auftragnehmer benennt Datenschutzbeauftragten oder -verantwortlichen /Prüfung anhand Zertifikat)	x
9.1.3.	Prüfung Datensicherheitsmaßnahmen (techn. u. org. Maßnahmen, Zertifikate/Gütesiegel, Datensicherheitskonzept)	x
9.2.	Schriftlicher Abschluss der notwendigen Vereinbarungen	
9.2.1.	Eindeutige Vertragsgestaltung mit Partnern	x
9.2.2.	Eindeutige Vertragsgestaltung mit Nachunternehmer	x
9.2.3.	Vereinbarung wirksamer Kontrollrechte ggü. Auftragnehmer	x
9.2.4.	Schriftliche Weisungen an den Auftragnehmer (z.B. innerhalb der Vereinbarung zur Datenverarbeitung im Auftrag)	x
9.2.5.	Verpflichtung der Mitarbeiter des Auftragnehmers auf die Vertraulichkeit	x
9.2.6.	Festlegung von Kontrollmöglichkeiten beim Auftragnehmer	x
9.2.7.	Formalisierte Auftragserteilung (Weisungsbefugnis Auftraggeber)	x
9.3.	Unternehmen ist selbst als Auftragnehmer tätig	-

10.	Datenschutz-Management	
10.1.	Datenschutzfreundliche Voreinstellung (Art. 25 Abs. 2 DS-GVO)	
10.1.1.	Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	x
10.1.2.	Einfache Ausübung des Widerspruchsrechts des Betroffenen durch techn. Maßnahmen (Löschung, Sperren)	x
10.2.	Incident-Response-Management	
10.2.1.	Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/Datenpannen	x
10.2.2.	Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen	x
10.2.3.	Einbindung Datenschutzbeauftragten in Sicherheitsvorfälle und Datenpannen	x
10.2.4.	Dokumentation von Sicherheitsvorfällen und Datenpannen	x
10.2.5.	Formalisierter Prozess und Verantwortlichkeiten zur Nacharbeitung von Sicherheitsvorfällen und Datenpannen	x
10.2.6.	Schulung und Belehrung der Mitarbeiter zu Datensicherheit und Verhalten bei Sicherheitsvorfällen und Datenpannen	x
10.3.	Organisationskontrolle	
10.3.1.	Bestellung Datenschutzbeauftragten	x
10.3.2.	Bestellung IT-Sicherheitsbeauftragten	x
10.3.3.	Schriftliche Verpflichtung der Mitarbeiter auf die Vertraulichkeit	x
10.3.4.	Regelmäßige Schulungen der Mitarbeiter in Datenschutz und Informationssicherheit	x
10.3.5.	Erfüllung der Informationspflichten gem. Artt. 13, 14 DSGVO	x

10.3.6. Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen	x
10.3.7. Formalisierter Prozess zur Bearbeitung von Löschanfragen	x
10.3.8. Löschkonzept	x
10.3.9. Formalisierter Prozess zur Bearbeitung von Widersprüchen/Widerrufen	x
10.3.10. Führen eines Verzeichnisses für Verarbeitungstätigkeiten	x
10.3.11. Risiko- und Schutzbedarfsermittlung zur Verarbeitungstätigkeit	x
10.3.12. Durchführung von Datenschutz-Folgenabschätzungen bei Anforderung	x
10.3.13. Führen eines Verzeichnisses für Datenverarbeitung im Auftrag	x
10.3.14. aktuelle und freigegebene Datenschutz- und IT-Sicherheitsrichtlinien	x
10.3.15. Durchführung von Datenschutz-Audits	x

Legende

X	erfüllt
-	nicht erfüllt
zT	teilweise
nR	nicht relevant

ANHANG IV

Liste der Unterauftragsverarbeiter

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

1.	Name:	Amazon Web Service (AWS)
	Anschrift:	<p>Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy, L-1855 Luxembourg Sitz der Gesellschaft: L-1855 Luxemburg eingetragen im Luxemburgischen Handelsregister unter R.C.S. B186284</p> <p>Amazon Web Services EMEA SARL, Niederlassung Deutschland Marcel-Breuer-Str. 12, 80807 München, Deutschland Sitz der Zweigniederlassung: München eingetragen im Handelsregister des Amtsgerichts München unter HRB 242240, USt-ID: DE317013094</p> <p>Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 United States</p> <p>Amazon Web Services, Inc. ist eine nach dem Recht des Staates Delaware gegründete und registrierte Gesellschaft. Registernummer: 4152954, Secretary of State, State of Delaware.</p> <p>Steuernr.: 204938068</p>
	Name, Funktion und Kontaktdaten der Kontaktperson:	Keine direkten Kontaktpersonen, alles anonyme Webservices.
		<p>Computing, Datenprozessierung und Datenspeicherung am AWS Standort Frankfurt am Main, Deutschland und für alle in Deutschland und Europa anfallenden Daten, insbesondere im Kundenauftrag.</p> <p>Computing, Datenprozessierung und Datenspeicherung am Standort Toronto, Kanada für alle in Kanada anfallenden Daten, insbesondere im Kundenauftrag.</p>

2.	Name:	YOPESO GmbH
	Anschrift:	Königstraße 31 70173 Stuttgart
	Name, Funktion und Kontaktdaten der Kontaktperson:	David Rodriguez CEO david.rodriquez@yopeso.com Berlin, DE Cluj-Napoca, RO Chisinau, MD Kota Kinabalu, MY Adrian Morutan Engineering Manager adrian.morutan@yopeso.com 44 Clinicilor street, 400006 Cluj-Napoca, Romania
	YOPESO erbringt Programmier-Leistungen für SimplyDelivery. Die Mitarbeiter von YOPESO haben keinen Zugriff auf Live-Daten von Kunden, Partnern oder Auftraggebern und verarbeiten keine Kunden-Daten. YOPES erhält ausschließlich Zugriff auf für die Erbringung notwendige Code-Teile.	

3.	Name:	Zoho Corporation Pvt. Ltd.
	Anschrift:	Estancia IT Park, Plot No. 140 & 151, GST Road 603 202 Chengalpattu Taluk, Kanchipuram District
	Name, Funktion und Kontaktdaten der Kontaktperson:	Natalie Söll Geschäftsführerin Damaschkestr. 1 95615 Marktredwitz zoho@zoftware.org
	Verarbeitung von Daten von Mitarbeitern bezüglich Personalwesen (Stammdaten, Urlaub & Krankheit, Abrechnungsdaten), interner und externer Kommunikation (Mails, Sofort-Nachrichten) und intern Daten zur Projektsteuerung. Ebenfalls alle Buchhaltungsdaten (Rechnungsstellung) und Kundendaten (CRM / Sales & Marketing).	

4.	Name:	kreuzwerk GmbH
	Anschrift:	info@kreuzwerker.de Fon: +49 30 609 8388 0 Fax: +49 30 609 8388 99 Ritterstraße 12-14 Hof 2, Aufgang 4, 3. OG 10969 Berlin
	Name, Funktion und Kontaktdaten der Kontaktperson:	Manuel Vogel Geschäftsführer Tel: +49 30 609 8388 0
	Unterstützung bei der Optimierung der aws Infrastruktur	