Fastdocs

Standardvertragsklauseln 2021/915

Übermittlung Verantwortlicher zu Auftragsverarbeiter

Inhaltsverzeichnis

ABSCHNITT I ... 3
1. Klausel 1 – Zweck und Anwendungsbereich ... 3
2. Klausel 2 – Unabänderbarkeit der Klauseln ... 3
3. Klausel 3 – Auslegung ... 3
4. Klausel 4 - Vorrang ... 3
5. Klausel 5 – Kopplungsklausel (nicht besetzt) ... 4
ABSCHNITT II ... 4
6. Klausel 6 – Beschreibung der Verarbeitung ... 4
7. Klausel 7 – Pflichten der Parteien ... 4
8. Klausel 8 – Unterstützung des Verantwortlichen ... 6
9. Klausel 9 – Meldung von Verletzungen des Schutzes personenbezogener Daten ... 7
ABSCHNITT III ... 8
10. Klausel 10 – Verstöße gegen die Klauseln und Beendigung des Vertrags ... 8
ANHANG I – Liste der Parteien ... 10
ANHANG II – Beschreibung der Verarbeitung ... 11
(1) Art und Zweck(e) der Verarbeitung ... 11
(2) Kategorien der personenbezogenen Daten ... 11
(3) Kategorien betroffener Person ... 11
(4) Dauer der Verarbeitung ... 11
ANHANG III – Technische und organisatorische Maßnahmen des Auftragnehmers ... 12
(1) Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO) ... 12
(2) Integrität (Art. 32 Abs. 1 lit. b DSGVO) ... 15
(3) Verfügbarkeit, Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO) Wiederherstellbarkeit (Art.32 Abs. 1 lit. c DSGVO) ... 16
(4) Verfahren zur regelm. Überpr., Bew. und Evaluierung (Art. 32 Abs. 1 lit. d & Art. 25 Abs. 1 DSGVO) ... 18
ANHANG IV – Unterauftragnehmer ... 20
Anhang V - Vereinbarung über die Verpflichtung zur Wahrnehmung des Berufsgeheimnisses nach §§ 203 und 204 StGB einschließlich Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung (§62a StBerG ... 22
(1) Der Auftraggeber belehrt die Firma ... 22
(2) Der Auftragsverarbeiter verpflichtet sich gegenüber dem Auftraggeber sowie den bei Auftraggeber tätigen Berufsgeheimnisträgern wie folgt: ... 22

ABSCHNITT I

1. 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 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 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 erfüllt werden.

2. 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.

3. Klausel 3 – Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 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 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

4. 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.

5. Klausel 5 – Kopplungsklausel (nicht besetzt)

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

6. 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.

7. 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 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 um-

fasst 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 personenbezogene 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 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 30 Tage 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 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 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.

8. 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:

d) 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;

e) 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;

f) 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;

g) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.

h) 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.

9. 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 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] oder, 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.

d) 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

10. 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 – 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 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 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

Verantwortlicher / Auftragsverarbeiter:

Name: Fastdocs.de GmbH (Fastdocs Crew)

Anschrift: Zeppelinstraße 1, 42781 Haan, Deutschland

Name, Funktion und Kontaktdaten der Kontaktperson: Evelyn Krämer, Geschäftsführerin der Fastdocs.de GmbH, Zeppelinstraße 1, 42781 Haan, E-Mail: emmy@fastdocs.de

_____

Unterschrift

Datenschutzbeauftragter des Auftragsverarbeiters:

Name: secjur GmbH

Anschrift: Steinhöft 920459 Hamburg, Deutschland

Name, Funktion und Kontaktdaten der Kontaktperson: Niklas Hanitsch, secjur GmbH, Steinhöft 920459 Hamburg, Deutschland, Telefon: +49 40 228 599 520, E-Mail: dsb@secjur.com

ANHANG II – Beschreibung der Verarbeitung

(1) Art und Zweck(e) der Verarbeitung

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

Zurverfügungstellung des Dienstes BoardMeOn (Service der Fastdocs.de GmbH), der einen Online-Fragebogen zur schnellen und fehlerfreien Erfassung von Personalstammdaten für Unternehmen. Mittels eines Online-Fragebogens werden die zur Durchführung / Begründung des Arbeitsvertrages notwendigen Daten im Bereich Personal direkt beim Arbeitnehmer erhoben und nach Fertigstellung an den Arbeitgeber sowie den Arbeitnehmer weitergeleitet. Die Weiterleitung erfolgt per verschlüsselter E-Mail oder, wenn eine von BoardMeOn (Service der Fastdocs.de GmbH) unterstützte Software genutzt wird, per Softwareschnittstelle direkt in die Unternehmenssoftware.

