TolaData

TolaData GmbH
Standardvertragsklauseln / Auftragsverarbeitungs-Vertrag

Verbundene Richtlinien	TolaData Technische und Organisatorische Maßnahmen (TOMs)
Rechtliche Rahmenbedingungen	Allgemeine Datenschutzverordnung der Europäischen Union (DS-GVO)
Genehmigt von	CEO, Jo Bennett
Letzte Überarbeitung	September 2021

Abschnitt I - Zweck und Anwendungsbereich

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 III 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.

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 umfangreichen Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

3. 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.

4. Vorrang

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

5. Koppelungsklausel

a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.
b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.
c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

Abschnitt II - Pflichten der Parteien

6. Beschreibung der Verarbeitung

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

7. 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 einen Monat 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.

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.

9. Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1 Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

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

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);
b) bei der Einholung der folgenden Informationen, die gemäß [OPTION 1: Artikel 33 Absatz 3 der Verordnung (EU) 2016/679] oder 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

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.

TolaData

ANNEX I

Liste der Parteien

Verantwortlicher

Unternehmen: _____

Adresse: _____

_____

Vertreten von

Name(n): _____ _____

Position(en): _____ _____

Ort, Datum _____ _____

Unterschrift(en) _____ _____

Auftragsverarbeiter

Unternehmen: TolaData GmbH

Adresse: Ringbahnstraße 32-34

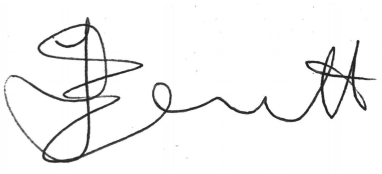
12099 Berlin (Germany)

Vertreten von

Namen: Jo Bennett Linda Kleemann

Positionen: CEO (Geschäftsführerin) CEO (Geschäftsführerin)

Ort, Datum Berlin , 28. September 2021



Digital unterschrieben
von Kleemann, Linda
Datum: 2021.09.29
19:14:42 +02'00'

Signatures _____ _____

Bitte unterschreiben Sie und senden Sie den unterschriebenen Scan per E-Mail an info@toladata.com

ANNEX II

1. Beschreibung der Verarbeitung

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden: Zu den betroffenen Personen gehören die Vertreter des für die Datenverarbeitung Verantwortlichen und die Endnutzer, einschließlich der Angestellten, Auftragnehmer, Mitarbeiter und Kunden des für die Datenverarbeitung Verantwortlichen. Zu den betroffenen Personen können auch Personen gehören, die versuchen, den Nutzern der vom Datenverarbeiter angebotenen Dienste personenbezogene Daten mitzuteilen oder zu übermitteln. TolaData nimmt zur Kenntnis, dass der Kunde je nach Nutzung der TolaData-Dienste auf eigene Verantwortung personenbezogene Daten von einer der folgenden Arten von Datensubjekten in die personenbezogenen Daten aufnehmen kann:

- Angestellte, Auftragnehmer und Zeitarbeiter (derzeitige, ehemalige und zukünftige) des Datenverantwortlichen;
- Mitarbeiter/Kontaktpersonen des für die Verarbeitung Verantwortlichen (natürliche Personen) oder Mitarbeiter, Auftragnehmer oder Zeitarbeitskräfte von juristischen Personen, die mit dem für die Verarbeitung Verantwortlichen zusammenarbeiten/Kontaktpersonen (derzeitige, zukünftige und ehemalige);
- Kunden (z. B. Begünstigte, Kunden, Klienten, Patienten, Besucher usw.) und andere betroffene Personen, die die Dienste des für die Verarbeitung Verantwortlichen in Anspruch nehmen;
- Partner, Interessenvertreter oder Personen, die aktiv mit Mitarbeitern des Datenverantwortlichen über Toladata.io zusammenarbeiten, kommunizieren oder anderweitig mit ihnen interagieren

