

## **AUFTRAGSVERARBEITUNGSVEREINBARUNG**

## Inhalt

1.	Hintergrund und Zweck .....	3
2.	Definitionen.....	3
3.	Verarbeitung von personenbezogenen Daten.....	3
4.	Verzeichnis von Verarbeitungstätigkeiten .....	5
5.	Vertraulichkeit und Sicherheitsmaßnahmen.....	5
6.	Audit und Auskunftersuchen.....	6
7.	Unterauftragsverarbeiter.....	7
8.	Verletzung des Schutzes personenbezogener Daten.....	8
9.	Haftung .....	8
10.	Entschädigung.....	9
11.	Effektive Laufzeit .....	9
12.	Beendigung .....	9
13.	Änderungen .....	9
14.	Standardvertragsklauseln.....	10
15.	Anwendbare Bestimmungen und Rangfolge.....	10
16.	Geltendes Recht und Gerichtsbarkeit .....	10
	ANHANG 1: STANDARDVERTRAGSKLAUSELN.....	12
	ANLAGE zu den Standardvertragsklauseln .....	26

## **Auftragsverarbeitungsvereinbarung („AVV“)**

zwischen \_\_\_\_\_, im Folgenden als „**Verantwortlicher**“ bezeichnet, und **SMART Technologies ULC**, im Folgenden als „**Auftragsverarbeiter**“ bezeichnet.

### **1. Hintergrund und Zweck**

- 1.1. Gemäß 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 („**DSGVO**“) ist eine schriftliche Vereinbarung zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter erforderlich, die die Verarbeitung personenbezogener Daten regelt, die der Auftragsverarbeiter im Auftrag des für die Verarbeitung Verantwortlichen vornimmt.
- 1.2. Diese AVV zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter („**Parteien**“) regelt die anfänglichen Verpflichtungen, die der Auftragsverarbeiter bei der Verarbeitung personenbezogener Daten im Auftrag des für die Verarbeitung Verantwortlichen hat. Mit dieser Vereinbarung soll sichergestellt werden, dass der Auftragsverarbeiter personenbezogene Daten im Einklang mit den Weisungen des für die Verarbeitung Verantwortlichen und dem geltenden Recht verarbeitet, wozu auch das geltende Recht innerhalb der EU / des EWR, verschiedene Verordnungen und Beschlüsse von Behörden sowie Empfehlungen des Europäischen Datenschutzausschusses gehören, die bei der Verarbeitung personenbezogener Daten im Geltungsbereich der DSGVO Anwendung finden.
- 1.3. Der für die Verarbeitung Verantwortliche sollte dem Auftragsverarbeiter keine Schülerdaten zur Verfügung stellen.

### **2. Definitionen**

- 2.1. Die Definitionen in dieser AVV haben die entsprechenden Definitionen, wie sie in der Datenschutz-Grundverordnung (DSGVO) festgelegt sind und hier aufgeführt werden.

### **3. Verarbeitung von personenbezogenen Daten**

- 3.1. Die Parteien haben diese AVV abgeschlossen, um die Bedingungen für die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß den jeweiligen Allgemeinen Geschäftsbedingungen und Datenschutzhinweisen des Auftragsverarbeiters („**AV-Bedingungen**“) zu regeln, die der Auftragsverarbeiter im Auftrag des für die Verarbeitung Verantwortlichen einzuhalten hat.
- 3.2. Der Auftragsverarbeiter und die Personen, die im Auftrag des Auftragsverarbeiters handeln, dürfen personenbezogene Daten nur in Übereinstimmung mit der AVV und allen zusätzlichen schriftlichen Anweisungen, die der für die Verarbeitung Verantwortliche von Zeit zu Zeit erteilt, verarbeiten.
- 3.3. Der Auftragsverarbeiter darf personenbezogene Daten nur verarbeiten, um seinen Verpflichtungen gemäß den AV-Bedingungen nachzukommen. Hat der Auftragsverarbeiter

keine Anweisungen erhalten oder ist er sich über den Zweck der Verarbeitung, die zur Erfüllung einer bestimmten Aufgabe, die eine Verarbeitung personenbezogener Daten bedeutet oder bedeuten könnte, erforderlich ist, nicht im Klaren, so unterrichtet er den für die Verarbeitung Verantwortlichen unverzüglich über die Angelegenheit und wartet, bis der für die Verarbeitung Verantwortliche weitere Anweisungen erteilt.

- 3.4. Der Auftragsverarbeiter muss jederzeit seinen Verpflichtungen nach geltendem Recht nachkommen und sich über diese Verpflichtungen in Bezug auf die Verarbeitung personenbezogener Daten gemäß der AVV auf dem Laufenden halten. Der Auftragsverarbeiter muss auch jederzeit die Verhaltenskodizes oder Zertifizierungen einhalten, zu deren Einhaltung er sich verpflichtet hat. Der Auftragsverarbeiter benennt zumindest im Rahmen dieser AVV eine geeignete Kontaktperson für spezifische Datenschutzfragen.
- 3.5. Der Auftragsverarbeiter verpflichtet sich, das geltende Recht zu befolgen, das in allen Fällen in Bezug auf die Art der Dienstleistungen des Auftragsverarbeiters auszulegen ist und in der Regel bedeutet, dass der Auftragsverarbeiter nicht nach eigenem Ermessen personenbezogene Daten erheben oder personenbezogene Daten für andere Zwecke verwenden darf als für die Erfüllung der vereinbarten Lieferung gemäß dem Hauptwiederverkäufervertrag. Der Auftragsverarbeiter darf in keinem Fall ohne Anordnung einer zuständigen Behörde oder mangels zwingenden Rechts:
- a) personenbezogene Daten von oder an Dritte erheben oder weitergeben, sofern die Parteien nicht schriftlich etwas anderes vereinbart haben,
  - b) die Methode zur Verarbeitung personenbezogener Daten ändern, die das Risiko für die Grundfreiheiten und -rechte der betroffenen Personen erhöhen würde,
  - c) personenbezogene Daten zur alleinigen Verwendung durch den Auftragsverarbeiter kopieren oder neu erstellen oder
  - d) in irgendeiner anderen Weise personenbezogene Daten zu anderen Zwecken als den in den Haupt-AV-Bedingungen und den dazugehörigen Anhängen genannten verarbeiten.
- 3.6. Der Auftragsverarbeiter muss alle angemessenen Maßnahmen ergreifen, die gemäß Artikel 32 DSGVO erforderlich sind. Die zusätzlichen Maßnahmen, die berücksichtigt werden sollten, sind in den beigefügten Anweisungen des für die Verarbeitung Verantwortlichen aufgeführt.
- 3.7. Der Auftragsverarbeiter unterstützt den für die Verarbeitung Verantwortlichen, indem er im Rahmen des Möglichen geeignete technische und organisatorische Sicherheitsmaßnahmen ergreift, die es dem für die Verarbeitung Verantwortlichen ermöglichen, seinen Pflichten als für die Verarbeitung Verantwortlicher und seinen Pflichten im Zusammenhang mit Anträgen auf Ausübung der Rechte der betroffenen Personen gemäß Kapitel III der DSGVO nachzukommen.
- 3.8. Der Auftragsverarbeiter unterstützt den für die Verarbeitung Verantwortlichen dabei, sicherzustellen, dass die in den Artikeln 33-36 DSGVO genannten Verpflichtungen erfüllt werden können, wobei die Art der Verarbeitung und die Informationen, zu denen der Auftragsverarbeiter Zugang hat, berücksichtigt werden.