(2) Kategorien der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

Personalstammdaten von Beschäftigten, die zur Begründung und Durchführung eines Beschäftigungsverhältnisses erforderlich sind. Hierbei handelt es sich in der Regel um folgende Daten:

<u>Persönliche Angaben:</u>

Name des Arbeitgebers, Name und Vorname des Mitarbeiters, Personalnummer, Anschrift, Postleitzahl, Ort, Geb.-Datum, Geburtsort, Geburtsland, Geschlecht, Familienstand, Staatsangehörigkeit, Sozialversicherungsnummer, Bankdaten, Schulbildung, Berufsbildung

<u>Beschäftigungsdaten:</u>

Eintrittsdatum, ausgeübte Tätigkeit, Beschäftigungsort, Status bei Beginn der Beschäftigung, Wöchentliche Arbeitszeit, Steueridentifikationsnummer, Krankenversicherung, Name der Krankenversicherung, Antrag zur Befreiung Rentenversicherungspflicht, Gehaltsdaten, Angaben von weiteren Beschäftigungen.

(3) Kategorien betroffener Person

Beschäftige des Auftraggebers.

(4) Dauer der Verarbeitung

Entspricht der Laufzeit des Hauptvertrages.

ANHANG III – Technische und organisatorische Maßnahmen des Auftragnehmers

Die technischen und organisatorischen Maßnahmen schließen gem. Art. 32 Abs. 1 S.2 lit. a) -c) unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

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

(1) Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren.

a) Vom Auftragnehmer umgesetzte Maßnahmen:

Der Zutritt in das Bürogebäude wird über ein Transponderschließsystem geregelt. Berechtigte Personen – in der Regel Mitarbeiter - haben grundsätzlich nur in die Bereiche Zutritt, die sie im Rahmen ihrer Aufgabenerfüllung benötigen. Funktionsbereiche des Unternehmens. Bei Verlust eines Transponders wird das Zutrittsmittel unverzüglich deaktiviert. Es liegt eine Dokumentation über die Vergabe und den Entzug von Zugangsberechtigungen und -mitteln liegt vor.

Das Bürogebäude verfügt über eine Alarmanlage mit Aufschaltung zu einem Sicherheitsdienst (Siemens).

Die Server befinden sich in externen Rechenzentren.

b) Externes Rechenzentrum im Rahmen eines Hostings

Die Datenverarbeitungsanlagen, insbesondere Fileserver, werden im Rahmen eines Hostings in externen Hochsicherheitsrechenzentren betrieben wie in ANHANG IV – Unterauftragnehmer beschrieben aufgeführt. Das Rechenzentrum ist 24/7 durch einen Wachdienst gesichert.

Die Eingänge und Sicherheitsbereiche des Rechenzentrums sind Videoüberwacht.

Es existiert eine Zugangskontrollanlage (ZKA). Ein Einbruchschutz ist mehrstufig gegeben, dabei werden alle sicherheitskritischen Bereiche mittels einer Einbruchmeldeanlage (EMA) überwacht. Die Anlage wird von einer Haupt- und einer Zusatzenergiequelle gespeist. Die Alarme werden an eine ständig besetzte Sicherheitszentrale übertragen.

Der Zutritt zu den Datenverarbeitungsanlagen ist nur für bestimmte berechtigte Personen möglich, die im Zuge von administrativen Tätigkeiten den Zugang benötigen.

Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Vom Auftragnehmer umgesetzte Maßnahmen:

a) Authentisierung

Die Authentisierung bezeichnet das Vorlegen eines Nachweises für die Identität des Nutzers gegenüber dem IT-System, an der er sich anmelden möchte.

Benutzer melden sich innerhalb des Unternehmensnetzwerkes mit Benutzernamen und Passwort an den jeweiligen IT-Systemen an.