Kategorien personenbezogener Daten, die verarbeitet werden : Die personenbezogenen Daten, die von den Vertretern und Endnutzern des für die Verarbeitung Verantwortlichen, einschließlich Mitarbeitern, Auftragnehmern, Mitarbeitern und Kunden, für die Nutzung von TolaData.io übermittelt werden, umfassen nur Kontaktinformationen und Authentifizierungsdaten. TolaData nimmt zur Kenntnis, dass der für die Verarbeitung Verantwortliche je nach Nutzung von TolaData.io durch den für die Verarbeitung Verantwortlichen auf eigene Verantwortung personenbezogene Daten aus einer der folgenden Kategorien in die personenbezogenen Daten aufnehmen kann:

- Grundlegende personenbezogene Daten (z.B. Geburtsort, Straßenname und Hausnummer (Adresse), Postleitzahl, Wohnort, Wohnsitzland, Mobiltelefonnummer, Vorname, Nachname, Initialen, E-Mail-Adresse, Geschlecht, Geburtsdatum), einschließlich grundlegender personenbezogener Daten über Familienmitglieder und Kinder;

- Authentifizierungsdaten (z. B. Benutzername, Passwort oder PIN-Code, Sicherheitsfrage, Prüfpfad);
- Kontaktinformationen (z. B. Adressen, E-Mail, Telefonnummern, Identifikatoren für soziale Medien; Kontaktangaben für Notfälle);
- Eindeutige Identifikationsnummern und Unterschriften (z. B. Sozialversicherungsnummer, Bankkontonummer, Reisepass- und Personalausweisnummer, Führerscheinnummer und Kfz-Zulassungsdaten, IP-Adressen, Mitarbeiternummer, Studentennummer, Patientennummer, Unterschrift, eindeutige Kennung in Tracking-Cookies oder ähnlichen Technologien);
- Pseudonyme Identifikatoren;
- Finanz- und Versicherungsdaten (z. B. Versicherungsnummer, Name und Nummer des Bankkontos, Name und Nummer der Kreditkarte, Rechnungsnummer, Einkommen, Art der Versicherung, Zahlungsverhalten, Kreditwürdigkeit);
- Kommerzielle Informationen (z. B. Kaufhistorie, Sonderangebote, Abonnement Informationen, Zahlungsverhalten);
- Biometrische Daten (z. B. DNA, Fingerabdrücke und Iris-Scans);
- Standortdaten (z. B. Zell-ID, geografische Netzwerkdaten, Standort bei Gesprächsbeginn/-ende. Standortdaten aus der Nutzung von WLAN-Zugangspunkten);
- Fotos, Video und Audio;
- Personal- und Einstellungsdaten (z. B. Erklärung des Beschäftigungsstatus, Einstellungsinformationen (z. B. Lebenslauf, Beschäftigungshistorie, Details zur Ausbildung), Job- und Positionsdaten, einschließlich Arbeitsstunden, Bewertungen und Gehalt, Details zur Arbeitserlaubnis, Verfügbarkeit, Beschäftigungsbedingungen, Steuerdetails, Zahlungsdetails, Versicherungsdetails sowie Standort und Organisationen);
- Bildungsdaten (z. B. Bildungsgeschichte, derzeitige Ausbildung, Noten und Ergebnisse, höchster erreichter Abschluss, Lernbehinderung);
- Staatsangehörigkeits- und Aufenthaltsdaten (z. B. Staatsangehörigkeit, Einbürgerungsstatus, Familienstand, Nationalität, Einwanderungsstatus, Reisepassdaten, Angaben zur Aufenthalts- oder Arbeitserlaubnis);
- Informationen, die zur Erfüllung einer Aufgabe verarbeitet werden, die im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erfolgt;
- Besondere Datenkategorien (z. B. rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten, Daten zum Sexualleben oder zur sexuellen Orientierung einer natürlichen Person oder Daten über strafrechtliche Verurteilungen oder Straftaten); oder
- alle anderen in Artikel 4 der DSGVO genannten personenbezogenen Daten.

Art und Zweck der Verarbeitung: Erbringung von Dienstleistungen durch die TolaData GmbH (Auftragsverarbeiter) für den Kunden (Verantwortlicher) im Rahmen ihres Hauptvertrags.

Dauer der Verarbeitung: Die Dauer der Verarbeitung entspricht der Dauer des Hauptvertrags.