#### **4. Verzeichnis von Verarbeitungstätigkeiten**

- 4.1. Der Auftragsverarbeiter oder sein Vertreter führt ein Verzeichnis über alle Kategorien von Verarbeitungstätigkeiten, die im Auftrag des für die Verarbeitung Verantwortlichen durchgeführt werden. Das Verzeichnis muss mindestens die folgenden Informationen enthalten:
- a) Name und Kontaktdaten des Auftragsverarbeiters oder jedes beauftragten Unterauftragsverarbeiters, des für die Verarbeitung Verantwortlichen sowie des Vertreters des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters und des Datenschutzbeauftragten;
  - b) die Kategorien von Verarbeitungen, die im Auftrag des für die Verarbeitung Verantwortlichen durchgeführt werden;
  - c) die Kategorien von Empfängern, an die die personenbezogenen Daten weitergegeben wurden oder werden, einschließlich Empfängern in Drittländern oder gegebenenfalls internationalen Organisationen;
  - d) die Dokumentation geeigneter Maßnahmen, die ergriffen wurden, wenn personenbezogene Daten in ein Drittland übermittelt werden, das nicht in einem Beschluss enthalten ist, der anwendbare Bestimmungen über ein angemessenes Sicherheitsniveau oder geeignete Sicherheitsmaßnahmen enthält, und
  - e) gegebenenfalls eine allgemeine Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen, die der Auftragsverarbeiter nach geltendem Recht getroffen hat.
- 4.2. Der Auftragsverarbeiter stellt diese Aufzeichnungen dem für die Verarbeitung Verantwortlichen oder der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung, wobei er die oben genannten Angaben macht.
- 4.3. Verlangt eine betroffene Person in Ausübung ihrer Rechte ein Verzeichnis über die Verarbeitung ihrer personenbezogenen Daten, so stellt der Auftragsverarbeiter nach Rücksprache mit dem für die Verarbeitung Verantwortlichen auf Antrag der betroffenen Person oder des für die Verarbeitung Verantwortlichen ein solches Verzeichnis mit dem Inhalt und in einer Weise zur Verfügung, die mit dem geltenden Recht vereinbar ist.

#### **5. Vertraulichkeit und Sicherheitsmaßnahmen**

- 5.1. Der Auftragsverarbeiter setzt die erforderlichen technischen und organisatorischen Garantien im Einklang mit dem geltenden Recht um und trifft damit geeignete technische und organisatorische Maßnahmen, um personenbezogene Daten vor unbeabsichtigter oder unrechtmäßiger Zerstörung, Verlust oder Veränderung, vor unbefugter Weitergabe oder vor unbefugtem Zugriff auf personenbezogene Daten zu schützen, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet werden, insbesondere wenn die Verarbeitung eine Anpassung oder Datenübertragung

über Netze und/oder eine sonstige unrechtmäßige Verarbeitung beinhaltet. Bei der Bewertung des angemessenen Sicherheitsniveaus sind die Risiken zu berücksichtigen, die sich aus der Verarbeitung ergeben, insbesondere die unbeabsichtigte oder unrechtmäßige Zerstörung, der Verlust oder die Veränderung sowie die unberechtigte Weitergabe personenbezogener Daten.

- 5.2. Der Auftragsverarbeiter verpflichtet sich, die personenbezogenen Daten streng vertraulich zu behandeln und sie nicht an Dritte weiterzugeben oder ihnen zugänglich zu machen, wenn nicht zuvor eine Genehmigung erteilt wurde oder dies auf andere Weise nach geltendem Recht oder zur Durchführung dieser AVV erforderlich ist.
- 5.3. Der Auftragsverarbeiter verpflichtet sich, dafür zu sorgen, dass nur relevante Mitarbeiter Zugang zu den personenbezogenen Daten des für die Verarbeitung Verantwortlichen erhalten, um die Verpflichtungen des Auftragsverarbeiters gemäß dieser AVV zu erfüllen. Der Auftragsverarbeiter stellt sicher, dass die Mitarbeiter, die befugt sind, unter diese AVV fallende personenbezogene Daten zu verarbeiten, entweder per Gesetz oder durch eine Vereinbarung, die mindestens den in dieser AVV festgelegten Vertraulichkeitsbestimmungen entsprechen sollte, zur Vertraulichkeit verpflichtet werden. Der Auftragsverarbeiter stellt außerdem sicher, dass die Mitarbeiter die Bedeutung der in dieser Datenschutzvereinbarung festgelegten Vertraulichkeit verstehen. Die Vertraulichkeit, zu der sich die Parteien in der AVV verpflichten, gilt auch für einen Zeitraum nach Ablauf dieser AVV. Sie gilt jedoch nur für einen Zeitraum, der im geltenden Recht festgelegt ist.
- 5.4. Der Auftragsverarbeiter darf personenbezogene Daten nicht ohne (i) die vorherige schriftliche Zustimmung des für die Verarbeitung Verantwortlichen und (ii) nachdem er sich vergewissert hat, dass eine solche Übermittlung im Einklang mit dem geltenden Recht erfolgt, außerhalb der EU / des EWR oder in ein Land übermitteln, das nicht auf der Liste der Länder steht, die nach geltendem Recht von einer solchen Übermittlung ausgenommen sind. Dieses Verbot gilt auch für technische Unterstützung, Wartung und ähnliche Dienstleistungen.

