Auftragsverarbeitungsvereinbarung

Abschnitt 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) 3. 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 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 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 14 Tage im Voraus ausdrücklich inschriftlicher 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.
f) Unterauftragsverarbeiter sind im Anhang IV aufgeführt.

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 Artikel 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 [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): [Kunde: Name und Kontaktdaten des/der Verantwortlichen und gegebenenfalls des Datenschutzbeauftragten des Verantwortlichen]

Name: _____

Anschrift: _____

_____

Name, Funktion und Kontaktdaten der Kontaktperson: _____

_____

Unterschrift und Beitrittsdatum: _____

Auftragsverarbeiter:

Name: CERTNET GmbH

Anschrift: Forstfeldstraße 2, 34123 Kassel

Name, Funktion und Kontaktdaten der Kontaktperson: Dirk Hildebrand, E-Mail: hildebrand@certnet.de, Tel.: +49 (561) 81679-123

Unterschrift und Beitrittsdatum: _____

ANHANG II

Beschreibung der Verarbeitung

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:
Mitarbeiterinnen und Mitarbeiter, sowie Schülerinnen und Schüler, bzw. Teilnehmerinnen und Teilnehmern an Maßnahmen von Bildungseinrichtungen. In der Regel werden die Daten für den Import (zur Erstellung von Microsoft 365 Benutzerkonten) benötigt.

Kategorien personenbezogener Daten, die verarbeitet werden:
Vorname, Nachname, Benutzername, Position, Abteilung oder Klasse und in wenigen Fällen zusätzliche dienstliche Kontaktdaten, wie Büronummer, Telefon (geschäftlich), Mobiltelefon, Faxnummer, Adresse, Ort, Bundesland/Kanton, Postleitzahl, Land oder Region.

Art der Verarbeitung:
Im Rahmen von Fernwartungsdienstleistung für den IT-Support von Microsoft 365 führen wir beispielsweise den Import von Nutzern durch. Dafür stellt der Kunde Listen bereit, die die beschriebenen Kategorien enthalten können. Die Listen verbleiben immer beim Kunde und die Verarbeitung wird auf den Systemen des Kunden, im Beisein des Kunden durchgeführt.

In einzelnen Fällen gewährt uns der Kunde direkten Zugang zu seiner Microsoft 365 Umgebung, mit der Bitte um Bestandsaufnahme von Konfigurationseinstellungen oder spezifischer Modifikation von Leistungen innerhalb des Tenants. Dabei werden keine personenbezogenen Daten von uns gespeichert.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden:
Das Lösen technischer Probleme und die Durchführung von Tenant-Einstellungen, sowie Konfigurationen von Microsoft 365 Tenants beim Kunden.

Dauer der Verarbeitung:
Die Dauer richtet sich nach der Laufzeit des Hauptvertrages.

ANHANG III

Technische und organisatorische Maßnahmen

Hinweis: Da in der Regel keine personenbezogenen Daten unserer Kunden gespeichert werden, sondern nur im Rahmen einer Fernwartungsdienstleistung auf deren Systeme zugegriffen wird, betonen wir, dass die folgenden genannten Maßnahmen primär für internen Prozesse und die Einhaltung der Anforderungen als Auftragsverarbeiter gelten. Kundendaten verbleiben in deren Verantwortungsbereich.

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

Um ein angemessenes Schutzniveau für die Verarbeitung personenbezogener Daten im Rahmen unserer Microsoft 365-Supportdienstleistungen zu gewährleisten, haben wir umfassende technische und organisatorische Sicherheitsmaßnahmen implementiert. Diese Maßnahmen berücksichtigen die Art, den Umfang, die Umstände und den Zweck der Verarbeitung sowie die Risiken für die Rechte und Freiheiten natürlicher Personen. Im Folgenden sind die wichtigsten Maßnahmen aufgeführt:

1. Zugangskontrolle

- **Technische Maßnahmen:**
  - Implementierung von rollenbasierten Zugriffsrechten (RBAC) zur Beschränkung des Zugriffs auf personenbezogene Daten auf autorisierte Mitarbeiter.
  - Verwendung von Multi-Faktor-Authentifizierung (MFA) für den Zugriff auf Microsoft 365 und interne Systeme.
  - Regelmäßige Überprüfung und Anpassung von Zugriffsrechten.
- **Organisatorische Maßnahmen:**
  - Schulung der Mitarbeiter zum sicheren Umgang mit Zugangsdaten.
  - Erstellung und Pflege von Zugriffsrichtlinien und -verfahren.

2. Datensicherheit

- **Technische Maßnahmen:**
  - Verschlüsselung von Daten sowohl während der Übertragung (TLS/SSL) als auch im Ruhezustand (AES-256).
  - Regelmäßige Sicherung von Daten und Testung der Wiederherstellungsprozesse.
  - Einsatz von Antivirensoftware und Firewalls zum Schutz vor Malware und unbefugtem Zugriff.
- **Organisatorische Maßnahmen:**
  - Regelmäßige Überprüfung und Aktualisierung der Sicherheitsrichtlinien.
  - Durchführung von Sicherheit-Checks im Rahmen regelmäßiger Schulungen.

3. Trennungsgebot

- **Technische Maßnahmen:**
  - Logische Trennung von Daten durch die Verwendung separater Datenbanken und Speicherbereiche für unterschiedliche Kunden und Zwecke.
- **Organisatorische Maßnahmen:**
  - Festlegung von Verfahren zur sicheren Handhabung und Trennung von Daten.