2. Liste der Unterauftragsverarbeiter für TolaData.io

Der für die Verarbeitung Verantwortliche hat die Verwendung des/der folgenden Unterauftragsverarbeiter(s) genehmigt:

Noris network: Thomas-Mann-Straße 16-20, 90471 Nuremberg, Germany;

Website: https://www.noris.de/

Art und Zweck der Verarbeitung: Hosting-Provider der TolaData GmbH.

TolaData

ANNEX III

Technische und Organisatorische Maßnahmen (TOMs)

Verbundene Richtlinien und Vertragsbedingungen	TolaData Datenschutzrichtlinie TolaData Geschäftsbedingungen TolaData IT-Richtlinie für Mitarbeiter
Relevanter Rechtsrahmen	Europäische Datenschutz-Grundverordnung (EU-DSGVO)
Genehmigt durch	CEO, Jo Bennett
Letzte Überarbeitung	March 2021

Datenschutz, Datensicherheit und Zugangskontrolle

Zusammenfassung: Hosting, Backup und Verfügbarkeit

- Die TolaData GmbH ist ein 2018 gegründetes Unternehmen mit Sitz in Berlin. Die TolaData-Software sowie alle Benutzerdaten werden bei der Firma noris network AG („Hosting Provider“) in Deutschland gehostet und erfüllen alle EU-Vorschriften zur Datensicherheit. Dieses Hosting entspricht den Normen ISO 20000-1, ISO / IEC 27001 und ISO 9001.
- Die Anwendungsdaten werden parallel in zwei verschiedenen Rechenzentren in Deutschland gespeichert; dieses stellt sicher, dass alle Daten auch bei möglichen Vorfällen und Gefahren in einem der Rechenzentren jederzeit verfügbar sind.
- Darüber hinaus werden täglich automatisch historische Backups erstellt.
- Wir garantieren eine Verfügbarkeit unserer Plattform von 99%.

DSGVO und Daten Aufbewahrungsrichtlinie

- Der Kunde bleibt jederzeit Eigentümer und damit Verantwortlicher seiner Daten und die TolaData GmbH wird die Daten gemäß unseren Nutzungsbedingungen auf unserer Website verarbeiten (oder auf Wunsch des Kunden löschen) (https://www.toladata.com/terms-of-use/).
- Gemäß der DSGVO werden wir personenbezogene Daten löschen, die wir über Benutzer gespeichert haben (Namen, E-Mail-Adressen usw.), wenn der Kunde dies wünscht oder spätestens zwei Jahre nach Beendigung des Vertrages.
- Daten, die der Kunde in die TolaData-Software eingibt unterliegen der Verantwortung des Kunden. Der Kunde selbst haftet dafür, die betreffenden Gesetze und Datenrichtlinien für diese Daten innerhalb seiner Instanz einzuhalten.
- Weitere Informationen finden Sie in unseren Datenschutzbestimmungen auf unserer Website. (https://www.toladata.com/data-privacy-policy/)

