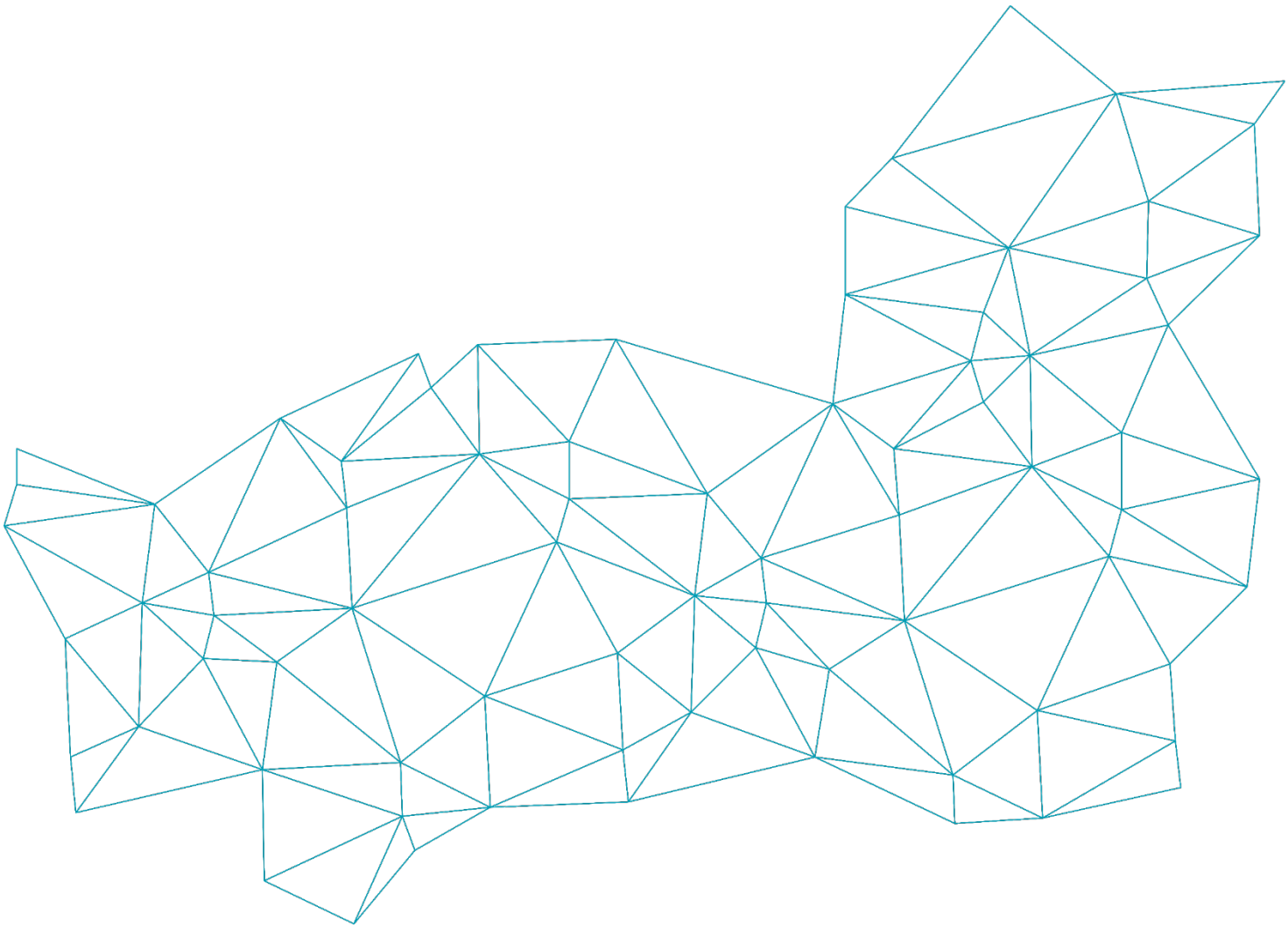
AUFTRAGSVERARBEITUNGS-VERTRAG (AVV)