4. Zertifizierungen und Compliance

- **Microsoft 365 Compliance:** Wir nutzen die integrierten Compliance- und Sicherheitsfunktionen von Microsoft 365, einschließlich Data Loss Prevention (DLP) und Advanced Threat Protection (ATP).

5. Schulung und Sensibilisierung

- **Regelmäßige Schulungen:** Alle Mitarbeiter werden regelmäßig in den Bereichen Datenschutz und Informationssicherheit geschult.

7. Dokumentation und Überprüfung

- **Dokumentation:** Alle technischen und organisatorischen Maßnahmen werden dokumentiert und regelmäßig aktualisiert.
- **Überprüfung:** Regelmäßige interne Audits zur Überprüfung der Wirksamkeit der Maßnahmen.

Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten

Eine Pseudonymisierung wird in unserem Unternehmen derzeit nicht durchgeführt, da dies für die von uns angebotenen Dienstleistungen und die Art der Datenverarbeitung nicht erforderlich ist. Stattdessen setzen wir auf eine umfassende Verschlüsselung, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten sicherzustellen.

1. Verschlüsselung personenbezogener Daten

- **Verschlüsselung während der Übertragung:**
  - Alle personenbezogenen Daten, die über Netzwerke übertragen werden, sind durch Verschlüsselungsprotokolle wie TLS (Transport Layer Security) mit mindestens TLS 1.2 geschützt. Dies gilt insbesondere für die Kommunikation zwischen unseren Systemen, den Systemen unserer Kunden und den Microsoft 365-Diensten.
  - E-Mail-Kommunikation wird über verschlüsselte Verbindungen (z. B. SMTP over TLS) abgewickelt, um den Schutz der Daten während der Übertragung zu gewährleisten.
- **Verschlüsselung im Ruhezustand:**
  - Personenbezogene Daten, die in Datenbanken, Dateisystemen oder Cloud-Speichern gespeichert werden, sind durch starke Verschlüsselungsalgorithmen (z.B. AES-256) geschützt.
  - Microsoft 365 bietet standardmäßig Verschlüsselung im Ruhezustand für alle gespeicherten Daten, was wir aktiv nutzen und unterstützen.
- **Verschlüsselung von Backups:**
  - Alle Sicherungen von personenbezogenen Daten werden verschlüsselt gespeichert, um sicherzustellen, dass sie auch im Falle eines unbefugten Zugriffs nicht lesbar sind.

2. Zugriffskontrolle auf verschlüsselte Daten

- **Rollenbasierte Zugriffskontrolle (RBAC):**
  - Der Zugriff auf verschlüsselte Daten ist auf autorisierte Mitarbeiter beschränkt, die über die erforderlichen Berechtigungen verfügen.
  - Multi-Faktor-Authentifizierung (MFA) wird für den Zugriff auf Systeme, die verschlüsselte Daten enthalten, eingesetzt.

3. Begründung für den Verzicht auf Pseudonymisierung

- **Keine Pseudonymisierung:**
  - Pseudonymisierung wird in unserem Unternehmen nicht durchgeführt, da dies für die von uns angebotenen Dienstleistungen und die Art der Datenverarbeitung nicht erforderlich ist, bzw. den Kundenwunsch nicht entspricht. Unsere Prozesse erfordern die Verarbeitung von personenbezogenen Daten in ihrer ursprünglichen Form, um einen effektiven Support für Microsoft 365-Dienste zu gewährleisten. Stattdessen setzen wir auf eine Verschlüsselung und andere technische sowie organisatorische Maßnahmen, um die Sicherheit der Daten zu gewährleisten.

Maßnahmen zur fortdauernden Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste

Um die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung sicherzustellen, haben wir folgende Maßnahmen implementiert:

1. Vertraulichkeit

- **Technische Maßnahmen:**
  - **Verschlüsselung:** Alle Fernwartungsverbindungen werden mit **TLS 1.2** und **AEAD**-Verschlüsselung, ähnlich wie beim Online-Banking verschlüsselt. Der asymmetrische Schlüsselaustausch erfolgt über **2048-bit RSA** oder **256-bit elliptische Kurven**.
- **Organisatorische Maßnahmen:**
  - **Schulungen:** Regelmäßige Schulungen der Mitarbeiter zum Thema Datenschutz und Informationssicherheit.
  - **Zugriffsrichtlinien:** Klare Richtlinien und Verfahren für den Zugriff auf Kundensysteme, die regelmäßig überprüft und aktualisiert werden.

2. Integrität

- **Technische Maßnahmen:**
  - **Sicherheitsupdates:** Regelmäßige Installation von Sicherheitsupdates und Patches für alle verwendeten Systeme und Tools.
- **Organisatorische Maßnahmen:**
  - **Change-Management:** Implementierung eines Change-Management-Prozesses, um sicherzustellen, dass alle Änderungen an Systemen und Diensten dokumentiert und überprüft werden.

3. Verfügbarkeit

- **Technische Maßnahmen:**
  - **Redundanz:** Einsatz von redundanten Systemen und Netzwerkverbindungen, um Ausfälle zu minimieren.
- **Organisatorische Maßnahmen:**
  - **Notfallwiederherstellungsplan:** Erstellung und Pflege eines Notfallwiederherstellungsplans (Disaster Recovery Plan), der regelmäßig getestet und aktualisiert wird.