1. Vertraulichkeit

Zutrittskontrolle	
Zutritts- kontrolle	Der Hosting-Anbieter verfügt über Server an sicheren Orten in Deutschland, deren Zutritt auf autorisiertes Personal beschränkt ist. Der physische Zugang wird gemäß ISO / IEC 27001 A.11 kontrolliert. Es wird kein öffentlicher Zutritt zu den Rechenzentren gewährt. Nur für die Systeme verantwortliche Parteien haben Zutritt. Schlüsselberechtigungen sind auf eine minimale Gruppe autorisierter Personen beschränkt. Alle relevanten Türen sind mit Zugangskontrollsystemen ausgestattet. Der Zugang zu den Rechenzentren über Zugangskarten wird protokolliert und vom Betriebsleiter des Rechenzentrums archiviert. Der reguläre Zugriff ist zeitlich auf die regulären Geschäftszeiten des Hosting-Anbieters beschränkt. Außerhalb der Geschäftszeiten ist ein Vier-Augen-Prinzip erforderlich, um die Rechenzentren zu betreten. TolaData kontrolliert den Zugang zu seinen Räumlichkeiten und Einrichtungen mit geeigneten Maßnahmen, diese sind: Zugang nur mit Schlüssel, Schlüsselverwaltung (kontrollierte Schlüsselausgabe), Besucher werden von autorisierten Mitarbeitern begleitet, Schränke und Büros sind verschlossen, wenn die Mitarbeiter nicht anwesend sind, das Reinigungspersonal wird sorgfältig ausgewählt.
Gefahren Erkennungs- Systeme	Die Rechenzentren sind mit einem Gefahrenerkennungssystem zur Brand- und Alarmerkennung ausgestattet. An das Überwachungssystem des Hosting-Anbieters und dessen 24-Stunden-Bereitschaftsdienst sind mehrere stille Alarmerkennungsleitungen sowie Rauchmelder angeschlossen. Das System leitet Brandalarme automatisch an die Brandmeldezentrale der jeweiligen Feuerwehr weiter.
Video Überwachung	Die Rechenzentren werden durch Videoüberwachung in den jeweiligen Sicherheitsbereichen für Doppeltüren und an allen relevanten Türen überwacht, die von einer Zone zur anderen führen.
Perimeter Schutz	Die Rechenzentren werden von Sicherheitspersonal überwacht.
Schlüssel Management	Die Zugriffsrechte der Mitarbeiter der Rechenzentren werden von der Personalabteilung des Hosting-Anbieters verwaltet.

	TolaData stellt Schlüssel nur seinen Mitarbeitern zur Verfügung, der Zugang zum Büro steht nur Schlüsselinhabern zur Verfügung.
Überwachung externer Parteien	Kein unbefugtes Personal hat Zugriff auf die Rechenzentren. Für den Fall, dass externe Dienstleister benötigt werden, gelten jedoch die entsprechenden Sicherheitsbestimmungen. Im TolaData-Büro werden Besucher von autorisierten Mitarbeitern begleitet.
Fenster und Türen	Die Rechenzentren sind fensterlos und Türen schließen automatisch. In TolaData-Büros werden Fenster und Türen verschlossen, wenn die Mitarbeiter die Büros verlassen.
Zugangskontrolle	
Daten- verarbeitung	Vor Beginn der Verarbeitungsaktivitäten wurden zwischen allen für die Verarbeitung Verantwortlichen und den Datenverarbeitern allgemeine Richtlinien und Verfahren für die Verarbeitung von Daten vereinbart.
Passwort Sicherheit	Die Richtlinie zu Kennwörtern und Berechtigungen im Rechenzentrum basiert auf den allgemeinen Bestimmungen zur Struktur von Kennwörtern gemäß bewährten Verfahren (z. B. Mindestlänge und Komplexitätsgrad). Darüber hinaus unterhält der Hosting-Anbieter eine Clean-Desk-Richtlinie, wenn es um Mitarbeiterpasswörter geht. Kennwörter von TolaData-Benutzern für den Zugriff auf die TolaData-Anwendung werden “hashed and salted”, nicht als einfacher Text gespeichert. Bei TolaData basiert die Richtlinie zu Kennwörtern und Berechtigungen auf den allgemeinen Bestimmungen zur Struktur von Kennwörtern gemäß bewährten Verfahren (z. B. Mindestlänge und Komplexitätsgrad). Darüber hinaus unterhält das Unternehmen eine Clean-Desk-Richtlinie, wenn es um