Eine Passwortrichtlinie ist vorhanden. Sie erzwingt systemseitig eine Passwortkomplexität (Zeichen aus Groß-, und Kleinschreibung, Buchstaben, Zahlen, Sonderzeichen, Mindestpasswortlänge 8 Zeichen).

b) Authentifizierung

Die Authentifizierung bezeichnet das Vorgehen zur Überprüfung der Behauptung der Identität und dessen Ergebnis, indem das IT-System diese mit den hinterlegten Informationen zur behaupteten Identität abgleicht.

Nach fünf Fehlversuchen bei der Anmeldung wird das Benutzerkonto gesperrt.

Beim Verlassen des Arbeitsplatzes werden IT-Systeme systemseitig nach 5 Minuten automatisch gesperrt.

c) Autorisierung

Bei erfolgreicher Authentifizierung erfolgt die Gewährung oder Beschränkung auf bestimmte Rechte innerhalb des Unternehmensnetzwerkes und der IT-Anwendungen.

Jeder Benutzer verfügt über ein Benutzerprofil, das die jeweiligen Rechte zur Datenverarbeitung beinhaltet. Es wird hierbei ein Rollenkonzept verwendet. Berechtigungen für gleiche oder ähnliche Geschäftsprozesse werden in Benutzerrollen zusammengefasst. Jedem Benutzer werden entsprechend seiner Funktion im Unternehmen entsprechenden Rollen zugewiesen.

Auf diese Weise wird erreicht, dass sowohl Veränderungen in den Zuständigkeiten des Benutzers als auch Veränderungen in den Geschäftsprozessen nur in den Benutzerrollen nachvollzogen werden müssen und das Berechtigungskonzept konsistent und überschaubar bleibt.

Die Definition von Benutzerrollen gehört zum Aufgabenfeld der Berechtigungsadministration. Die Festlegung der Zuordnung zum einzelnen Benutzer erfolgt über den Vorgesetzten. Die technische Umsetzung wird von der IT-Systemadministration durchgeführt.

d) Mobile Geräte

Mobile IT-Systeme (Notebooks, Smartphones) sind mit einer dem Stand der Technik entsprechenden vollständigen Verschlüsselung versehen. Das gilt auch für mobile Datenträger (z.B. USB-Sticks).

e) Schutz vor Schadsoftware

Alle Server und Clients sind mit Virenschutzsoftware versehen, deren Signaturen sich automatisch aktualisieren.

f) Firewall

Es wird eine Firewall eingesetzt. Innerhalb des Unternehmensnetzwerkes wird der Datenprivacy shield zwischen den einzelnen Endgeräten über Software-Firewalls geregelt.

g) Distributed Denial of Service attack - DDSO Systeme

Es wird ein Distributed Denial of Service attack - DDSO System eingesetzt, um Angriffe gegen das Rechnernetz zu erkennen. Erkannte Angriffe werden in Log-Daten aufgesammelt und dem Administrator mitgeteilt.

Ein Distributed Denial of Service attack - DDSO System erkennt Angriffe automatisiert und verhindert diese aktiv.

h) Sicherheitsupdates

Sicherheitsupdates werden nach Verfügbarkeit und Prüfung durch die Systemadministration in einem laufenden und automatisierten Verfahren eingespielt.

Trennungskontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Vom Auftragnehmer umgesetzte Maßnahmen:

Daten, die verschiedenen Zwecken dienen, werden getrennt voneinander verarbeitet (Multi-Tenant-System). Das gilt insbesondere für Daten von Mandanten, die in einer Weise verarbeitet werden, die sicherstellt, dass ein Zugriff von Mandanten auf Daten andere Mandanten ausgeschlossen ist. Technisch umgesetzt wird dies durch folgende Maßnahmen:

- Logische Mandantentrennung: Die Daten werden in den Datenbanken logisch getrennt und verwaltet.
- Festlegung von Datenbankrechten
- Ordnerstrukturen mit entsprechenden Berechtigungsvergaben.