4. Maßnahmen zur schnellen Wiederherstellung bei physischen oder technischen Zwischenfällen

- **Technische Maßnahmen:**
  - **Backups:** Regelmäßige Sicherung aller kritischen Systeme und Daten, um im Falle eines Zwischenfalls eine schnelle Wiederherstellung zu ermöglichen.

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

Um die fortlaufende Wirksamkeit unserer technischen und organisatorischen Maßnahmen (TOMs) zur Gewährleistung der Sicherheit der Verarbeitung personenbezogener Daten sicherzustellen, haben wir ein strukturiertes Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung implementiert. Dieses Verfahren umfasst folgende Schritte:

1. Regelmäßige interne Audits

- **Durchführung:** Interne Audits werden in regelmäßigen Abständen (z.B. jährlich) durchgeführt, um die Einhaltung der festgelegten Sicherheitsmaßnahmen zu überprüfen.
- **Bewertungskriterien:** Die Audits basieren auf festgelegten Bewertungskriterien, die sich an den Anforderungen der DSGVO und anderen relevanten Standards (z.B. ISO/IEC 27001) orientieren.
- **Dokumentation:** Die Ergebnisse der internen Audits werden dokumentiert und dienen als Grundlage für Verbesserungsmaßnahmen.

2. Risikobewertungen

- **Regelmäßige Risikobewertungen:** Wir führen regelmäßige Risikobewertungen durch, um potenzielle Sicherheitsrisiken zu identifizieren und zu bewerten.
- **Anpassung der Maßnahmen:** Basierend auf den Ergebnissen der Risikobewertungen passen wir unsere technischen und organisatorischen Maßnahmen an, um neuen und sich ändernden Risiken gerecht zu werden.

3. Überprüfung der Zugriffsrechte

- **Regelmäßige Überprüfung:** Die Zugriffsrechte aller Mitarbeiter werden regelmäßig überprüft, um sicherzustellen, dass nur autorisierte Personen Zugriff auf personenbezogene Daten haben.
- **Anpassung der Rechte:** Bei Bedarf werden Zugriffsrechte angepasst oder widerrufen, um die Sicherheit der Daten zu gewährleisten.

4. Schulungen und Sensibilisierung

- **Regelmäßige Schulungen:** Alle Mitarbeiter werden regelmäßig in den Bereichen Datenschutz und Informationssicherheit geschult, um das Bewusstsein für Sicherheitsrisiken zu stärken.

5. Dokumentation und Berichterstattung

- **Dokumentation:** Alle Überprüfungen, Bewertungen und Evaluierungen werden dokumentiert, um eine nachvollziehbare Grundlage für zukünftige Maßnahmen zu schaffen.
- **Berichterstattung:** Die Ergebnisse der Überprüfungen werden an die Geschäftsleitung berichtet, um Transparenz und kontinuierliche Verbesserung sicherzustellen.

6. Kontinuierliche Verbesserung

- **Feedback-Schleifen:** Wir etablieren Feedback-Schleifen, um Erkenntnisse aus Audits, Risikobewertungen und Sicherheitstests in die kontinuierliche Verbesserung unserer Sicherheitsmaßnahmen einfließen zu lassen.
- **Anpassung der Verfahren:** Basierend auf den gewonnenen Erkenntnissen passen wir unsere Verfahren und Maßnahmen kontinuierlich an, um ein hohes Schutzniveau aufrechtzuerhalten.

Maßnahmen zur Identifizierung und Autorisierung der Nutzer

Um sicherzustellen, dass nur autorisierte Nutzer Zugriff auf unsere Systeme und Dienste haben, haben wir umfassende Maßnahmen zur Identifizierung und Autorisierung implementiert. Diese Maßnahmen umfassen sowohl technische als auch organisatorische Aspekte und sind darauf ausgelegt, die Sicherheit und Integrität der verarbeiteten Daten zu gewährleisten.

1. Identifizierung der Nutzer

- **Technische Maßnahmen:**
  - **Benutzerkonten:** Jeder Nutzer erhält ein individuelles Benutzerkonto, das eindeutig zugeordnet ist.
  - **Anmeldeverfahren:** Verwendung von sicheren Anmeldeverfahren, die eine eindeutige Identifizierung der Nutzer ermöglichen.
  - **Multi-Faktor-Authentifizierung (MFA):** Implementierung von Zwei-Faktor-Authentifizierung, um die Sicherheit der Anmeldeverfahren zu erhöhen.
- **Organisatorische Maßnahmen:**
  - **Schulungen:** Regelmäßige Schulungen der Mitarbeiter zum sicheren Umgang mit Benutzerkonten und Anmeldeinformationen.

2. Autorisierung der Nutzer

- **Technische Maßnahmen:**
  - **Rollenbasierte Zugriffskontrolle (RBAC):** Implementierung von rollenbasierten Zugriffsrechten, um sicherzustellen, dass Nutzer nur auf die Daten und Funktionen zugreifen können, die für ihre Rolle erforderlich sind.
- **Organisatorische Maßnahmen:**
  - **Zugriffsrichtlinien:** Erstellung und Pflege von Zugriffsrichtlinien, die die Vergabe und Verwaltung von Zugriffsrechten regeln.

    - **Regelmäßige Überprüfung:** Regelmäßige Überprüfung und Anpassung der Zugriffsrechte, um sicherzustellen, dass sie den aktuellen Anforderungen entsprechen.