NACH ART. 28 ABS. 7 DS-GVO



con terra GmbH
Martin-Luther-King-Weg 20
48155 Münster
conterra.de

con terra
locate the future

Inhalt

ABSCHNITT I **1**
Klausel 1 Zweck und Anwendungsbereich 1
Klausel 2 Unabänderbarkeit der Klauseln 1
Klausel 3 Auslegung 1
Klausel 4 Vorrang 2
Klausel 5 Kopplungsklausel 2
ABSCHNITT II PFLICHTEN DER PARTEIEN **2**
Klausel 6 Beschreibung der Verarbeitung 2
Klausel 7 Pflichten der Parteien 2
7.1. Weisungen 2
7.2. Zweckbindung 3
7.3. Dauer der Verarbeitung personenbezogener Daten 3
7.4. Sicherheit der Verarbeitung 3
7.5. Sensible Daten 3
7.6. Dokumentation und Einhaltung der Klauseln 3
7.7. Einsatz von Unterauftragsverarbeitern 4
7.8. Internationale Datenübermittlungen 5
Klausel 8 Unterstützung des Verantwortlichen 5
Klausel 9 Meldung von Verletzungen des Schutzes personenbezogener Daten 6
9.1. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten 6
9.2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten 7
ABSCHNITT III SCHLUSSBESTIMMUNGEN **7**
Klausel 10 Verstöße gegen die Klauseln und Beendigung des Vertrags 7
ANHANG I Liste der Parteien **9**
ANHANG II Beschreibung der Verarbeitung **10**
ANHANG III Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten **11**
ANHANG IV Liste der Unterauftragsverarbeiter **12**
Anhang V Regelung zum Umgang mit kurzfristigen Auftragsverarbeitungen und Unterauftragsverarbeitern **13**

Standardvertragsklauseln

ABSCHNITT I

Klausel 1
Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung sichergestellt werden.

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

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

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

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

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

Klausel 2
Unabänderbarkeit der Klauseln

a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3
Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4
Vorrang

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

Klausel 5
Kopplungsklausel

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

b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.

c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

ABSCHNITT II
PFLICHTEN DER PARTEIEN

Klausel 6
Beschreibung der Verarbeitung

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

Klausel 7
Pflichten der Parteien

7.1. Weisungen

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2. Zweckbindung

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

7.3. Dauer der Verarbeitung personenbezogener Daten

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

7.4. Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5. Sensible Daten

Falls die Verarbeitung 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) ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG: Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens (siehe Anhang V) im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

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

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen

Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8. Internationale Datenübermittlungen

a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8
Unterstützung des Verantwortlichen

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko

zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

4) Verpflichtungen gemäß 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 Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

ABSCHNITT III
SCHLUSSBESTIMMUNGEN

Klausel 10
Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

    1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;

3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

ANHANG I
Liste der Parteien

Verantwortliche(r):
Nutzende des Onlineservices https://dataservices.conterra.de/apps

Auftragsverarbeiter:
con terra GmbH
Martin-Luther-King-Weg 20, 48155 Münster
Name, Funktion und Kontaktdaten der Kontaktperson: Periklis Kremetis, datenschutz@conterra.de

Datenschutzbeauftragter von con terra GmbH:
DataCo GmbH, Sandstrasse 33, 80335 München
datenschutz@conterra.de

Der Vertrag erlangt Rechtswirksamkeit durch elektronische Bestätigung durch den Verantwortlichen. Eine Unterzeichnung in Schriftform ist nicht erforderlich.

ANHANG II
Beschreibung der Verarbeitung

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

Mitarbeiter, Grundstückbesitzer, Lieferanten und Dienstleister, Eigentümer von Kulturgütern oder historischen Objekten, Bürger / Anwohner, Endnutzer / Kunden, Institutionelle Partner und öffentliche Stellen. Darüber hinaus können weiteren Personen betroffen sind, deren personenbezogene Daten vom Verantwortlichen zur Verarbeitung in die Systeme eingebracht werden.

Kategorien personenbezogener Daten, die verarbeitet werden

Stammdaten (Name, Vorname, Titel, Geschlecht, Geburtsdatum), Kontaktdaten (Adresse, Telefonnummer, E-Mail-Adresse, ggf. dienstliche Kontaktdaten), Beschäftigtendaten, (Mitarbeiter-ID, Funktion, Abteilung, Arbeitsort, Arbeitszeiten, Zutritts- oder Berechtigungsinformationen), Grundstücks- und Immobiliendaten (Grundstücksnummer, Lage-/Geokoordinaten, Nutzungsart, Eigentumsverhältnisse, Wertangaben, Flächenangaben), Vertrags- und Lieferantendaten (Lieferanten-ID, Vertragsnummern, Leistungsumfang, Ansprechpartner, Bank- oder Abrechnungsinformationen), Nutzungs- und Protokolldaten (Logfiles, Zugriffsdaten, Nutzerkennung, IP-Adressen, Zeitstempel), Sonstige Kommunikationsdaten (Schriftverkehr, Notizen zu Gesprächen, Angaben zu Ansprechpartnern bei Behörden oder Partnerorganisationen). Darüber hinaus können alle weiteren personenbezogenen Daten verarbeitet werden, die der Verantwortliche im Rahmen der Nutzung der Systeme einträgt oder zur Verarbeitung bereitstellt.