	Mitarbeiterpasswörter geht, und die Mitarbeiter müssen den Passwortmanager des Unternehmens verwenden.
Verschlüsse- lung	Die Datenübertragung zwischen Nutzer und TolaData-Anwendung wird mit SSL verschlüsselt. Das Engineering-Team von TolaData greift über eine verschlüsselte SSH-Verbindung (Secure Shell) auf die Datenbanken der Anwendung zu. Für die Produktionsdatenbank (d.h. die Datenbank, die von Nutzern eingegebene Daten enthält) werden die Zugriffsdaten nur für das autorisierte Personal freigegeben, für das dies erforderlich ist. Vom Hosting-Anbieter erstellte automatisierte Backups werden verschlüsselt. eMails werden von TolaData generell per TLS übertragen, sofern der eMail Anbieter des Empfänger eine TLS-Verschlüsselung unterstützt. Bei Bedarf können eMails auch per S/MIME Verfahren verschlüsselt und signiert werden. Die IT-Richtlinie der TolaData GmbH schreibt den Mitarbeitern verbindlich vor, sensible und Kundendaten - sofern eine Speicherung unumgänglich ist - auf Festplatten oder externen Datenträgern generell zu verschlüsseln.
Daten- verarbeitung durch Dritte	Die TolaData-Datenschutzrichtlinie enthält alle Parteien (Dritte), mit denen und zu welchem Zweck Kundendaten verarbeitet werden. Die Datenschutzrichtlinie ist auf der Website erhältlich.
Zugriffskontrolle	
Rollenbasierte Zugriffs- Steuerungen	Die TolaData-Software verfügt über rollenbasierte Zugriffssteuerungen, bei denen Nutzer unterschiedliche Rollen - basierend auf unterschiedlichen Funktionen - zugewiesen werden. Die Nutzer werden bei der Anmeldung anhand ihrer zugewiesenen Rollen authentifiziert. Für TolaData-Mitarbeiter werden jeder Rolle (die an der Verarbeitung personenbezogener Daten beteiligt ist) bestimmte Zugriffsrechte - nach dem “Need-to-know-Prinzip - zugeordnet. Eine entsprechende Richtlinie wurde mit den Mitarbeitern vereinbart und dokumentiert.

Nutzer Konten und Berechtigungen	In der TolaData-Software hat jeder Kunde einen oder mehrere designierte Org-Administratoren, die Einladungen für neue Nutzer und die Deaktivierung von alten Nutzern verwalten. Für das Unternehmen TolaData werden in allen benutzen Applikationen Zugangskontrollsysteme angewendet, die das Erstellen, Genehmigen, Überprüfen und Löschen von Benutzerkonten und Berechtigungen der Mitarbeiter ermöglichen. Die Verwendung von gemeinsamen Benutzerkonten wird vermieden.
Kontrolle des Zugriffs auf Daten / Aufzeichnungen	In der TolaData-Software gewähren Org-Admins den Benutzern Zugriffsrechte auf jedes Projekt und alle damit verbundenen Daten. Dieser Zugriff kann ein Bearbeitungszugriff oder nur eine Ansicht (view only) sein. Zusätzlich gibt es für jedes Projekt einen oder mehrere Projekt-Admins, die anderen Benutzern Zugriff auf dieses spezielle Projekt gewähren. Für TolaData-Mitarbeiter wurden spezifische Berechtigungen nach dem Need-to-know-Prinzip vergeben. Eine Berechtigungs-Kontroll-Richtlinie wurde vereinbart und dokumentiert.
Verwaltung privilegierter und sensitiver Konten	Org Admin-Konten werden auf Wunsch des Kunden vom TolaData Support Team erstellt und kontrolliert. Projekt-Admin-Konten werden von den/dem Org-Admin(s) verwaltet. Für das Unternehmen TolaData werden Konten der privilegierten Ebene durch einen zugewiesenen Org Admin und ein Passwort Verwaltungssystem gesichert, dass alle Konten in einem zentralisierten “Vault” in vollständig verschlüsselter Form verwaltet.
Protokollierung von Server-Zugriffen	Für die Software TolaData wird beim Zugriff auf den Server das Datenzugriffs-Protokoll (inklusive Zugriffsversuche) im Systemprotokoll geführt. Für Sitzungen gibt es ein vordefiniertes Timeout. Für TolaData-Mitarbeiter werden die Datenzugriffe in allen verwendeten Systemen protokolliert. Für alle Sitzungen müssen definierte Timeouts vorhanden sein.