3. Protokollierung und Überwachung

- **Technische Maßnahmen:**
    - **Logging:** Protokollierung aller Anmelde- und Zugriffsversuche, um eine nachträgliche Überprüfung zu ermöglichen (innerhalb der Möglichkeiten von Microsoft 365).
- **Organisatorische Maßnahmen:**
    - **Audit-Protokolle:** Regelmäßige Überprüfung der Audit-Protokolle, um sicherzustellen, dass die Zugriffsrichtlinien eingehalten werden.

4. Schulungen und Sensibilisierung

- **Regelmäßige Schulungen:** Alle Mitarbeiter werden regelmäßig in den Bereichen Identifizierung und Autorisierung geschult, um das Bewusstsein für Sicherheitsrisiken zu stärken.

5. Dokumentation und Berichterstattung

- **Dokumentation:** Alle Maßnahmen zur Identifizierung und Autorisierung der Nutzer werden dokumentiert, um eine nachvollziehbare Grundlage für zukünftige Maßnahmen zu schaffen.
- **Berichterstattung:** Die Ergebnisse der Überprüfungen und Audits werden an die Geschäftsleitung berichtet, um Transparenz und kontinuierliche Verbesserung sicherzustellen.

Maßnahmen zum Schutz der Daten während der Übermittlung

Um die Sicherheit und Vertraulichkeit personenbezogener Daten während der Übermittlung zu gewährleisten, haben wir eine Reihe von technischen und organisatorischen Maßnahmen implementiert. Diese Maßnahmen stellen sicher, dass Daten während der Übertragung vor unbefugtem Zugriff, Verlust oder Manipulation geschützt sind. Im Folgenden sind die wichtigsten Maßnahmen aufgeführt:

1. Verschlüsselung der Datenübertragung

- **TLS/SSL:** Alle Datenübertragungen zwischen unseren Systemen und denen unserer Kunden erfolgen über verschlüsselte Verbindungen mittels Transport Layer Security (TLS) oder Secure Sockets Layer (SSL). Dies gewährleistet, dass die Daten während der Übertragung vor Abhör- und Man-in-the-Middle-Angriffen geschützt sind.

2. Sichere Protokolle

- **SFTP/FTPS:** Für die Übertragung von Dateien verwenden wir sichere Protokolle wie SFTP (Secure File Transfer Protocol) oder FTPS (File Transfer Protocol Secure), die eine verschlüsselte Datenübertragung gewährleisten.
- **HTTPS:** Alle Webanwendungen und -dienste, die wir verwenden, sind über HTTPS (Hypertext Transfer Protocol Secure) abgesichert, um die Integrität und Vertraulichkeit der übertragenen Daten zu schützen.

3. Authentifizierung und Autorisierung

- **Multi-Faktor-Authentifizierung (MFA):** Der Zugriff auf Systeme und Dienste, die für die Datenübertragung verwendet werden, ist durch Multi-Faktor-Authentifizierung gesichert. Dies stellt sicher, dass nur autorisierte Personen auf die Systeme zugreifen können.
- **Zugriffskontrolle:** Wir implementieren rollenbasierte Zugriffskontrollen (RBAC), um sicherzustellen, dass nur berechtigte Mitarbeiter Zugriff auf die Daten und Systeme haben, die für die Datenübertragung erforderlich sind.

4. Schulungen und Sensibilisierung

- **Regelmäßige Schulungen:** Alle Mitarbeiter, die an der Datenübertragung beteiligt sind, werden regelmäßig in den Bereichen Datenschutz und Informationssicherheit geschult.

5. Regelmäßige Überprüfung und Anpassung

- **Sicherheitsaudits:** Wir führen regelmäßige Sicherheitsaudits durch, um die Wirksamkeit unserer Maßnahmen zum Schutz der Daten während der Übermittlung zu überprüfen.

- **Anpassung der Maßnahmen:** Basierend auf den Ergebnissen der Audits und neuen Erkenntnissen im Bereich der Informationssicherheit passen wir unsere Maßnahmen kontinuierlich an, um ein hohes Schutzniveau aufrechtzuerhalten.

Maßnahmen zum Schutz der Daten während der Speicherung

Um die Sicherheit der Daten während der Speicherung zu gewährleisten, nutzen wir umfassende technische und organisatorische Maßnahmen. Diese Maßnahmen berücksichtigen die Anforderungen der DSGVO und zielen darauf ab, die Vertraulichkeit, Integrität und Verfügbarkeit der Daten zu schützen. Im Folgenden sind die wichtigsten Maßnahmen beschrieben:

1. Verschlüsselung der gespeicherten Daten

- **Technische Maßnahmen:**
  - Alle Daten, die auf unseren Systemen gespeichert werden, sind durch starke Verschlüsselungsverfahren (z. B. AES-256 oder BitLocker) geschützt.
  - Die Verschlüsselung gilt sowohl für Daten im Ruhezustand („Data at Rest“) als auch für Backups.

2. Zugangskontrolle

- **Technische Maßnahmen:**
  - Der Zugriff auf gespeicherte Daten ist durch rollenbasierte Zugriffsrechte (RBAC) geregelt. Nur autorisierte Mitarbeiter haben Zugriff auf Daten, und dies nur im erforderlichen Umfang.
  - Multi-Faktor-Authentifizierung (MFA) wird für den Zugriff auf Systeme und Datenbanken verwendet.
- **Organisatorische Maßnahmen:**
  - Regelmäßige Überprüfung und Anpassung der Zugriffsrechte, um sicherzustellen, dass nur berechtigte Personen Zugriff haben.
  - Schulungen der Mitarbeiter zum sicheren Umgang mit Zugangsdaten und zur Einhaltung der Zugriffsrichtlinien.