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

Der Service ist nicht dafür vorgesehen, im Rahmen seiner bestimmungsgemäßen Nutzung besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO zu verarbeiten.

Art der Verarbeitung

Die Verarbeitung personenbezogener Daten erfolgt über den Cloud-Dienst des Auftragnehmers. Dazu gehören insbesondere die automatisierte Konvertierung, Migration und Speicherung der Daten sowie deren Bereitstellung für den Verantwortlichen zum Download.

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

Die Verarbeitung erfolgt zum Zweck der automatisierten Konvertierung, Migration, Speicherung und Bereitstellung von Daten des Verantwortlichen durch den Cloud-Dienst des Auftragnehmers.

Dauer der Verarbeitung

Die personenbezogenen Daten werden für die Dauer der Verarbeitung (in der Regel bis zu 24 Stunden) sowie bis zu 72 Stunden nach Abschluss der Konvertierung gespeichert und anschließend automatisch gelöscht.

Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.

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

Siehe Anlage „TOM con_terra_GmbH 2026 04 24.pdf“

ANHANG IV
Liste der Unterauftragsverarbeiter

Derzeit sind keine Unterauftragsverarbeiter vorgesehen.

Anhang V
Regelung zum Umgang mit kurzfristigen Auftragsverarbeitungen und Unterauftragsverarbeitern

1. Gegenstand dieses Anhangs

Dieser Anhang konkretisiert die in Klausel 7.7 der Standardvertragsklauseln (Einsatz von Unterauftragsverarbeitern) geregelte Informationspflicht über Änderungen an Unterauftragsverarbeitern für den Fall, dass die Verarbeitung personenbezogener Daten ausschließlich kurzfristig und automatisiert erfolgt.

2. Besonderheit der Verarbeitung

Die im Rahmen dieses Vertrags durchgeführten Verarbeitungsvorgänge sind technisch bedingt kurzfristig (regelmäßig unter 4 Tage) und vollständig automatisiert. Eine vorherige individuelle Information des Verantwortlichen über Änderungen an Unterauftragsverarbeitern ist aufgrund des zeitlich engen und dynamischen Prozessablaufs faktisch nicht möglich.

3. Informationsverfahren

Der Auftragsverarbeiter führt eine aktuelle Liste aller eingesetzten Unterauftragsverarbeiter öffentlich abrufbar oder auf Anfrage verfügbar ist. Derzeit sind keine Unterauftragsverarbeiter vorgesehen.

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich nachträglich über jede wesentliche Änderung dieser Liste, insbesondere über die Hinzufügung oder den Austausch von Unterauftragsverarbeitern.

4. Einspruchsrecht

Der Verantwortliche kann innerhalb von 14 Kalendertagen nach Kenntnisnahme einer Änderung Einspruch gegen die Beauftragung eines neuen Unterauftragsverarbeiters erheben, sofern er hierfür berechtigte datenschutzrechtliche Gründe vorbringt. Erfolgt kein Widerspruch innerhalb dieser Frist, gilt die Änderung als genehmigt.

5. Wahrung des Zwecks von Art. 28 Abs. 2 DSGVO

Diese Regelung wahrt den in Art. 28 Abs. 2 DSGVO vorgesehenen Zweck der Kontrolle durch den Verantwortlichen, berücksichtigt jedoch die technische Eigenart der kurzfristigen, automatisierten Verarbeitung. Sie stellt sicher, dass Transparenz, Nachvollziehbarkeit und Widerspruchsmöglichkeit weiterhin gewährleistet bleiben.

***** Ende des Dokuments *****

DataGuard

con terra GmbH

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Stand: 24.04.2026

IT & Sicherheit

1. Physische Sicherheit der Infrastruktur
2. Serversysteme
3. Netzwerkstruktur
4. Business Continuity
5. Endgeräte
6. Datentransfers
7. Personal
8. Organisation
9. Videoüberwachung

Vorwort

Das Dokument beschreibt die verbindlichen technischen und organisatorischen Maßnahmen, die im Zusammenhang mit den von der Organisation durchgeführten Datenverarbeitungsvorgängen festgelegt wurden. Die beschriebenen Maßnahmen spiegeln somit das Datenschutz- und Datensicherheitskonzept in der Praxis der Organisation wider.