Isolations-Kontrolle	
Daten-Speicherung & Entsorgung	Speicherung und Entsorgung werden konform mit DSGVO vorgenommen. Kundendaten werden für die Dauer der Nutzung der Software gespeichert und auf Wunsch des Kunden oder spätestens zwei Jahre nach der Deaktivierung des Kontos gelöscht.
Umgebungen	Es gibt eine Isolationskontrolle, bei der die verschiedenen Umgebungen (Produktion, Test, Entwicklung) beim Hosting-Provider getrennt sind. Nur autorisierte Mitarbeiter (wo dies erforderlich ist) haben Zugriff auf die Produktionsdatenbanken.
Pseudonymisierung	
Schutz von personenbezogenen Daten	Die TolaData-Anwendung erfordert außer bei der Registrierung und dem Login keine Eingabe von personenbezogenen Daten. Mit den Nutzungsbedingungen vereinbaren TolaData und der Kunde, dass der Kunde allein der Controller aller (personenbezogenen und sonstwie sensitiven) Daten ist, die der Kunde durch die Software verarbeitet. Auf die vom Kunden eingegebenen Daten können nur die von der Organisation des Kunden zugewiesenen Nutzer zugreifen, und die Berechtigungen für die Daten der einzelnen Projekte werden von den Administratoren des Kunden festgelegt und verwaltet. Das Eigentum und die rechtliche Verantwortung für solche Daten liegt immer beim Kunden. TolaData kontrolliert und haftet nicht für die Kunden vom Kunden gegebenenfalls eingegebenen oder hochgeladenen personenbezogenen oder sonstwie sensitiven Daten. Wir fördern jedoch Best Practices, raten zur Pseudonymisierung von personenbezogenen Daten und geben Empfehlungen in Bezug auf die Verwaltung personenbezogener Daten basierend auf den spezifischen Daten-, Tracking- und Berichtsanforderungen jedes Projekts.

2. Integrität

Steuerung der Datenübertragung	
Gemeinsame Nutzung und Übertragung von Daten	Die Datenübertragung erfolgt remote und es gibt ein Protokoll aller Personen, die von unserem Hosting-Provider darauf zugreifen. Darüber hinaus werden die Daten unterwegs verschlüsselt, um eine Verletzung während der gemeinsamen Nutzung/Übertragung zu vermeiden. Die Mitarbeiter von TolaData greifen ebenfalls remote auf Server und Datenbanken zu und sind verpflichtet, keine lokalen Kopien von Kundendaten anzufertigen oder Datenträger zu verwenden. Darüber hinaus sind die Mitarbeiter angehalten, nur vom Unternehmen offiziell freigegebene Hard- und Software zu verwenden, keine sensiblen Dokumente auszudrucken und keine Informationen an Externe weiterzugeben.
Dateneingabe Steuerung	
Logging	Im Rechenzentrum werden alle Maßnahmen getroffen, die sicherstellen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Daten in das Datenverarbeitungssystem eingegeben, geändert oder entfernt wurden (u.a. automatische Zugangsanmeldung, Passwort Politik, Auswertung von Logfiles auf bestimmte Ereignisse). Gleiches gilt für die TolaData-Software, die Ergänzungen, Bearbeitungen und Löschungen von Daten durch den Benutzer automatisch protokolliert. Gleiches gilt für die Mitarbeiter von TolaData: Zugriff auf Datenverarbeitungssysteme nur nach Anmeldung möglich, keine Weitergabe von Passwörtern, Passwort-Policy u.a. zum Vorgehen bei Bekanntwerden eines Passwortes sowie automatische Protokollierung bei Eingabe, Änderung und Löschung von Daten.

3. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle	
Datensicherung und	Unser Hosting-Betreiber betreibt unsere Datenbanken parallel in zwei verschiedenen Rechenzentren in Deutschland (Redundanzkonzept). Die von den Nutzern eingegebenen Daten werden also in zwei verschiedenen