3. Sicherung der Daten (Backups)

- **Technische Maßnahmen:**
  - Regelmäßige Sicherung aller kritischen Daten, um Datenverluste im Falle von Systemausfällen oder technischen Zwischenfällen zu verhindern.
  - Backups werden verschlüsselt und an sicheren Speicherorten aufbewahrt.
  - Testung der Wiederherstellungsprozesse in regelmäßigen Abständen, um die Verfügbarkeit der Daten im Notfall sicherzustellen.
- **Organisatorische Maßnahmen:**
  - Erstellung und Pflege eines Backup- und Wiederherstellungsplans, der regelmäßig überprüft und aktualisiert wird.

4. Schutz vor unbefugtem Zugriff und Manipulation

- **Technische Maßnahmen:**
  - Einsatz von Firewalls, um unbefugte Zugriffe auf die Speichersysteme zu verhindern.
  - Regelmäßige Sicherheitsupdates und Patches für alle Systeme, um bekannte Schwachstellen zu schließen.
  - Einsatz von Antivirensoftware und Malware-Schutzmechanismen, um die Integrität der gespeicherten Daten zu gewährleisten.
- **Organisatorische Maßnahmen:**
  - Regelmäßige Überprüfung der Sicherheitsrichtlinien und -verfahren, um sicherzustellen, dass sie den aktuellen Bedrohungen entsprechen.

5. Physische Sicherheit der Speichersysteme

- **Technische Maßnahmen:**

    - Die physischen Speichersysteme befinden sich in unseren Büroräumen, die über Zugangskontrollen verfügen.
- **Organisatorische Maßnahmen:**
    - Zutrittskontrollen und Besucherbeschränkungen für alle physischen Standorte, an denen Daten gespeichert werden.

6. Datenlöschung und -vernichtung

- **Technische Maßnahmen:**
    - Daten, die nicht mehr benötigt werden, werden sicher und endgültig gelöscht.
    - Bei der Außerbetriebnahme von Speichermedien werden diese physisch zerstört oder mittels spezieller Software vollständig überschrieben.
- **Organisatorische Maßnahmen:**
    - Festlegung von Aufbewahrungsfristen und Löschfristen für alle gespeicherten Daten.
    - Regelmäßige Überprüfung der gespeicherten Daten, um sicherzustellen, dass keine Daten länger als notwendig aufbewahrt werden.

7. Überwachung und Protokollierung

- **Technische Maßnahmen:**
    - Kontinuierliche Überwachung der Speichersysteme, um verdächtige Aktivitäten oder Sicherheitsvorfälle frühzeitig zu erkennen.
- **Organisatorische Maßnahmen:**
    - Untersuchung von Auffälligkeiten.

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

Um eine effektive Governance und Verwaltung der IT und der IT-Sicherheit sicherzustellen, haben wir ein Rahmenwerk etabliert, das klare Verantwortlichkeiten, Prozesse und Kontrollmechanismen definiert. Dieses Rahmenwerk gewährleistet, dass unsere IT-Systeme und -Dienste sicher, zuverlässig und konform mit den Anforderungen der DSGVO und anderen relevanten Standards betrieben werden. Im Folgenden sind die wichtigsten Maßnahmen beschrieben:

1. Strukturierte Verantwortlichkeiten und Rollen

- **IT-Sicherheitsbeauftragter:** Wir haben einen IT-Sicherheitsbeauftragten benannt, der für die Koordination und Überwachung aller IT-Sicherheitsmaßnahmen verantwortlich ist. Er ist auch interner Datenschutzbeauftragter und unterstützt uns bei der Einhaltung der datenschutzrechtlichen Anforderungen.
- **Rollen und Verantwortlichkeiten:** Klare Definition von Rollen und Verantwortlichkeiten für IT- und Sicherheitsprozesse, einschließlich der Eskalationswege bei Sicherheitsvorfällen.

2. Richtlinien und Verfahren

- **Datenschutzrichtlinien:** Spezifische Richtlinien zur Einhaltung der DSGVO, einschließlich der Verarbeitung personenbezogener Daten, der Rechte der Betroffenen und der Meldung von Datenschutzverletzungen.
- **Regelmäßige Aktualisierung:** Alle Richtlinien und Verfahren werden regelmäßig überprüft und aktualisiert, um sicherzustellen, dass sie den aktuellen Anforderungen und Bedrohungen entsprechen.

3. Risikomanagement

- **Risikobewertungen:** Regelmäßige Durchführung von Risikobewertungen, um potenzielle Sicherheitsrisiken zu identifizieren und zu bewerten.
- **Risikobehandlungspläne:** Entwicklung und Implementierung von Risikobehandlungsplänen, um identifizierte Risiken zu minimieren oder zu beseitigen.
- **Kontinuierliche Überwachung:** Kontinuierliche Überwachung der Risikolage und Anpassung der Maßnahmen bei Bedarf.

4. Schulungen und Sensibilisierung

- **Regelmäßige Schulungen:** Alle Mitarbeiter werden regelmäßig in den Bereichen IT-Sicherheit und Datenschutz geschult, um das Bewusstsein für Sicherheitsrisiken zu stärken.

5. Überwachung und Audits

- **Interne Audits:** Regelmäßige interne Audits zur Überprüfung der Einhaltung der IT-Sicherheitsrichtlinien und -verfahren.