## **6. Audit und Auskunftersuchen**

- 6.1. Der Auftragsverarbeiter unterrichtet den für die Verarbeitung Verantwortlichen unverzüglich über mögliche Kontakte mit der zuständigen Aufsichtsbehörde oder einer anderen Behörde im Zusammenhang mit der Verarbeitung personenbezogener Daten. Der Auftragsverarbeiter ist nicht berechtigt, den für die Verarbeitung Verantwortlichen zu vertreten oder in irgendeiner Weise im Namen des für die Verarbeitung Verantwortlichen gegenüber der zuständigen Aufsichtsbehörde oder einem Dritten zu handeln, es sei denn, der für die Verarbeitung Verantwortliche hat seine schriftliche Zustimmung erteilt.
- 6.2. Der Auftragsverarbeiter gewährt dem für die Verarbeitung Verantwortlichen oder einem von den Parteien ermächtigten Dritten Zugang zu allen nicht vertraulichen Informationen, die erforderlich und notwendig sind, damit der für die Verarbeitung Verantwortliche die Einhaltung der in dieser AVV, der DSGVO und anderen Vorschriften festgelegten Verpflichtungen durch den Auftragsverarbeiter überprüfen und kontrollieren kann. Der Auftragsverarbeiter muss auch Prüfungen, einschließlich Inspektionen, die von dem für die Verarbeitung Verantwortlichen oder von einem von dem für die Verarbeitung Verantwortlichen beauftragten Dritten durchgeführt werden, ermöglichen und dabei mitwirken.

- 6.3. Der Auftragsverarbeiter hat Anspruch auf Entschädigung durch den für die Verarbeitung Verantwortlichen, um die angemessenen direkten Kosten, die dem Auftragsverarbeiter durch eine solche Prüfung oder Inspektion entstanden sind, auszugleichen.
- 6.4. Der Auftragsverarbeiter gewährt dem für die Verarbeitung Verantwortlichen Zugang zu allen nicht vertraulichen Informationen, die erforderlich und notwendig sind, damit der für die Verarbeitung Verantwortliche überprüfen kann, ob die Verpflichtungen, die sich aus dieser AVV ergeben, eingehalten werden und ob die Verarbeitung den Anforderungen des geltenden Rechts entspricht.
- 6.5. In Fällen, in denen eine betroffene Person, eine zuständige Aufsichtsbehörde oder ein sonstiger Dritter eine der Vertragsparteien um Auskunft über personenbezogene Daten ersucht, arbeiten die Vertragsparteien zusammen und tauschen im erforderlichen Umfang Informationen aus.
- 6.6. Der Auftragsverarbeiter darf keine Informationen weitergeben, wenn er keine schriftliche Zustimmung des für die Verarbeitung Verantwortlichen dazu erhalten hat oder wenn eine solche Verpflichtung nicht nach geltendem Recht oder aufgrund einer Anordnung einer zuständigen Behörde besteht.

## **7. Unterauftragsverarbeiter**

- 7.1. Der Auftragsverarbeiter darf keine Unterauftragsverarbeiter mit der Verarbeitung personenbezogener Daten im Auftrag des für die Verarbeitung Verantwortlichen beauftragen, ohne den für die Verarbeitung Verantwortlichen dreißig (30) Tage vor einer solchen Beauftragung schriftlich darüber zu informieren, dass der Auftragsverarbeiter einen Unterauftragsverarbeiter beauftragen wird.
- 7.2. Für den Fall, dass der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Verarbeitung personenbezogener Daten beauftragt, erlegt er diesem dieselben Verpflichtungen und Auflagen auf, die sich aus dieser DSGVO ergeben. Der Auftragsverarbeiter verpflichtet sich außerdem, dafür zu sorgen, dass der Unterauftragsverarbeiter die Bestimmungen dieser AV-Bedingungen einhält und auch sonst das geltende Recht beachtet.
- 7.3. Beauftragt der Auftragsverarbeiter im Einklang mit dieser AVV einen Unterauftragsverarbeiter, so stellt er sicher, dass die Vereinbarung zwischen dem Auftragsverarbeiter und dem Unterauftragsverarbeiter so ausgelegt wird, dass auch der Unterauftragsverarbeiter an diese AVV sowie an die in dieser Vereinbarung festgelegten Anforderungen und das geltende Recht gebunden ist. Kommt der Unterauftragsverarbeiter seinen Verpflichtungen nicht nach, so haftet der Auftragsverarbeiter gegenüber dem für die Verarbeitung Verantwortlichen in vollem Umfang für die Erfüllung der Verpflichtungen dieses Unterauftragsverarbeiters. Der Auftragsverarbeiter führt von Zeit zu Zeit eine aktualisierte Liste der Unterauftragsverarbeiter, die beauftragt werden können. Auf Ersuchen des für die Verarbeitung Verantwortlichen legt der Auftragsverarbeiter dem für die Verarbeitung Verantwortlichen eine Kopie dieser Liste vor.
- 7.4. Der für die Verarbeitung Verantwortliche oder ein von ihm Beauftragter hat das Recht, vom Auftragsverarbeiter bei der Durchführung einer Inspektion oder Prüfung der Verarbeitung personenbezogener Daten durch den beauftragten Unterauftragsverarbeiter unterstützt zu werden.

## **8. Verletzung des Schutzes personenbezogener Daten**

- 8.1. Für den Fall, dass der Auftragsverarbeiter irgendeine Art von Sicherheitsverletzung vermutet oder feststellt, wie z. B. unbefugten Zugriff, Zerstörung, Veränderung personenbezogener Daten oder ähnliches, oder wenn der Auftragsverarbeiter aus irgendeinem Grund die Zusagen und Verpflichtungen in dieser AVV nicht einhalten kann, muss der Auftragsverarbeiter den Vorfall unverzüglich untersuchen und geeignete Maßnahmen ergreifen, um den Vorfall zu beheben und eine Wiederholung solcher Ereignisse zu verhindern.
- 8.2. Der Auftragsverarbeiter benachrichtigt den für die Verarbeitung Verantwortlichen unverzüglich, nachdem er von einer Verletzung des Schutzes personenbezogener Daten erfahren hat, und informiert den für die Verarbeitung Verantwortlichen fortlaufend über die Verletzung, sobald ihm Informationen über die Verletzung zugänglich werden.