Wiederherstellung	Rechenzentren gespeichert. Dementsprechend sind auch im Falle einer Gefährdung in einem Rechenzentrum die Daten nicht betroffen, sondern würden ohne Unterbrechung aus dem anderen Rechenzentrum weiter bereitgestellt werden. Als zusätzliche Sicherheitsmaßnahme führt unser Hosting-Provider täglich automatisierte Datenbank-Backups durch und legt diese verschlüsselt ab. Diese Backups ermöglichen es dem technischen Team, die Daten zu bestimmten Sicherungspunkten wiederherzustellen.
Unterbrechungsfreie Stromversorgung	Die Rechenzentren unseres Hosting-Providers folgen dem 24/7-Prinzip der Stromversorgung zum nachhaltigen Schutz vor Ausfällen. Redundante Klimakammern (abgesichert über USV und Dieselgeneratoren) sorgen dafür, dass auch bei Störungen keine Systemausfälle auftreten.
Reporting Verfahren	Unser Hosting-Provider unterhält geregelte Verfahren und Prozesse für Sicherheitspatches ("Patch-Days") und gemeldete Schwachstellen und veranlasst zusätzlich Eskalationen bei systemrelevanten Sicherheitsmeldungen des jeweiligen CERTs.
Management von Vorfällen der Daten-Verletzung	Der Hosting-Provider bietet eine Isolationskontrolle, unterschiedliche Umgebungen (Produktion, Test) werden auf separaten Instanzen mit Redundanz betrieben. Im Falle eines Vorfalls können die täglichen Backups innerhalb weniger Stunden wiederhergestellt werden, und das TolaData Team steht in Bereitschaft, um die Datenwiederherstellung zu unterstützen. Sowohl der Hosting-Provider als auch das Unternehmen TolaData haben Pläne zur Reaktion auf einen Vorfall mit detaillierten Verfahren definiert und dokumentiert, einschließlich einer Liste möglicher Abhilfemaßnahmen und einer klaren Zuweisung von Rollen. Jeder Vorfall und jede Datenverletzung müssen sofort an die Geschäftsleitung sowie die Datenschutzbeauftragte gemeldet werden. Die Datenschutz-beauftragte meldet den Vorfall innerhalb von 72 Stunden an die zuständige Aufsichtsbehörde; betroffene Kunden bzw. Personen werden umgehend durch TolaData informiert.

	Es gibt einen Notfall-Maßnahmenplan: Vorbereitung und Reaktions- maßnahmen sind dokumentiert, einschließlich einer Liste der notwendigen Schritte und einer klaren Zuweisung von Rollen im Fall einer Datenverletzung.
Anti-virus	Auf allen TolaData-Rechnern ist ein Antivirus-Programm installiert. Unser Hosting-Provider verwendet ebenfalls Antiviren-Software, um sicherzustellen, dass die TolaData-Anwendung dort, wo sie gehostet wird, nicht kompromittiert wird.
Malware	Die auf allen Rechnern installierte Antiviren-Software schützt vor Malware. Unser Hosting-Provider hat ebenfalls Malware-Software installiert, um sicherzustellen, dass die Software nicht mit Malware kompromittiert wird.
Anti-spyware	Die auf allen Rechnern installierte Antiviren-Software schützt vor Spyware. Unser Hosting-Provider verwendet auch Antiviren-Software, die über Anti-Spyware-Funktionen verfügt.
Intrusion detection	Die TolaData-Software wird überwacht und es werden sofort Berichte verschickt, wenn eine Verletzung oder ein Eindringen festgestellt wird. Unser Hosting-Provider hat ebenfalls Systeme zur Erkennung von Eindringlingen im Einsatz.
Firewalls	Es gibt Firewalls für das Netzwerk, das im Büro und beim Hosting der TolaData-Software verwendet wird.
Schwachstellen Scans	Es gibt automatische Antiviren-Scans auf allen Workstations.
Schnelle Recovery	
Geschäftskontinuität / Disaster recovery	Es gibt Standardverfahren für die Geschäftskontinuität. Dazu gehören: technisches Fachwissen, das jederzeit bereitsteht, um Probleme zu untersuchen und zu beheben, eine Notfallwiederherstellung auf der Datenbankebene der Anwendung und tägliche Backups. Unser Hosting-Provider verfügt über einen Disaster-Recovery-Plan, der im Falle eines Vorfalls aktiviert wird. Dieser beinhaltet Snapshots für VM-Produkte, Datenbank-Backups und Archiv-Logs.
System Monitoring	Die TolaData-Software wird überwacht und bei jeder Art von Verletzung werden sofort Alarme gesendet.
Testing	Der Wiederherstellungsprozess wurde zwischen unserem Hosting-Provider und dem technischen Team von TolaData getestet.