Zugriffskontrolle

Es ist Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Vom Auftragnehmer umgesetzte Maßnahmen:

a) Berechtigungsvergabe

Das Autorisierungsverfahren ermöglicht eine differenzierte Vergabe der Berechtigungen. Je nach Anwendung existieren differenzierte Zugriffsrechte für Lesen, Schreiben oder Ändern von Daten. Die Vergabe der Benutzerrollen und damit einhergehender Berechtigungen erfolgt durch einen definierten und dokumentierten Unternehmensprozess.

Generell gilt das „Need-to-Know-Prinzp" bei der Berechtigungsvergabe.

Die Rechte von Personen werden beim Ausscheiden aus dem Unternehmen oder beim Wechsel einer Aufgabe im Unternehmen entzogen. Hierfür ist ein definierter und dokumentierter Unternehmensprozess vorhanden.

Die Anzahl der Mitarbeiter, die über administrative Rechte verfügen, ist auf das notwenige Maß begrenzt.

b) Protokollierungsfunktionen

Jegliche Zugriffe auf die Anwendung und Daten werden im System protokolliert.

c) Löschung von Datenträgern

Defekte bzw. nicht mehr verwendete Datenträger werden durch einen zertifizierten Dienstleister gemäß DIN 66399 im Rahmen einer datenschutzrechtlichen Auftragsverarbeitung nach Art. 28 DSGVO vernichtet. Die Vernichtung wird vom Dienstleister protokolliert.

d) Löschung von Papierunterlagen

Papierunterlagen mit vertraulichen und/oder personenbezogenen Daten werden in verschlossenen Sammelbehältern entsorgt und durch einen zertifizierten Dienstleister gemäß DIN 66399 im Rahmen einer datenschutzrechtlichen Auftragsverarbeitung nach Art. 28 DSGVO vernichtet. Die Vernichtung wird vom Dienstleister protokolliert.

Pseudonymisierung

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

Vom Auftragnehmer umgesetzte Maßnahmen:

- *Es wird keine Pseudonymisierung eingesetzt*

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

Weitergabekontrolle

Es ist Sorge zu tragen, 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.

Vom Auftragnehmer umgesetzte Maßnahmen:

a) VPN-Technologie

Der Zugriff der Standorte auf das Unternehmensnetzwerk erfolgt über VPN-Technologie (Virtual Private Network). Hierbei handelt es sich um ein in sich geschlossenes Kommunikationsnetz, die eine abhör- und manipulationssichere verschlüsselte Kommunikation zwischen den VPN-Partnern ermöglicht

b) Verschlüsselte Datenträger

Datenträger werden vor der Übermittlung verschlüsselt und mit einem Passwort geschützt. Die Verschlüsselung erfolgt mit einer AES-256-Bit-Verschlüsselung.

c) Verschlüsselte Dateianhänge

Schützenswerte Dateianhänge in E-Mails sind verschlüsselt und passwortgeschützt.

d) E-Mailverschlüsselung

Es besteht grundsätzlich die Möglichkeit E-Mails zu verschlüsseln. Dies wird nach Absprache mit dem Kommunikationspartner festgelegt.

Für die Ver- und Entschlüsselung von E-Mails stehen die Verschlüsselungsstandards S/MIME v3, und OpenPGP/MIME zur Verfügung. Für den E-Mail-Empfang wird die Verschlüsselungsart S/MIME v3. Verwendet.

e) STARTTLS-Verschlüsselung

Für die E-Mailkommunikation wird STARTTLS mittels TLS (Transport Layer Security) eingesetzt.

Diese Transportverschlüsselung sorgt dafür, dass die E-Mail auf dem Weg vom E-Mailserver des Absenders zum E-Mailserver des Empfängers verschlüsselt ist. TLS zum E-Mailserver der Empfänger wird, wenn technisch möglich, verwendet.

2. Eingabekontrolle

Es ist Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Vom Auftragnehmer umgesetzte Maßnahmen:

Jegliche Benutzerzugriffe sowie Änderungen an Daten werden mit Datum und Uhrzeit protokolliert. Hierbei kann genau zugeordnet werden, welcher Nutzer welche Änderungen am System vorgenommen hat. Zudem sind die Eingabemöglichkeiten der einzelnen Nutzer durch das konfigurierbare Rollensystem einschränkbar.