Die Mitteilung muss mindestens folgende Angaben enthalten:

- a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, wenn möglich, die Kategorien und die ungefähre Zahl der betroffenen Personen sowie die Kategorien und die ungefähre Zahl der betroffenen personenbezogenen Datensätze;
  - b) Angabe des Namens und der Kontaktinformationen des Datenschutzbeauftragten oder anderer Kontaktstellen, bei denen weitere Informationen erhältlich sind,
  - c) eine Beschreibung der voraussichtlichen Folgen der Verletzung des Schutzes personenbezogener Daten und
  - d) eine Beschreibung der Maßnahmen, die der Auftragsverarbeiter ergriffen oder vorgeschlagen hat, um den Verstoß zu beheben, und die gegebenenfalls Maßnahmen zur Abschwächung der potenziellen negativen Auswirkungen umfassen.
- 8.3. Der Auftragsverarbeiter muss den für die Verarbeitung Verantwortlichen unverzüglich informieren, wenn;
- a) der Auftragsverarbeiter weiterhin Kenntnis von einer Verarbeitung personenbezogener Daten hat, die der Weisung des für die Verarbeitung Verantwortlichen oder dieser AVV widerspricht, und/oder
  - b) der Auftragsverarbeiter der Ansicht ist, dass eine Anweisung dem geltenden Recht widerspricht.
- 8.4. Wenn eine bestimmte Art der Verarbeitung, insbesondere im Hinblick auf die Verwendung neuer Technologien und unter Berücksichtigung von Art, Umfang, Kontext und Zweck, wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führen kann, muss der Auftragsverarbeiter den für die Verarbeitung Verantwortlichen vor der Durchführung der Verarbeitung bei der Bewertung der geplanten Auswirkungen der Verarbeitung auf den Schutz personenbezogener Daten unterstützen.

## **9. Haftung**



- 9.1. Artikel 82 DSGVO gilt für den Fall, dass einer betroffenen Person durch ein Gerichtsurteil oder eine andere Entscheidung aufgrund eines Verstoßes gegen eine Bestimmung dieser AVV, eine Anweisung des für die Verarbeitung Verantwortlichen oder der geltenden Datenschutzvorschriften Schadenersatz zugesprochen wird.
- 9.2. Wenn ein Bußgeld gemäß Artikel 83 DSGVO oder des anwendbaren nationalen Rechts verhängt wird, ist das Bußgeld von der Partei zu zahlen, die dieses Bußgeld erhält.
- 9.3. Erhält eine Vertragspartei Kenntnis von einem Umstand, der zu einem Schaden für die andere Vertragspartei führen kann, so informiert sie die andere Vertragspartei unverzüglich über diesen Umstand und arbeitet aktiv mit der anderen Vertragspartei zusammen, um einen solchen Schaden zu verhindern oder zu minimieren.
- 9.4. Ungeachtet der Angaben in den AV-Bedingungen der Parteien und den dazugehörigen Anhängen gelten die Abschnitte 9.1. und 9.2. der AVV vor allen anderen Bestimmungen über die Beendigung der zwischen den Parteien bestehenden Verpflichtungen in Bezug auf die Verarbeitung personenbezogener Daten.

## **10. Entschädigung**

- 10.1. Der Auftragsverarbeiter hat keinen Anspruch auf Entschädigung für Maßnahmen, die er im Zusammenhang mit der Verarbeitung personenbezogener Daten ergreift, es sei denn, in dieser AVV oder in der Wiederverkäufervereinbarung der Parteien ist etwas anderes festgelegt.

## **11. Effektive Laufzeit**

- 11.1. Diese AVV tritt am Tag ihrer Unterzeichnung in Kraft und gilt so lange, wie der Auftragsverarbeiter personenbezogene Daten im Rahmen der AV-Bedingungen der Parteien verarbeitet.

## **12. Beendigung**

- 12.1. Wenn der Auftragsverarbeiter die Verarbeitung personenbezogener Daten im Auftrag des für die Verarbeitung Verantwortlichen im Rahmen dieser AVV einstellt, muss er nach Wahl des für die Verarbeitung Verantwortlichen alle personenbezogenen Daten, die mit dieser Vereinbarung in Verbindung stehen, gemäß den Anweisungen des für die Verarbeitung Verantwortlichen vernichten, löschen und/oder an den für die Verarbeitung Verantwortlichen zurückgeben und sicherstellen, dass sich keine personenbezogenen Daten oder Kopien personenbezogener Daten mehr im Besitz des Auftragsverarbeiters befinden, es sei denn, dies ist aufgrund geltender Rechtsvorschriften oder aus finanziellen Gründen, einschließlich steuerlicher Gründe, erforderlich.
- 12.2. Der Auftragsverarbeiter stellt nach Beendigung dieser AVV sicher, dass die in Abschnitt 12.1 der AVV genannte Verpflichtung auch für alle Unterauftragsverarbeiter gilt.

## **13. Änderungen**

13.1. Der für die Verarbeitung Verantwortliche kann den Inhalt der AVV ändern, wenn dies zur Einhaltung des geltenden Rechts erforderlich ist. Eine Änderung kann dreißig (30) Tage, nachdem der für die Verarbeitung Verantwortliche dem Auftragsverarbeiter die Änderung mitgeteilt hat, in Kraft treten. Akzeptiert der Auftragsverarbeiter die betreffende Änderung nicht, hat der für die Verarbeitung Verantwortliche das Recht, alle Verträge mit dem Auftragsverarbeiter zu kündigen, in deren Rahmen der Auftragsverarbeiter personenbezogene Daten verarbeiten soll.

13.2. Änderungen dieser AVV bedürfen zu ihrer Rechtswirksamkeit der Schriftform und der Unterzeichnung durch beide Parteien.