Datenschutz- und Datensicherheitskonzept

Der folgende Maßnahmenkatalog beschreibt die zu treffenden technischen und organisatorischen Einzelmaßnahmen gemäß den einschlägigen gesetzlichen Bestimmungen. Diese Bestimmungen verpflichten Unternehmen die Datenverarbeitung personenbezogener Daten durch angemessene, technische und organisatorische Maßnahmen abzusichern und personenbezogene Daten nach Möglichkeit zu pseudonymisieren. Die getroffenen Maßnahmen müssen dabei dem Risiko des jeweiligen Datenverarbeitungsvorgangs Rechnung tragen und dem derzeitigen Stand der Technik entsprechen. Diese Anforderungen erfüllt der Auftragnehmer durch ein wirksames Zusammenspiel aus Datenschutzmanagement und Informationssicherheitsmanagement und hat angemessene Maßnahmen zur Absicherung der Datenverarbeitungsvorgänge getroffen. Insbesondere die Schutzwerte: Verfügbarkeit, Vertraulichkeit, Integrität und Belastbarkeit. Den Schutzwerten werden dabei folgende informationssicherheitsrelevanten Definitionen zugrunde gelegt:

- Vertraulichkeit: Daten, Informationen und Programme sind vor unberechtigten Zugriffen und unbefugter Preisgabe zu schützen.
- Integrität: Der Begriff Integrität bezieht sich auf die Korrektheit der verarbeiteten Informationen und Daten.
- Verfügbarkeit: Der Begriff der Verfügbarkeit bezieht sich auf Informationen, Daten, Applikationen sowie Systeme und betrifft deren Funktionsfähigkeit bzw. Abrufbarkeit.
- Belastbarkeit: Die Belastbarkeit stellt als besonderen Aspekt der Verfügbarkeit die Anforderung, dass Systeme auch im Störfall, Fehlerfall oder bei hoher Belastung möglichst widerstandsfähig ausgestaltet sein müssen.

Physische Sicherheit der Infrastruktur

Physische Sicherheit beschreibt Maßnahmen zur Verhinderung eines unbefugten Zutrittes, einer Beschädigung oder Beeinträchtigung von Informationswerten, personenbezogenen Daten und informationsverarbeitenden Einrichtungen eines Unternehmens.

Standort / Unternehmensräumlichkeiten

Die Unternehmensräumlichkeiten sind vom öffentlichen Bereich abgegrenzt durch:

• Abschließbare Tür

• Abgetrennte Räumlichkeiten in Gebäudekomplex

Es befinden sich keine weiteren Parteien im Gebäude, die Zutritt zu den Unternehmensräumlichkeiten haben.

Im Unternehmen wird ein Zutrittskontrollsystem eingesetzt, um den Zutritt zu Räumen, in denen personenbezogene Daten verarbeitet werden, zu schützen.

Das Unternehmensgelände bzw. Teile davon werden durch einen Pförtner oder Wachschutz bewacht.

Im Unternehmen erfolgt die Besucheranmeldung durch:

• Besucherausweise

• Besucherbuch

• Begleitung durch Mitarbeiter

• Empfang / Rezeption

• Klingel

Im Unternehmen sind Räume abschließbar, in denen Zugriff auf personenbezogene Daten möglich ist.

Im Unternehmen sind personenbezogene Daten in Bereichen mit Publikumsverkehr nicht frei zugänglich.

Im Unternehmen werden Arbeitsplätze zur Verarbeitung besonderer Kategorien personenbezogener Daten (z. B. Bewerber-/Gesundheitsdaten) räumlich von anderen Arbeitsplätzen getrennt.

Es existieren besondere Sicherheitsbereiche.

Im Unternehmen existiert ein Berechtigungskonzept für den Zutritt zu Sicherheitsbereichen.

Im Unternehmen ist die Zutrittsberechtigungsstruktur für die Sicherheitsbereiche auf das Notwendigste beschränkt.

Im Unternehmen existiert eine unternehmensweite Richtlinie bzw. Handlungsanweisungen in schriftlicher Form zur Gebäudesicherheit.

Serversysteme

Dieser Prozess bezieht sich auf Serversysteme, die mit besonderer Sorgfalt gesichert werden müssen, da Sicherheitsverletzungen dort aufgrund der großen Menge an personenbezogenen Daten in der Regel enorme Folgen haben können.

Server-Infrastruktur

Es werden virtualisierte Server im Unternehmen eingesetzt.

Netzwerkstruktur

Netzwerkstruktur beschreibt den Aufbau und Zusammenschluss von informationsverarbeitenden Einrichtungen im Unternehmen, sowie die Maßnahmen zum Schutz von Information in Netzwerken.

Netzwerkdokumentation

Im Unternehmen existiert eine Netzwerkdokumentation.