6. Incident Management und Notfallwiederherstellung

- **Incident Response Plan:** Wir haben einen Incident Response Plan entwickelt, der klare Verfahren für die Erkennung, Meldung und Behebung von Sicherheitsvorfällen definiert.
- **Notfallwiederherstellungsplan:** Ein umfassender Notfallwiederherstellungsplan (Disaster Recovery Plan) gewährleistet, dass kritische Systeme und Daten im Falle eines Zwischenfalls schnell wiederhergestellt werden können.
- **Regelmäßige Tests:** Regelmäßige Tests des Incident Response Plans und des Notfallwiederherstellungsplans, um deren Wirksamkeit sicherzustellen.

7. Dokumentation und Berichterstattung

- **Dokumentation:** Alle IT- und Sicherheitsprozesse, Richtlinien und Verfahren werden detailliert dokumentiert, um eine nachvollziehbare Grundlage für die Überprüfung und Verbesserung zu schaffen.
- **Berichterstattung:** Regelmäßige Berichterstattung an die Geschäftsleitung und relevante Stakeholder über den Status der IT-Sicherheit, identifizierte Risiken und durchgeführte Maßnahmen.

8. Kontinuierliche Verbesserung

- **Feedback-Schleifen:** Wir etablieren Feedback-Schleifen, um Erkenntnisse aus Audits, Risikobewertungen und Sicherheitstests in die kontinuierliche Verbesserung unserer IT-Sicherheitsmaßnahmen einfließen zu lassen.
- **Anpassung der Verfahren:** Basierend auf den gewonnenen Erkenntnissen passen wir unsere Verfahren und Maßnahmen kontinuierlich an, um ein hohes Schutzniveau aufrechtzuerhalten.

Maßnahmen zur Gewährleistung der Datenminimierung

Gemäß dem Grundsatz der Datenminimierung stellen wir sicher, dass personenbezogene Daten auf das notwendige Maß beschränkt werden, das für die Erfüllung der jeweiligen Verarbeitungszwecke erforderlich ist. Da wir in der Regel keine personenbezogenen Daten unserer Kunden speichern, sondern nur im Rahmen der Fernwartung auf deren Systeme zugreifen, konzentrieren sich unsere Maßnahmen zur Datenminimierung auf die folgenden Aspekte:

1. Prinzip der Datenvermeidung

- **Keine Speicherung von Kundendaten:** Wir speichern grundsätzlich keine personenbezogenen Daten unserer Kunden, es sei denn, dies ist aus technischen oder vertraglichen Gründen unbedingt erforderlich. In solchen Fällen werden die Daten auf das absolut notwendige Minimum beschränkt.
- **Temporäre Verarbeitung:** Falls im Rahmen der Fernwartung temporär auf Kundendaten zugegriffen wird, erfolgt dies nur in Anwesenheit des Kunden und ohne dauerhafte Speicherung der Daten auf unseren Systemen.

2. Technische Maßnahmen zur Datenminimierung

- **Begrenzung der Datenverarbeitung:** Unsere Systeme und Tools sind so konfiguriert, dass sie nur die für die Fernwartung erforderlichen Daten verarbeiten. Überflüssige Daten werden nicht erfasst oder gespeichert.

3. Organisatorische Maßnahmen zur Datenminimierung

- **Schulungen der Mitarbeiter:** Unsere Mitarbeiter werden regelmäßig im Umgang mit dem Prinzip der Datenminimierung geschult. Sie sind angehalten, nur die Daten zu erfassen und zu verarbeiten, die für die Erfüllung ihrer Aufgaben erforderlich sind.

- **Klare Richtlinien:** Wir haben interne Richtlinien und Verfahren entwickelt, die sicherstellen, dass die Datenminimierung in allen Geschäftsprozessen berücksichtigt wird. Diese Richtlinien werden regelmäßig überprüft und aktualisiert.

4. Datenverarbeitungsverträge (AVV) und Auftragsverarbeitung

- **Vertragliche Vereinbarungen:** In unseren Verträgen mit Kunden und Partnern legen wir fest, dass nur die für die Erbringung der Dienstleistungen erforderlichen Daten verarbeitet werden.
- **Überprüfung der Datenflüsse:** Wir überprüfen regelmäßig die Datenflüsse zwischen uns und unseren Kunden, um sicherzustellen, dass keine überflüssigen Daten verarbeitet oder übertragen werden.

5. Transparenz und Dokumentation

- **Transparenz gegenüber Kunden:** Wir informieren unsere Kunden transparent über die von uns verarbeiteten Daten und die ergriffenen Maßnahmen zur Datenminimierung.

Maßnahmen zur Gewährleistung einer begrenzten Vorratsdatenspeicherung

Um den Grundsatz der begrenzten Speicherdauer zu gewährleisten, haben wir technische und organisatorische Maßnahmen implementiert, die sicherstellen, dass personenbezogene Daten und andere relevante Informationen nur so lange gespeichert werden, wie dies für die Erfüllung der Verarbeitungszwecke erforderlich ist. Da wir in der Regel keine personenbezogenen Daten unserer Kunden speichern, sondern nur im Rahmen der Fernwartung auf deren Systeme zugreifen, konzentrieren sich unsere Maßnahmen auf die folgenden Aspekte:

1. Festlegung von Speicherfristen

- **Klare Speicherrichtlinien:** Wir haben interne Richtlinien festgelegt, die die maximale Speicherdauer für verschiedene Arten von Daten definieren. Diese Richtlinien basieren auf den gesetzlichen Anforderungen und den betrieblichen Erfordernissen.
- **Differenzierte Fristen:** Die Speicherfristen werden je nach Art der Daten und ihrem Verwendungszweck differenziert festgelegt. Beispielsweise werden technische Logs nur für einen begrenzten Zeitraum (z. B. 30 Tage) gespeichert, es sei denn, sie werden für spezifische Zwecke (z. B. Fehleranalyse) benötigt.