#### **14. Standardvertragsklauseln**

14.1. Im Anwendungsbereich des Durchführungsbeschlusses (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates gelten die in Anhang 1 beigefügten Standardvertragsklauseln („SCC“).

#### **15. Anwendbare Bestimmungen und Rangfolge**

15.1. Die Vereinbarungen zwischen den Parteien gelten in der folgenden Reihenfolge, wobei im Falle von Widersprüchen die Bestimmungen der zuerst genannten Dokumente Vorrang vor den Bestimmungen der später genannten Dokumente haben:

- a) SCC, die dieser AVV unterliegen, in Anhang 1;
- b) die Bestimmungen dieser AVV und
- c) die Bestimmungen der AV-Bedingungen.

#### **16. Geltendes Recht und Gerichtsbarkeit**

16.1. Diese AVV unterliegt dem materiellen Recht von \_\_\_\_\_. Alle Streitigkeiten, Meinungsverschiedenheiten oder Ansprüche, die sich aus oder im Zusammenhang mit dieser AVV ergeben, werden vor den allgemeinen Gerichten von \_\_\_\_\_ endgültig entschieden, wobei das Amtsgericht von \_\_\_\_\_ die erste Instanz ist.

**Diese AVV kann in einer beliebigen Anzahl von Ausfertigungen, auch elektronisch, ausgefertigt werden.**

\_\_\_\_\_  
Datum

\_\_\_\_\_  
Datum

---

**Unterschrift des Verantwortlichen**

---

**Unterschrift des Auftragsverarbeiters**

---

Name und Titel in Druckbuchstaben

---

Name und Titel in in Druckbuchstaben

## ANHANG 1: STANDARDVERTRAGSKLAUSELN

### MODUL ZWEI: Übertragung von Verantwortlichen an Auftragsverarbeiter

#### ABSCHNITT I

##### 1. Klausel 1 - Zweck und Anwendungsbereich

- 1.1. Mit diesen Standardvertragsklauseln soll sichergestellt werden, dass die Anforderungen 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)<sup>1</sup> bei der Übermittlung personenbezogener Daten an ein Drittland eingehalten werden.
- 1.2. Die Parteien:
  - 1.2.1. die in Anhang I.A aufgeführte(n) natürliche(n) oder juristische(n) Person(en), Behörde(n), Agentur(en) oder sonstige(n) Stelle(n) (im Folgenden „Einrichtung(en)“), die die personenbezogenen Daten übermittelt/n (im Folgenden jeweils „Datenexporteur“), und
  - 1.2.2. die in Anhang I.A aufgeführte(n) Einrichtung(en) in einem Drittland, die die personenbezogenen Daten direkt oder indirekt über eine andere Einrichtung, die ebenfalls Partei dieser Klauseln ist, erhält/erhalten (im Folgenden jeweils „Datenimporteur“),  
  
haben sich mit diesen Standardvertragsklauseln (nachstehend „Klauseln“ genannt) einverstanden erklärt.
- 1.3. Diese Klauseln gelten für die Übermittlung personenbezogener Daten, gemäß Anhang I.B.
- 1.4. Die Anlage zu diesen Klauseln mit den darin enthaltenen Anhängen ist Bestandteil dieser Klauseln.

##### 2. Klausel 2 - Wirkung und Unveränderlichkeit der Klauseln

- 2.1. Diese Klauseln enthalten geeignete Garantien, einschließlich durchsetzbarer Rechte betroffener Personen und wirksamer Rechtsbehelfe gemäß Artikel 46 Absatz 1 und Artikel 46 Absatz 2 Buchstabe c der Verordnung (EU) 2016/679 sowie — in Bezug auf Datenübermittlungen von Verantwortlichen an Auftragsverarbeiter und/oder von Auftragsverarbeitern an Auftragsverarbeiter — Standardvertragsklauseln gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679, sofern

---

<sup>1</sup> Handelt es sich bei dem Datenexporteur um einen Auftragsverarbeiter, der der Verordnung (EU) 2016/679 unterliegt und der im Auftrag eines Organs oder einer Einrichtung der Union als Verantwortlicher handelt, so gewährleistet der Rückgriff auf diese Klauseln bei der Beauftragung eines anderen Auftragsverarbeiters (Unterauftragsverarbeitung), der nicht unter die Verordnung (EU) 2016/679 fällt, ebenfalls die Einhaltung von Artikel 29 Absatz 4 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39), insofern als diese Klauseln und die gemäß Artikel 29 Absatz 3 der Verordnung (EU) 2018/1725 im Vertrag oder in einem anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegten Datenschutzpflichten angeglichen sind. Dies ist insbesondere dann der Fall, wenn sich der Verantwortliche und der Auftragsverarbeiter auf die im Beschluss 2021/915 enthaltenen Standardvertragsklauseln stützen.

diese nicht geändert werden, mit Ausnahme der Auswahl des entsprechenden Moduls oder der entsprechenden Module oder der Ergänzung oder Aktualisierung von Informationen in der Anlage. Dies hindert die Parteien nicht daran, die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und/oder weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu diesen Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

- 2.2. Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Datenexporteur gemäß der Verordnung (EU) 2016/679 unterliegt.

### **3. Klausel 3 - Drittbegünstigte**

- 3.1. Betroffene Personen können diese Klauseln als Drittbegünstigte gegenüber dem Datenexporteur und/oder dem Datenimporteur geltend machen und durchsetzen, mit folgenden Ausnahmen:
- 3.2. Klausel 1, Klausel 2, Klausel 3, Klausel 6, Klausel 7;
- 3.3. Klausel 8 – Klausel 8.1.2, 8.9.1, 8.9.3, 8.9.4 und 8.9.5;
- 3.4. Klausel 9 – Klausel 9.1, 9.3, 9.4 und 9.5;
- 3.5. Klausel 12 – Klausel 12.1, 12.4 und 12.6;
- 3.6. Klausel 13;
- 3.7. Klausel 15.1.3, 15.1.4 und 15.1.5;
- 3.8. Klausel 16.5;
- 3.9. Klausel 18.1 und 18.2.
- 3.10. Die Rechte betroffener Personen gemäß der Verordnung (EU) 2016/679 bleiben von Buchstabe a unberührt

### **4. Klausel 4 - Auslegung**

- 4.1. Werden in diesen Klauseln in der Verordnung (EU) 2016/679 definierte Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in dieser Verordnung.
- 4.2. Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 auszulegen.
- 4.3. Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die mit den in der Verordnung (EU) 2016/679 vorgesehenen Rechten und Pflichten im Widerspruch steht.