Die Netzwerkdokumentation wird regelmäßig überprüft und Soll- und Ist-Zustand abgeglichen, um etwaige Lücken aufzuzeigen.

Netzwerkarchitektur

Das WLAN ist wie folgt verschlüsselt:

• WPA 3

Es besteht eine Client-Sever-Segmentierung.

Es gibt eine Trennung "Internet/öffentliches Netz".

• Nicht interne Geräte können keinen Zugang zum internen Netzwerk/sicherheitszonen erhalten.

Netzwerkfernzugriff

Im Unternehmen werden zum Schutz des Netzwerks Firewalls eingesetzt.

Folgende Arten von Firewalls werden eingesetzt:

• Software-Firewall(s)

Im Unternehmen sind Firewall(s) und Switches an die unterbrechungsfreie Stromversorgung angeschlossen.

Im Unternehmen werden moderne Netzwerkgeräte (Hubs, Switches) eingesetzt.

• Es werden sichere Verfahren für den Fernzugriff auf das Unternehmensnetzwerk genutzt.

Folgende sichere Verfahren für den Fernzugriff werden genutzt:

• VPN (Virtual Private Network)

Dieser ist an folgender Stelle platziert:

• Hinter der Firewall

Der Fernzugriff ist wie folgt abgesichert:

• Radius-Server

Im Unternehmen wurden Mitarbeiter, die von außerhalb auf das Netzwerk zugreifen, auf die Einhaltung einschlägiger Datenschutzvorschriften an ihrem Arbeitsplatz hingewiesen.

Im Unternehmen werden Fernwartungen durchgeführt.

Im Unternehmen wird jeder Fernwartungszugriff individuell freigegeben.

Netzwerküberwachung

Im Unternehmen wird eine Software zur Überwachung des Netzwerks und der Anwendungen verwendet.

Business Continuity

Business Continuity beschreibt die organisatorischen, technischen und personellen Maßnahmen, die zur Absicherung und Fortführung des Kerngeschäfts eines Unternehmens nach Eintritt eines Notfalls bzw. eines Sicherheitsvorfalls notwendig sind.

Wiederherstellbarkeit

Im Unternehmen werden (regelmäßig) Datensicherungen der relevanten Systeme durchgeführt.

Im Unternehmen ist für die Durchführung von Sicherungen verantwortlich:

• Externer Dienstleister

• Cloud-Anbieter

Die Wiederherstellungsmöglichkeiten umfassen folgende Bereiche:

• Benutzerkonten

• Daten

• Installationen

• Konfigurationen (Einstellungen und Freigaben)

• Log-Daten

• Systemdateien- und Datencontainer

Im Unternehmen wird folgende Art der Datensicherung durchgeführt:

• Differenzielle Sicherung

• Inkrementelle Sicherung

• Komplett-/Vollsicherung

• Speicherabbildsicherung (Image Backup)

Im Unternehmen werden Sicherungen in einem separaten Brandabschnitt gelagert.

Im Unternehmen werden Datensicherungsverfahren regelmäßig getestet und bei Bedarf angepasst.

Im Unternehmen wurde eine schriftliche Richtlinie zu Sicherungen definiert.

Im Unternehmen werden Datensicherungen verschlüsselt gespeichert.

Notfallvorsorge

Im Unternehmen wurde ein schriftlicher Notfallplan (Disaster Recovery Plan) definiert.

Im Unternehmen wurde der Notfallplan auch in ausgedruckter Form sicher abgelegt.

Im Unternehmen wurde der Notfallplan bereits auf Funktionalität erfolgreich getestet.

• Verantwortliche Personen wurden definiert und sensibilisiert.

Im Unternehmen existiert ein schriftliches Berechtigungskonzept, einschließlich Vertretungsregelungen, für Notfallsituationen.

Im Unternehmen wurde für den Notfall ein Administratorenzugang hinterlegt.

Im Unternehmen wird der Zugriff auf die hinterlegten Administratorenzugänge protokolliert.

Im Unternehmen sind kritische Systeme und ggf. die Infrastruktur redundant ausgelegt.

Endgeräte

Endgeräte umfassen die für die tägliche Arbeit genutzten Clients und Datenträger im Unternehmen. Bei der Handhabung dieser Endgeräte soll die unerlaubte Offenlegung, Veränderung, Entfernung oder Zerstörung von Information und personenbezogenen Daten verhindert werden.

Clientstruktur und –management

Im Unternehmen wird ein zentrales Endpoint Management für Computer verwendet.

Im Unternehmen werden Sicherheits- und Softwareupdates der mobilen Endgeräte regelmäßig durchgeführt.