3. Sonstige Technische und Organisatorische Maßnahmen zur Gewährleistung der Integrität

Vom Auftragnehmer umgesetzte Maßnahmen:

(3) Verfügbarkeit, Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO) Wiederherstellbarkeit (Art.32 Abs. 1 lit. c DSGVO)

Personenbezogene Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Vom Auftragnehmer umgesetzte Maßnahmen:

Die Server sind im Rahmen eines Hostings in externen zertifizierten Rechenzentren mit den Standorten gemäß ANHANG IV – Unterauftragnehmer untergebracht.

a) Standortauswahl

Gefährdungspotenziale aus dem Umfeld (Wasser-, Explosions-, Trümmer-, Erschütterungs- und Schadstoffgefährdung) sind gemieden.

Die Gebäudekonstruktion sowie Fenster und Türen bieten einen Zutritts-, Brand- und Trümmerschutz. Das Gebäude ist gegen Blitzeinschlag geschützt. Der Sicherheitsbereich liegt abseits öffentlicher Zugänge und gefährlicher Produktionsprozesse und bildet einen eigenen Brandabschnitt. Eine Trennung zwischen Grob- und Feintechnik ist erfolgt. Es besteht ein baulicher Brand- und Wasserschutz.

b) Brandschutz

Eine Brandmeldeanlage ist installiert und zu einer Alarmempfangsstelle aufgeschaltet. Benachbarte Räume, doppelter Fußboden, abgehängte Decken und Luftkanäle sind in die Brandüberwachung einbezogen. Neben der Alarmierung werden Abschaltfunktionen und Schadensbegrenzungsmaßnahmen ausgelöst, z. B. durch eine Gaslöschanlage. Eine zusätzliche Versorgung mit geeigneten Handfeuerlöschern ist gegeben.

c) Energieversorgung

Die Elektroinstallation erfolgte nach den einschlägigen DIN-Normen und VDE-Vorschriften. Es existieren angepasste Aufteilungen und Absicherungen der Stromkreise. Sie sind gegen Überspannung geschützt. Ausfälle sind durch eine redundante Auslegung abgefangen.

Im Falle eines Stromausfalls wird das Rechenzentrum über Notstromaggregate hinreichend versorgt.

d) Klimatisierung

Die Abwärme der Server und Infrastrukturkomponenten wird durch Kühlung hinreichend abgefangen. Es ist sichergestellt, dass Lufttemperatur, Luftfeuchte und Staubbelastung entsprechende Grenzen einhalten. Feuer- und Rauchklappen sind gemäß eines Brandschutzkonzeptes eingebaut. Die Einhaltung der Klimavorgaben wird fernüberwacht. Ausfälle sind durch eine redundante Auslegung abgefangen.

e) Sicherheitseinrichtungen

Alle Sicherheitseinrichtungen werden einem regelmäßigen Funktionstest unterzogen. Regelmäßige Wartungen an Verschleißteilen der Infrastrukturkomponenten sind in einem Wartungsplan festgelegt.

Darüber hinaus greifen im Notfall robuste Maßnahmen zur Notfallwiederherstellung. So geht beispielsweise bei einem Brand oder einer anderen Störung der Datenzugriff automatisch und reibungslos auf ein anderes Rechenzentrum über, sodass die Nutzer unterbrechungsfrei weiterarbeiten können.

f) Server

Daten eines einzelnen Nutzers werden auf eine Reihe von Servern an unterschiedlichen Standorten verteilt und gespeichert. Diese Daten werden dann in Blöcke unterteilt und auf zahlreiche Systeme repliziert, um einen Single Point of Failure zu vermeiden. Die Datenblöcke erhalten als zusätzliche Sicherheitsmaßnahme zufällig generierte Namen, sodass sie für Menschen nicht lesbar sind.

g) Datensicherung

Es erfolgt eine tägliche Datensicherung. Backups sind zugriffsgeschützt und werden regelmäßig auf Konsistenz geprüft.

Ein Datensicherungs- und Wiederherstellungskonzept ist vorhanden und wird regelmäßig getestet. Jede Sicherungskopie hat einen Lebenszyklus von 30 Tagen und wird nach Ablauf des Intervalls automatisch und unwiderruflich gelöscht.

h) Speicherdauer

Die Speicherdauer richtet sich nach dem Status und Alter der Vorgänge wie folgt:

Nicht abgeschlossene Vorgänge: Daten eines Nutzers, die im Rahmen eines nicht abgeschlossenen Vorgangs erfasst werden, verbleiben maximal 30 Tage im System. Die Frist endet mit Ablauf des 30.sten Tages. Beginn ist der Ablauf des Tages der Erfassung.