### **5. Klausel 5 - Vorrang**

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen von damit zusammenhängenden Vereinbarungen zwischen den Parteien, die zu dem Zeitpunkt bestehen, zu dem diese Klauseln vereinbart oder eingegangen werden, haben diese Klauseln Vorrang.

## 6. Klausel 6 - Beschreibung der Datenübermittlungen

Die Einzelheiten der Datenübermittlung(en), insbesondere die Kategorien der übermittelten personenbezogenen Daten und der/die Zweck(e), zu dem/denen sie übermittelt werden, sind in Anhang I.B aufgeführt.

## 7. Klausel 7 - Kopplungsklausel

7.1. *[Klausel nicht einbezogen]*

## ABSCHNITT II - PFLICHTEN DER PARTEIEN

## 8. Klausel 8 - Datenschutzgarantien

Der Datenexporteur versichert, sich im Rahmen des Zumutbaren davon überzeugt zu haben, dass der Datenimporteur — durch die Umsetzung geeigneter technischer und organisatorischer Maßnahmen — in der Lage ist, seinen Pflichten aus diesen Klauseln nachzukommen.

### 8.1. Weisungen

8.1.1. Der Datenimporteur verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Datenexporteurs. Der Datenexporteur kann solche Weisungen während der gesamten Vertragslaufzeit erteilen.

8.1.2. Der Datenimporteur unterrichtet den Datenexporteur unverzüglich, wenn er diese Weisungen nicht befolgen kann.

### 8.2. Zweckbindung

Der Datenimporteur verarbeitet die personenbezogenen Daten nur für den/die in Anhang I.B genannten spezifischen Zweck(e), sofern keine weiteren Weisungen des Datenexporteurs bestehen.

### 8.3. Transparenz

Auf Anfrage stellt der Datenexporteur der betroffenen Person eine Kopie dieser Klauseln, einschließlich der von den Parteien ausgefüllten Anlage, unentgeltlich zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich der in Anhang II beschriebenen Maßnahmen und personenbezogener Daten, notwendig ist, kann der Datenexporteur Teile des Textes der Anlage zu diesen Klauseln vor der Weitergabe einer Kopie unkenntlich machen; er legt jedoch eine aussagekräftige Zusammenfassung vor, wenn die betroffene Person andernfalls den Inhalt der Anlage nicht verstehen würde oder ihre Rechte nicht ausüben könnte. Auf Anfrage teilen die Parteien der betroffenen Person die Gründe für die Schwärzungen so weit wie möglich mit, ohne die geschwärzten Informationen offenzulegen. Diese Klausel gilt unbeschadet der Pflichten des Datenexporteurs gemäß den Artikeln 13 und 14 der Verordnung (EU) 2016/679.

#### 8.4. Richtigkeit

Stellt der Datenimporteur fest, dass die erhaltenen personenbezogenen Daten unrichtig oder veraltet sind, unterrichtet er unverzüglich den Datenexporteur. In diesem Fall arbeitet der Datenimporteur mit dem Datenexporteur zusammen, um die Daten zu löschen oder zu berichtigen.

#### 8.5. Dauer der Verarbeitung und Löschung oder Rückgabe der Daten

Die Daten werden vom Datenimporteur nur für die in Anhang I.B angegebene Dauer verarbeitet. Nach Wahl des Datenexporteurs löscht der Datenimporteur nach Beendigung der Erbringung der Datenverarbeitungsdienste alle im Auftrag des Datenexporteurs verarbeiteten personenbezogenen Daten und bescheinigt dem Datenexporteur, dass dies erfolgt ist, oder gibt dem Datenexporteur alle in seinem Auftrag verarbeiteten personenbezogenen Daten zurück und löscht bestehende Kopien. Bis zur Löschung oder Rückgabe der Daten stellt der Datenimporteur weiterhin die Einhaltung dieser Klauseln sicher. Falls für den Datenimporteur lokale Rechtsvorschriften gelten, die ihm die Rückgabe oder Löschung der personenbezogenen Daten untersagen, sichert der Datenimporteur zu, dass er die Einhaltung dieser Klauseln auch weiterhin gewährleistet und diese Daten nur in dem Umfang und so lange verarbeitet, wie dies gemäß den betreffenden lokalen Rechtsvorschriften erforderlich ist. Dies gilt unbeschadet von Klausel 14, insbesondere der Pflicht des Datenimporteurs gemäß Klausel 14.5, den Datenexporteur während der Vertragslaufzeit zu benachrichtigen, wenn er Grund zu der Annahme hat, dass für ihn Rechtsvorschriften oder Gepflogenheiten gelten oder gelten werden, die nicht mit den Anforderungen in Klausel 14.1 im Einklang stehen.

#### 8.6. Sicherheit der Verarbeitung

8.6.1. Der Datenimporteur und, während der Datenübermittlung, auch der Datenexporteur treffen geeignete technische und organisatorische Maßnahmen, um die Sicherheit der Daten zu gewährleisten, einschließlich des Schutzes 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 diesen 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 dem/den Zweck(en) der Verarbeitung sowie den mit der Verarbeitung verbundenen Risiken für die betroffenen Personen gebührend Rechnung. Die Parteien ziehen insbesondere eine Verschlüsselung oder Pseudonymisierung, auch während der Datenübermittlung, in Betracht, wenn dadurch der Verarbeitungszweck erfüllt werden kann. Im Falle einer Pseudonymisierung verbleiben die zusätzlichen Informationen, mit denen die personenbezogenen Daten einer speziellen betroffenen Person zugeordnet werden können, soweit möglich, unter der ausschließlichen Kontrolle des Datenexporteurs. Zur Erfüllung seiner Pflichten gemäß diesem Absatz setzt der Datenimporteur mindestens die in Anhang II aufgeführten technischen und organisatorischen Maßnahmen um. Der Datenimporteur führt regelmäßige Kontrollen durch, um sicherzustellen, dass diese Maßnahmen weiterhin ein angemessenes Schutzniveau bieten.