Im Unternehmen existiert ein Freigabeprozess für die Installation und Verwendung von Software.

Im Unternehmen wird ein Bestandsverzeichnis der verwendeten Endgeräte geführt.

Im Unternehmen existiert ein dokumentierter Prozess zur Ausgabe von unternehmenseigenen Gegenständen an Mitarbeiter.

Im Unternehmen wird sichergestellt, dass sämtliche unternehmenseigene Gegenstände mit Bezug zu personenbezogenen Daten von einer ausscheidenden Person zurückgefordert werden.

Geräte werden über ein geregeltes Wiedereingliederungsmanagement wieder dem IT-Inventar zur Weiterverwendung zugeführt.

Datenträgermanagement

Im Unternehmen sind Richtlinien in schriftlicher Form zum Umgang mit mobilen Datenträgern definiert.

Im Unternehmen existiert eine Sicherheitsrichtlinie für mobile Endgeräte.

Im Unternehmen existiert eine Richtlinie zur sicheren und sachgerechten Aufbewahrung von mobilen Datenträgern.

Im Unternehmen existiert eine Richtlinie für die Entsorgung von Datenträgern.

Im Unternehmen wurden Benutzer von mobilen Endgeräten auf die geeignete Aufbewahrung (z. B. in einem verschließbaren Container) verpflichtet.

Im Unternehmen werden mobile Endgeräte außerhalb der Nutzungszeiten gegen Diebstahl gesichert bzw. verschlossen aufbewahrt.

Im Unternehmen ist ein Prozess definiert, wie sich Beschäftigte verhalten sollen, falls ein Datenträger abhandenkommt.

Im Unternehmen werden Datenträger vor der Benutzung auf Schadsoftware geprüft.

Im Unternehmen werden Dateien nur auf Wechseldatenträger übertragen, wenn diese Dateien zuvor auf Schadsoftware geprüft worden sind.

Im Unternehmen werden Datenträger hinsichtlich ihrer Vertraulichkeit in verschiedene Schutzbedarfsstufen eingeteilt.

Im Unternehmen werden die in IT-Systemen verbauten Datenträger verschlüsselt.

Im Unternehmen besteht die Möglichkeit zur Fernlöschung von Daten auf mobilen Endgeräten.

Diese Endgeräte verfügen über Zugriffssperren.

Beschäftigte sind dazu angehalten personenbezogene Daten fachgerecht zu entsorgen.

• Daten elektronischer Datenträger werden sicher gelöscht, um eine sichere Wiederverwendung zu gewährleisten.

Im Unternehmen werden elektronische Datenträger sicher gelöscht.

Im Unternehmen werden Datenträger (auch Papierakten) regelmäßig entsorgt.

Im Unternehmen werden Papierakten mit Hilfe eines Schredders vernichtet.

Im Unternehmen werden zur Entsorgung gesammelte schutzbedürftige Datenträger vor unberechtigtem Zugriff geschützt.

Im Unternehmen werden elektronische Datenträger vor deren Entsorgung physisch zerstört.

Der externe Dienstleister verfügt über folgende Zertifizierungen:

• Im Unternehmen wird zur Entsorgung von Datenträgern ein nach der DIN 66399 zertifizierter Dienstleister eingesetzt.

Datentransfers

Dieses Verfahren bezieht sich auf Datenübermittlungen innerhalb Ihrer Organisation und unter Einbeziehung Dritter. Dies ist insbesondere im Zusammenhang mit der Übermittlung personenbezogener Daten relevant.

Datenübertragung & Kommunikation

Im Unternehmen werden zum Versand von Email digitale Signaturen eingesetzt.

Folgende Verschlüsselungsverfarhen werden beim Emailversand benutzt:

• Im Unternehmen werden Emails bei der Übertragung mit entsprechenden Verfahren/Protokollen (S/MIME) verschlüsselt.

Im Unternehmen werden langfristig archivierte E-Mails verschlüsselt gespeichert.

Einzelne Daten-Objekte, wie z.B. Container, Ordner oder einzelne Dateien (File & Folder Encryption), werden vor dem Datentransfer verschlüsselt.

Es wurde mit allen Dienstleistern ein Auftragsverarbeitungsvertrag geschlossen.

Personal

Personal umfasst die Sensibilisierung der Mitarbeiter zu Informationssicherheits- und Datenschutzrelevanten Themen, sowie die Berechtigungen und Maßnahmen zur Authentifizierung der Mitarbeiter beim Zugriff auf unternehmensintern IT-Systeme und Dienste.