Wireless Networking	Es gibt einen drahtlosen Zugang in den TolaData-Büros mit SSIDs und Passwörtern, die regelmäßig geändert werden und den Standards entsprechen.
Wiederherstellbarkeit	In den Rechenzentren unseres Hosting Providers können alle Systeme über redundante Systeme - hochverfügbar und geo-redundant - wiederhergestellt werden. Ein umfassendes Monitoring (z.B. Incident Response Management nach ISO/IEC 27001 A.16) ermöglicht es, auf potentielle Ausfälle zu reagieren, bevor sie entstehen.

4. Verfahren zur regelmäßigen Prüfung, Beurteilung und Bewertung

Datenschutz-Management	
Datenschutz Beauftragte und Trainings	TolaData hat eine Datenschutzbeauftragte ernannet: Susanne Eggers, GFA Consulting Group GmbH, Eulenkrugstraße 82, 22359 Hamburg, Germany. email: susanne.eggers@gfa-group.de, telephone: +49 (40) 60306-105 TolaData stellt sicher, dass alle Mitarbeiter angemessen über alle Datenschutz- und IT-Sicherheitsrelevanten Aspekte informiert sind, die ihre tägliche Arbeit betreffen. Dies beinhaltet strukturierte und regelmäßige Schulungsprogramme für bestehende und neue Mitarbeiter. Alle Mitarbeiter von TolaData werden aufgefordert, die Sicherheitsrichtlinien sowie entsprechende Vertraulichkeits- und Geheimhaltungsvereinbarungen zu unterzeichnen.
Störfall Response Management	
Störfall Management	Im Falle eines Vorfalls können tägliche Backups innerhalb weniger Stunden wiederhergestellt werden. Ein Team steht bereit, um die Wiederherstellung der Daten zu unterstützen und sicherzustellen, dass die Dienste schnell wieder zur Verfügung stehen. Unser Hosting Provider führt das Incident Response Management nach ISO/IEC 27001 A.16 durch.
Datenschutz durch Design und Standards	
DGSVO Compliance	TolaData arbeitet vollständig DSGVO-konform und der Datenschutz steht bei der Entscheidungsfindung an vorderster Stelle. In diesem Sinne sind Datenschutz by Design und by Default in alle Strukturen des Unternehmens und die entwickelte Software integriert.
Auftrags oder Vertragssteuerung	

Auftrags-Kontrolle	TolaData ergreift alle notwendigen Maßnahmen, um sicherzustellen, dass Daten, die im Auftrag des Kunden verarbeitet werden, nur gemäß der Anweisung des Kunden verarbeitet werden. TolaData verarbeitet die Daten des Kunden nur für Zwecke im Rahmen der Geschäftsbeziehung, es werden alle notwendigen Verträge gemäß DSGVO abgeschlossen. Die Lieferanten werden sorgfältig ausgewählt und die Mitarbeiter der Lieferanten haben nur Zugang zu den Informationen, die sie für die Ausführung des Auftrags benötigen. Die Mitarbeiter der Lieferanten sind auf die Einhaltung der Datenschutzgrundsätze der DSGVO verpflichtet. Die Kontrolle der Vertragsdurchführung ist gewährleistet.
Datenverarbeitung durch Dritte	Für die TolaData-Software werden die Daten nur mit dem deutschen Hosting-Provider noris network AG geteilt. Für die Anmeldung in der Software über die Unternehmenswebsite sowie für die Kommunikation und den Support der Kunden werden die Daten mit einer Reihe von Dritt-Verarbeitern geteilt, die in unserer Datenschutzerklärung aufgelistet sind: (https://www.toladata.com/data-privacy-policy/) Jegliche Datenverarbeitung durch Dritte erfolgt in Übereinstimmung mit Art. 28 DSGVO, entsprechenden Normen der DSGVO und ggf. dem BDSG oder anderen relevanten Datenschutzgesetzen und -richtlinien.