8.6.2. Der Datenimporteur gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Er gewährleistet, dass sich die zur Verarbeitung

der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

8.6.3. Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Datenimporteur gemäß diesen Klauseln ergreift der Datenimporteur geeignete Maßnahmen zur Behebung der Verletzung, darunter auch Maßnahmen zur Abmilderung ihrer nachteiligen Auswirkungen. Zudem meldet der Datenimporteur dem Datenexporteur die Verletzung unverzüglich, nachdem sie ihm bekannt wurde. Diese Meldung enthält die Kontaktdaten einer Anlaufstelle für weitere Informationen, eine Beschreibung der Art der Verletzung (soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen personenbezogenen Datensätze), die wahrscheinlichen Folgen der Verletzung und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung etwaiger nachteiliger Auswirkungen. Wenn und soweit nicht alle 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.

8.6.4. Unter Berücksichtigung der Art der Verarbeitung und der dem Datenimporteur zur Verfügung stehenden Informationen arbeitet der Datenimporteur mit dem Datenexporteur zusammen und unterstützt ihn dabei, seinen Pflichten gemäß der Verordnung (EU) 2016/679 nachzukommen, insbesondere die zuständige Aufsichtsbehörde und die betroffenen Personen zu benachrichtigen

## 8.7. Sensible Daten

Soweit die Übermittlung personenbezogener Daten umfasst, 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 Datenimporteur die in Anhang I.B beschriebenen speziellen Beschränkungen und/oder zusätzlichen Garantien an.

## 8.8. Weiterübermittlungen

Der Datenimporteur gibt die personenbezogenen Daten nur auf dokumentierte Weisung des Datenexporteurs an Dritte weiter. Die Daten dürfen zudem nur an Dritte weitergegeben werden, die (in demselben Land wie der Datenimporteur oder in einem anderen Drittland) außerhalb der Europäischen Union<sup>2</sup> ansässig sind (im Folgenden „Weiterübermittlung“), sofern der Dritte im Rahmen des betreffenden Moduls an diese Klauseln gebunden ist oder sich mit der Bindung daran einverstanden erklärt oder falls

---

<sup>2</sup> Das Abkommen über den Europäischen Wirtschaftsraum (EWR-Abkommen) regelt die Einbeziehung der drei EWR-Staaten Island, Liechtenstein und Norwegen in den Binnenmarkt der Europäischen Union. Das Datenschutzrecht der Union, darunter die Verordnung (EU) 2016/679, ist in das EWR-Abkommen einbezogen und wurde in Anhang XI aufgenommen. Daher gilt eine Weitergabe von Daten durch den Datenimporteur an einen im EWR ansässigen Dritten nicht als Weiterübermittlung im Sinne dieser Klauseln.



- 8.8.1. die Weiterübermittlung an ein Land erfolgt, für das ein Angemessenheitsbeschluss nach Artikel 45 der Verordnung (EU) 2016/679 gilt, der die Weiterübermittlung abdeckt,
- 8.8.2. der Dritte auf andere Weise geeignete Garantien gemäß Artikel 46 oder Artikel 47 der Verordnung (EU) 2016/679 im Hinblick auf die betreffende Verarbeitung gewährleistet,
- 8.8.3. die Weiterübermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit bestimmten Verwaltungs-, Gerichts- oder regulatorischen Verfahren erforderlich ist oder
- 8.8.4. die Weiterübermittlung erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.

Jede Weiterübermittlung erfolgt unter der Bedingung, dass der Datenimporteur alle anderen Garantien gemäß diesen Klauseln, insbesondere die Zweckbindung, einhält.

#### 8.9. Dokumentation und Einhaltung der Klauseln

- 8.9.1. Der Datenimporteur bearbeitet Anfragen des Datenexporteurs, die sich auf die Verarbeitung gemäß diesen Klauseln beziehen, umgehend und in angemessener Weise.
- 8.9.2. Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können. Insbesondere führt der Datenimporteur geeignete Aufzeichnungen über die im Auftrag des Datenexporteurs durchgeführten Verarbeitungstätigkeiten.
- 8.9.3. Der Datenimporteur stellt dem Datenexporteur alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der in diesen Klauseln festgelegten Pflichten nachzuweisen; auf Verlangen des Datenexporteurs ermöglicht er diesem, die unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung zu prüfen, und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Datenexporteur einschlägige Zertifizierungen des Datenimporteurs berücksichtigen.
- 8.9.4. Der Datenexporteur kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Datenimporteurs umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.
- 8.9.5. Die Parteien stellen der zuständigen Aufsichtsbehörde die unter Klausel 8.9.2 und 8.9.3 genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

### 9. Klausel 9 - Einsatz von Unterauftragsverarbeitern

- 9.1. ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG. Der Datenimporteur besitzt die allgemeine Genehmigung des Datenexporteurs für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Datenimporteur unterrichtet den Datenexporteur mindestens dreißig (30) Tage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt

dem Datenexporteur damit ausreichend Zeit ein, um vor der Beauftragung des/der Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Datenimporteur stellt dem Datenexporteur die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

- 9.2. Beauftragt der Datenimporteur einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Datenexporteurs), so muss diese Beauftragung im Wege eines schriftlichen Vertrags erfolgen, der im Wesentlichen dieselben Datenschutzpflichten vorsieht wie diejenigen, die den Datenimporteur gemäß diesen Klauseln binden, einschließlich im Hinblick auf Rechte als Drittbegünstigte für betroffene Personen.<sup>3</sup> Die Parteien erklären sich damit einverstanden, dass der Datenimporteur durch Einhaltung der vorliegenden Klausel seinen Pflichten gemäß Klausel 8.8 nachkommt. Der Datenimporteur stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Datenimporteur gemäß diesen Klauseln unterliegt.
- 9.3. Der Datenimporteur stellt dem Datenexporteur 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 Datenimporteur den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.
- 9.4. Der Datenimporteur haftet gegenüber dem Datenexporteur in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Datenimporteur geschlossenen Vertrag nachkommt. Der Datenimporteur benachrichtigt den Datenexporteur, wenn der Unterauftragsverarbeiter seinen Pflichten gemäß diesem Vertrag nicht nachkommt.
- 9.5. Der Datenimporteur vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Datenexporteur — sollte der Datenimporteur faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sein — das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

## **10. Klausel 10 - Rechte betroffener Personen**

- 10.1. Der Datenimporteur unterrichtet den Datenexporteur unverzüglich über jeden Antrag, den er von einer betroffenen Person erhalten hat. Er beantwortet diesen Antrag nicht selbst, es sei denn, er wurde vom Datenexporteur dazu ermächtigt.
- 10.2. Der Datenimporteur unterstützt den Datenexporteur bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte gemäß der Verordnung (EU) 2016/679 zu beantworten. Zu diesem Zweck legen die Parteien in Anhang II unter Berücksichtigung der Art der Verarbeitung die geeigneten technischen und organisatorischen Maßnahmen, durch die Unterstützung geleistet wird, sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

---

<sup>3</sup> Diese Anforderung ist gegebenenfalls vom Unterauftragsverarbeiter zu erfüllen, der diesen Klauseln gemäß Klausel 7 im Rahmen des betreffenden Moduls beiträgt.