Mitarbeiter Awareness & Sensibilisierung

Im Unternehmen werden Beschäftigte auf die Einhaltung von Verhaltensregeln gemäß den Grundsätzen der DSGVO verpflichtet.

Im Unternehmen werden die Beschäftigen zu datenschutzrechtlichen Themen geschult.

Im Unternehmen werden Schulungen der Beschäftigten zur Sensibilisierung zum Datenschutz regelmäßig durchgeführt.

Im Unternehmen werden die Beschäftigten regelmäßig über Neuigkeiten zum Datenschutz und IT-Sicherheit informiert.

Im Unternehmen erfolgt eine Sensibilisierung des Personals zum Umgang mit externen Personen/Unternehmen/Parteien.

Im Unternehmen sind Beschäftigten verpflichtet, personenbezogene Daten bei Verlassen des Arbeitsplatzes vor unbefugtem Zugriff zu schützen (sog. Clean-Desk-Policy).

Im Unternehmen sind relevante Informationen, Richtlinien und Handlungsempfehlungen für die Mitarbeiter leicht auffindbar.

IT-Personal und Administratoren werden im Unternehmen ausreichend sensibilisiert und geschult.

Berechtigungsmanagement

Im Unternehmen existiert ein geregelter Prozess zur zentralen Verwaltung von Benutzeridentitäten, insbesondere zur Anlage (z. B. neuer Mitarbeiter), Änderung (z. B. Namenswechsel nach Heirat) und Löschung (z. B. Ausscheiden Mitarbeiter).

Im Unternehmen existiert ein formalisiertes Berechtigungskonzept, welches die Rollen und Rechte der Mitarbeiter dokumentiert.

Im Unternehmen wird die Vergabe sowie der Entzug von Zugangs- und Zugriffsberechtigungen für IT-Systeme dokumentiert.

Im Unternehmen wird ein zentraler Verzeichnisdienst (LDAP, AD, etc.) für die Berechtigungsattestierung eingesetzt.

Im Unternehmen werden regelmäßig die zugelassenen Benutzer, angelegte Benutzergruppen sowie die Rechteprofile geprüft

Im Unternehmen ist die Dokumentation der zugelassenen Benutzer, Benutzergruppen und Rechteprofile vor unbefugtem Zugriff geschützt.

Im Unternehmen erfolgt die Vergabe von Zugangs- und Zugriffsberechtigungen anhand der Funktion der Zugangs- bzw. Zugriffsberechtigten.

Im Unternehmen existiert ein Funktionstrennungsprozess, um Berechtigungen zu vermeiden, die miteinander in Konflikt stehen.

Im Unternehmen wird sichergestellt, dass sämtliche Zugangsberechtigungen und Zugriffsberechtigungen einer ausscheidenden Person zeitnah gesperrt und ggf. gelöscht werden.

Im Unternehmen wurde für alle IT-Systeme und IT-Netze Administratoren sowie deren Stellvertreter bestimmt.

Im Unternehmen werden spezielle Administratorenkonten eingesetzt.

Im Unternehmen werden die Aktivitäten innerhalb der Administratorenkonten protokolliert.

Authentifizierungsverfahren

Im Unternehmen wird ein Passwort-Manager eingesetzt.

Der eingesetzte Passwort-Manager bietet eine ausreichende Zugriffskontrolle und eine verschlüsselte Speicherung

Im Unternehmen wird eine Multi-Faktor-Authentifizierung eingesetzt.

Im Unternehmen wird ein Single-Sign-On Verfahren zum Login eingesetzt.

Im Unternehmen wird zur Anmeldung mittels Single-Sign-On eine Multi-Faktor-Authentifizierung eingesetzt.

Im Unternehmen werden Benutzeraccounts nach Inaktivität automatische gesperrt (Bildschirmsperre).

Im Unternehmen werden die Benutzerkonten der IT-Systeme, auf denen personenbezogene Daten verarbeitet werden, durch Passwörter geschützt.

Im Unternehmen werden Falscheingaben von Benutzern protokolliert.

Folgende Personen werden informiert:

• IT-Administrator

Im Unternehmen müssen Initialpasswörter bei der ersten Anmeldung geändert werden.

Im Unternehmen werden Benutzerkonten nach einer definierten Anzahl von Falschanmeldungen gesperrt.

Im Unternehmen erfolgt eine Vergabe von eindeutigen Kennungen für individuelle Nutzer von IT-Systemen, durch die personenbezogene Daten verarbeitet werden.

Im Unternehmen existieren keine unverschlüsselten Passwortlisten.

Im Unternehme existieren konkrete Richtlinien für die Festlegung von Passwörtern oder systemseitige Forderung von Passwortanforderungen.