Abgeschlossene Vorgänge: Daten eines Nutzers, die im Rahmen eines abgeschlossenen Vorgangs erfasst wurden, verbleiben maximal 14 Tage im System. Die Frist endet mit Ablauf des 14.sten Tages. Beginn ist der Ablauf des Tages der Erfassung.

Das System überprüft täglich den Status und das Alter der Vorgänge. Nach Ablauf der jeweiligen maximalen Speicherdauer werden die Daten automatisch gelöscht.

(4) Verfahren zur regelm. Überpr., Bew. und Evaluierung (Art. 32 Abs. 1 lit. d & Art. 25 Abs. 1 DSGVO)

1. Auftragskontrolle

Eine Auftragsverarbeitung i.S. von Art. 28 DSGVO findet nicht ohne entsprechende Weisung des Auftraggebers statt. Auftragsverarbeitungen erfolgen über eine eindeutige Vertragsgestaltung, ein formalisiertes Auftragsmanagement, eine strenge Auswahl des Dienstleisters und Nachkontrollen.

2. Externe Prüfungen, Audits, Zertifizierungen

Zertifizierung Google Rechenzentrum (ISO 27001, ISO 27018 etc) - Übersicht über Compliceberichte | Google Cloud und Compliance | Einhaltung von Datenschutzgesetzen (safety.google)

3. Sonstige Technische und Organisatorische Maßnahmen zur Überprüfung, Bewertung und Evaluierung

Vom Auftragnehmer umgesetzte Maßnahmen:

a) Organisation

Die Verantwortlichkeiten für Datenschutz und Informationssicherheit sind klar geregelt.

Alle Beschäftigten sind auf die Vertraulichkeit verpflichtet und werden regelmäßig im Datenschutz sensibilisiert.

Es sind für alle Beschäftigten verbindliche Richtlinien zum Datenschutz und zur IT-Sicherheit in Kraft.

b) Datenschutz-Managementsystem

Das Datenschutz-Managementsystem sichert und dokumentiert die Einhaltung der DSGVO über das gesamte Unternehmen. Es erfüllt insbesondere die Rechenschafts- und Nachweispflichten-des Art. 5 Abs. 1 DSGVO. Es enthält überdies die von der DSGVO geforderten Dokumentationen (Verzeichnis von Verarbeitungstätigkeiten)

Im Datenschutz-Managementsystem sind Prozesse und Maßnahmen für den Umgang mit Betroffenenrechten, Informationspflichte, Datenschutz-Folgenabschätzungen, Privacy by Design/by Default etc. definiert.

c) Incident-Response-Management

Für den Fall einer Verletzung des Schutzes personenbezogener Daten („Datenpanne“) wurden Prozesse und Verfahren definiert, die sicherstellen, dass Datenschutzverletzungen erkannt und unverzüglich gemeldet werden.

ANHANG IV – Unterauftragnehmer

Der *Auftragnehmer* nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

☐	Es werden keine Unterauftragnehmer eingesetzt
☒	Es werden folgende Unterauftragnehmer eingesetzt (Name, Adresse, Genaue Beschreibung der Tätigkeit) ▪ ***falls noch weitere Unterauftragsverarbeiter bekannt sind bitte ergänzen***

Firma, Anschrift	**Serverstandorte**	**Art der Verarbeitung**	**Zweck**	**Art der Daten**	**Kategorien der betroffenen Personen**
Stripe Technology Europe, Ltd., The One Building, Grand Canal Street Lower, Dublin 2, Ireland.	Irland	Zahlungsabwicklung	Zahlungen von Nutzern empfangen und verwalten	Kontaktdaten von Nutzern, Zahlungsinformationen	Nutzer
Sendinblue GmbH, Köpenicker Straße 126, 10179 Berlin	Deutschland	Versand von E-Mails	Kontakt zu Nutzern	E-Mail Adressen der Empfänger	Nutzer, Beschäftigte