2. Technische Maßnahmen zur begrenzten Speicherung (Backups)

- **Backup-Rotation:** Backups werden in regelmäßigen Abständen überschrieben oder gelöscht, um sicherzustellen, dass auch in Backups enthaltene Daten nicht länger als notwendig gespeichert werden.

3. Organisatorische Maßnahmen zur begrenzten Speicherung

- **Regelmäßige Überprüfung:** Wir führen regelmäßige Überprüfungen der gespeicherten Daten durch, um sicherzustellen, dass diese nicht länger als notwendig aufbewahrt werden.
- **Schulungen der Mitarbeiter:** Unsere Mitarbeiter werden regelmäßig im Umgang mit den Speicherrichtlinien geschult, um sicherzustellen, dass sie die Vorgaben zur begrenzten Speicherdauer einhalten.

4. Dokumentation und Nachweisbarkeit

- **Dokumentation der Speicherfristen:** Alle festgelegten Speicherfristen und die zugrunde liegenden Gründe werden dokumentiert. Dies dient als Nachweis für die Einhaltung des Grundsatzes der begrenzten Speicherdauer.

5. Ausnahmen und Sonderfälle

- **Rechtliche Aufbewahrungspflichten:** Falls gesetzliche Aufbewahrungspflichten (z. B. steuerrechtliche Vorschriften) bestehen, werden die betroffenen Daten nur so lange gespeichert, wie dies gesetzlich vorgeschrieben ist.
- **Fehleranalyse und Incident Management:** Im Falle von technischen Problemen oder Sicherheitsvorfällen können Daten über die reguläre Speicherfrist hinaus aufbewahrt werden, um die Ursachen zu analysieren und zukünftige Vorfälle zu verhindern. In solchen Fällen werden die Daten nach Abschluss der Analyse umgehend gelöscht.

6. Transparenz gegenüber Kunden

- **Information der Kunden:** Wir informieren unsere Kunden transparent über die von uns gespeicherten Daten und die festgelegten Speicherfristen. Dies erfolgt im Rahmen unserer Datenschutzerklärung und der Vertragsvereinbarungen.
- **Auskunftsrecht:** Kunden können jederzeit Auskunft über die bei uns gespeicherten Daten und die geplanten Löschfristen verlangen.

Maßnahmen zur Gewährleistung der Rechenschaftspflicht

Um die Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO zu erfüllen, haben wir umfassende technische und organisatorische Maßnahmen implementiert, die sicherstellen, dass wir die Einhaltung der datenschutzrechtlichen Anforderungen nachweisen können. Diese Maßnahmen umfassen die folgenden Aspekte:

1. Dokumentation der Verarbeitungstätigkeiten

- **Verzeichnis von Verarbeitungstätigkeiten:** Wir führen ein Verzeichnis aller Verarbeitungstätigkeiten, die personenbezogene Daten betreffen. Dieses Verzeichnis enthält Angaben zu den Verarbeitungszwecken, den betroffenen Datenkategorien, den Empfängern der Daten und den Speicherfristen.
- **Dokumentation der Auftragsverarbeitung:** Für alle Auftragsverarbeitungen, die wir im Namen unserer Kunden durchführen, bieten wir klare Verträge (Auftragsverarbeitungsverträge, AVV) an, in denen die Verantwortlichkeiten und Pflichten beider Parteien festgelegt sind.

2. Richtlinien und Verfahren

- **Datenschutzrichtlinien:** Wir haben umfassende Datenschutzrichtlinien entwickelt, die die Grundsätze der DSGVO (z. B. Datenminimierung, Speicherbegrenzung, Transparenz) in unseren Geschäftsprozessen verankern.
- **Verfahrensanweisungen:** Klare Verfahrensanweisungen für die Durchführung von Datenschutz-Folgenabschätzungen (DSFA), die Meldung von Datenschutzverletzungen und die Wahrung der Betroffenenrechte.

3. Schulungen und Sensibilisierung

- **Regelmäßige Schulungen:** Alle Mitarbeiter werden regelmäßig in den Bereichen Datenschutz und Informationssicherheit geschult, um das Bewusstsein für die datenschutzrechtlichen Anforderungen zu stärken.
- **Spezielle Schulungen für verantwortliche Personen:** Mitarbeiter, die mit der Verarbeitung personenbezogener Daten betraut sind, erhalten spezielle Schulungen zu den relevanten Datenschutzbestimmungen und -verfahren.

4. Technische Maßnahmen zur Nachweisbarkeit

- **Verschlüsselung und Zugangskontrolle:** Der Zugriff auf personenbezogene Daten ist durch Verschlüsselung und rollenbasierte Zugriffsrechte (RBAC) geschützt. Diese Maßnahmen werden dokumentiert und regelmäßig überprüft.