• Im Unternehmen gibt es eine Vorgabe für die Passwortzusammensetzung.

Im Unternehmen bestehen die Passwörter mindestens aus folgenden Bestandteilen:

• Buchstaben

• Zahlen

• Sonderzeichen

Im Unternehmen gibt es eine Vorgabe für die Passwortkomplexität.

Im Unternehmen gibt es eine Vorgabe für die Passwortlänge.

Im Unternehmen bestehen Passwörter aus mindestens 8 Zeichen.

Organisation

Organisation umfasst die unternehmensinternen Regelungen und Richtlinien zur Auswahl und dem Einsatz von externen Dienstleistern und Drittanbietertechnologien sowie zur Softwareentwicklung.

Auftragskontrolle

Mit allen Dienstleistern, die einen Teilbereich der Verarbeitung personenbezogener Daten auf die Weisung des Unternehmens übernehmen, wurde ein Auftragsverarbeitungsvertrag abgeschlossen.

• Mit allen Dienstleistern, deren Datenverarbeitungsprozesse in Drittländern außerhalb der EU stattfinden, wurden zusätzliche geeignete Garantien geschlossen, um den Datentransfer zusätzlich abzusichern.

Externe Dienstleister, die Zugriff auf personenbezogene Daten haben könnten, werden stets bei ihren Tätigkeiten überwacht.

Entwicklung und Auswahl von Software

Im Unternehmen werden Produktiv- und Entwicklungs-/Testsysteme voneinander getrennt.

Im Unternehmen wird der Zugang zum Source-Code bei der Entwicklung von Software beschränkt.

Im Unternehmen wurde ein Berechtigungskonzept in den Test- und Entwicklungsumgebungen umgesetzt.

Im Unternehmen wird eine Mandantenfähigkeit von entwickelter Software sichergestellt.

Reale Nutzerdaten werden nicht in Test- und Entwicklungsumgebungen genutzt.

Im Unternehmen wird Software regelmäßig aktualisiert und etwaige Schwachstellen geschlossen.

Sonstige organisatorische Maßnahmen

Im Unternehmen existiert ein IT-Sicherheitskonzept, welches die grundlegenden technischen und organisatorischen Maßnahmen darstellt, die im Unternehmen zur Gewährleistung von Datenschutz und Datensicherheit getroffen werden.

Im Unternehmen wurde ein Archivierungskonzept definiert, welches regelt, wie und wie lange Dokumente archiviert werden.

Im Unternehmen existiert ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen.

Im Unternehmen existiert ein Verfahren zur regelmäßigen Überprüfung und Aktualisierung der Konzepte und Dokumentationen zum

Datenschutz.

Im Unternehmen besteht die Möglichkeit auf Antrag personenbezogene Daten zu sperren und zu löschen

• Im Unternehmen wird jede Verarbeitung von personenbezogenen Daten protokolliert.

• Es gibt Unternehmen eine unternehmensweite Richtlinie zur Protokollierung.

• Im Unternehmen wird jede Löschung von personenbezogenen Daten protokolliert.

• Im Unternehmen werden die Protokolle über die Verarbeitung personenbezogener Daten spätestens am Ende des auf deren Generierung folgenden Jahres gelöscht.

Im Unternehmen existieren Anweisungen und Eskalationsprozesse bei Sicherheitsverletzungen.

Im Unternehmen erfolgt eine konsequente Dokumentation und Protokollierung von Sicherheitsvorkommnissen (Security Reporting).

Im Unternehmen erfolgt eine konsequente Einbindung des Datenschutzbeauftragten bei Sicherheitsfragen und -vorfällen.

Zertifizierungen

Das Unternehmen verfügt über folgende Zertifizierungen: ISO27001/2022

Videoüberwachung

Die Verarbeitung der personenbezogenen Daten findet im Rahmen der Videoüberwachung statt.

Videoüberwachung

Es ist sichergestellt, dass die Videodaten, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind, gelöscht werden.

• Die Kamera bietet nicht die Möglichkeit an, flexibel weitere Bereiche zu erfassen, z.B. durch Zoom oder Schwenkbarkeit des Bildwinkels.

Der Zugriff auf die Aufnahmen der Videoüberwachung ist eingeschränkt.

Der Zugriff zu den Aufnahmen ist durch ein Authentifizierungsverfahren gesichert.

• Die Aufnahmen werden in einem separaten Netzwerkabschnitt verarbeitet.

Die Videoaufnahmen werden verschlüsselt übertragen.

Regelmäßige Softwareupdates werden durchgeführt.

Updates werden wie folgt durchgeführt:

• Automatisiert