6. Meldung von Datenschutzverletzungen

- **Incident Response Plan:** Wir haben einen Incident Response Plan entwickelt, der klare Verfahren für die Erkennung, Meldung und Behebung von Datenschutzverletzungen definiert.
- **Dokumentation von Vorfällen:** Alle Datenschutzverletzungen werden dokumentiert, einschließlich der ergriffenen Maßnahmen und der Kommunikation mit den betroffenen Personen und Aufsichtsbehörden.

7. Zusammenarbeit mit Aufsichtsbehörden

- **Transparenz und Kooperation:** Wir arbeiten transparent und kooperativ mit den zuständigen Datenschutzaufsichtsbehörden zusammen und stellen auf Anfrage alle erforderlichen Informationen zur Verfügung.
- **Meldepflichten:** Wir erfüllen alle gesetzlichen Meldepflichten im Falle von Datenschutzverletzungen oder anderen relevanten Vorfällen.

8. Regelmäßige Überprüfung und Audits

- **Interne Audits:** Regelmäßige interne Audits zur Überprüfung der Einhaltung der datenschutzrechtlichen Anforderungen.

9. Dokumentation und Berichterstattung

- **Dokumentation aller Maßnahmen:** Alle technischen und organisatorischen Maßnahmen, Richtlinien und Verfahren werden dokumentiert, um eine nachvollziehbare Grundlage für die Rechenschaftspflicht zu schaffen.
- **Berichterstattung an die Geschäftsleitung:** Regelmäßige Berichterstattung an die Geschäftsleitung über den Status der Datenschutzmaßnahmen, identifizierte Risiken und durchgeführte Verbesserungen.

Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung

Um die Anforderungen an die Datenübertragbarkeit gemäß Art. 20 DSGVO und die Löschung personenbezogener Daten gemäß Art. 17 DSGVO zu erfüllen, haben wir technische und organisatorische Maßnahmen implementiert. Da wir in der Regel keine personenbezogenen Daten unserer Kunden speichern, sondern nur im Rahmen der Fernwartung auf deren Systeme zugreifen, konzentrieren sich unsere Maßnahmen auf die folgenden Aspekte:

1. Datenübertragbarkeit

- **Strukturierte Datenformate:** Falls wir personenbezogene Daten verarbeiten, stellen wir sicher, dass diese in einem strukturierten, gängigen und maschinenlesbaren Format (z. B. JSON, XML, CSV) gespeichert werden, um die Datenübertragbarkeit zu erleichtern.
- **Unterstützung bei Datenübertragungen:** Auf Anfrage unterstützen wir unsere Kunden bei der Übertragung ihrer Daten an einen anderen Verantwortlichen, sofern dies technisch machbar ist und keine Rechte Dritter entgegenstehen.

2. Löschung personenbezogener Daten

- **Technische Maßnahmen:**
  - **Sichere Löschverfahren:** Bei der Löschung von Daten verwenden wir Löschverfahren, um sicherzustellen, dass die Daten vollständig und unwiederbringlich gelöscht werden.
  - **Backup-Rotation:** Backups werden in regelmäßigen Abständen überschrieben oder gelöscht, um sicherzustellen, dass auch in Backups enthaltene Daten nicht länger als notwendig gespeichert werden.
- **Organisatorische Maßnahmen:**
  - **Löschrichtlinien:** Wir haben interne Richtlinien festgelegt, die die Löschung personenbezogener Daten regeln. Diese Richtlinien berücksichtigen die gesetzlichen Aufbewahrungspflichten und die betrieblichen Erfordernisse.
  - **Schulungen der Mitarbeiter:** Unsere Mitarbeiter werden regelmäßig im Umgang mit den Löschrichtlinien geschult, um sicherzustellen, dass sie die Vorgaben zur Löschung personenbezogener Daten einhalten.

3. Bearbeitung von Betroffenenanfragen

- **Anfragen zur Datenübertragbarkeit:** Anfragen von Betroffenen zur Datenübertragbarkeit werden innerhalb der gesetzlichen Fristen bearbeitet. Wir stellen sicher, dass die Daten in einem gängigen Format bereitgestellt werden und keine Rechte Dritter entgegenstehen.
- **Löschungsanfragen:** Anfragen von Betroffenen zur Löschung ihrer personenbezogenen Daten werden unverzüglich bearbeitet, sofern keine gesetzlichen Aufbewahrungspflichten oder berechtigten Interessen entgegenstehen. Die Löschung wird dokumentiert, und die betroffene Person wird über die Durchführung informiert.

4. Transparenz gegenüber Kunden

- **Information der Kunden:** Wir informieren unsere Kunden transparent über ihre Rechte auf Datenübertragbarkeit und Löschung. Dies erfolgt im Rahmen unserer Datenschutzerklärung.

- **Auskunftsrecht:** Kunden können jederzeit Auskunft über die bei uns gespeicherten Daten und die geplanten Löschfristen verlangen.

ANHANG IV

Unterauftragsverarbeiter

Der Auftragsnehmer nimmt für die Verarbeitung von Daten im Auftrag des Verantwortlichen Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“). Dabei handelt es sich um nachfolgende Unternehmen:

AnyDesk Software GmbH
Türlenstraße 2
70191 Stuttgart

Art der Leistung: Nutzung eines Tools für Fernwartungsdienstleistungen.
Die Datenschutzerklärung befindet sich hier: https://anydesk.com/de/datenschutz

alternativ

RustDesk
Canberra Drive
YishunDesk
Singapur

Art der Leistung: Nutzung eines Tools für Fernwartungsdienstleistungen.
Die Datenschutzerklärung befindet sich hier: https://rustdesk.com/privacy/