- 10.3. Bei der Erfüllung seiner Pflichten gemäß den Klauseln 10.1 und 10.2 befolgt der Datenimporteur die Weisungen des Datenexporteurs.

## **11. Klausel 11 - Rechtsbehelf**

- 11.1. Der Datenimporteur informiert die betroffenen Personen in transparenter und leicht zugänglicher Form mittels individueller Benachrichtigung oder auf seiner Website über eine Anlaufstelle, die befugt ist, Beschwerden zu bearbeiten. Er bearbeitet umgehend alle Beschwerden, die er von einer betroffenen Person erhält.
- 11.2. Im Falle einer Streitigkeit zwischen einer betroffenen Person und einer der Parteien bezüglich der Einhaltung dieser Klauseln bemüht sich die betreffende Partei nach besten Kräften um eine zügige gütliche Beilegung. Die Parteien halten einander über derartige Streitigkeiten auf dem Laufenden und bemühen sich gegebenenfalls gemeinsam um deren Beilegung.
- 11.3. Macht die betroffene Person ein Recht als Drittbegünstigte gemäß Klausel 3 geltend, erkennt der Datenimporteur die Entscheidung der betroffenen Person an,
- 11.3.1. eine Beschwerde bei der Aufsichtsbehörde des Mitgliedstaats ihres gewöhnlichen Aufenthaltsorts oder ihres Arbeitsorts oder bei der zuständigen Aufsichtsbehörde gemäß Klausel 13 einzureichen,
- 11.3.2. den Streitfall an die zuständigen Gerichte im Sinne der Klausel 18 zu verweisen.
- 11.4. Die Parteien erkennen an, dass die betroffene Person von einer Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht gemäß Artikel 80 Absatz 1 der Verordnung (EU) 2016/679 vertreten werden kann.
- 11.5. Der Datenimporteur unterwirft sich einem nach geltendem Unionsrecht oder dem geltenden Recht eines Mitgliedstaats verbindlichen Beschluss.
- 11.6. Der Datenimporteur erklärt sich damit einverstanden, dass die Entscheidung der betroffenen Person nicht ihre materiellen Rechte oder Verfahrensrechte berührt, Rechtsbehelfe im Einklang mit geltenden Rechtsvorschriften einzulegen.

## **12. Klausel 12 - Haftung**

- 12.1. Jede Partei haftet gegenüber der/den anderen Partei(en) für Schäden, die sie der/den anderen Partei(en) durch einen Verstoß gegen diese Klauseln verursacht.
- 12.2. Der Datenimporteur haftet gegenüber der betroffenen Person, und die betroffene Person hat Anspruch auf Schadenersatz für jeden materiellen oder immateriellen Schaden, den der Datenimporteur oder sein Unterauftragsverarbeiter der betroffenen Person verursacht, indem er deren Rechte als Drittbegünstigte gemäß diesen Klauseln verletzt.
- 12.3. Ungeachtet von Klausel 12.2 haftet der Datenimporteur gegenüber der betroffenen Person, und die betroffene Person hat Anspruch auf Schadenersatz für jeden materiellen oder immateriellen Schaden, den der Datenexporteur oder der Datenimporteur (oder dessen Unterauftragsverarbeiter) der betroffenen Person verursacht, indem er deren Rechte als Drittbegünstigte gemäß diesen

Klauseln verletzt. Dies gilt unbeschadet der Haftung des Datenexporteurs und, sofern der Datenexporteur ein im Auftrag eines Verantwortlichen handelnder Auftragsverarbeiter ist, unbeschadet der Haftung des Verantwortlichen gemäß der Verordnung (EU) 2016/679 oder gegebenenfalls der Verordnung (EU) 2018/1725.

- 12.4. Die Parteien erklären sich damit einverstanden, dass der Datenexporteur, der nach Klausel 12.3 für durch den Datenimporteur (oder dessen Unterauftragsverarbeiter) verursachte Schäden haftet, berechtigt ist, vom Datenimporteur den Teil des Schadenersatzes zurückzufordern, der der Verantwortung des Datenimporteurs für den Schaden entspricht.
- 12.5. Ist mehr als eine Partei für Schäden verantwortlich, die der betroffenen Person infolge eines Verstoßes gegen diese Klauseln entstanden sind, so haften alle verantwortlichen Parteien gesamtschuldnerisch, und die betroffene Person ist berechtigt, gegen jede der Parteien gerichtlich vorzugehen.
- 12.6. Die Parteien erklären sich damit einverstanden, dass eine Partei, die nach Klausel 12.5 haftbar gemacht wird, berechtigt ist, von der/den anderen Partei(en) den Teil des Schadenersatzes zurückzufordern, der deren Verantwortung für den Schaden entspricht.
- 12.7. Der Datenimporteur kann sich nicht auf das Verhalten eines Unterauftragsverarbeiters berufen, um sich seiner eigenen Haftung entziehen.

### **13. Klausel 13 - Aufsicht**

- 13.1. Wenn der Datenexporteur in einem EU-Mitgliedsstaat niedergelassen ist: Die Aufsichtsbehörde, die dafür verantwortlich ist, sicherzustellen, dass der Datenexporteur bei Datenübermittlungen die Verordnung (EU) 2016/679 einhält, fungiert als zuständige Aufsichtsbehörde (entsprechend der Angabe in Anhang I.C).

Wenn der Datenexporteur nicht in einem EU-Mitgliedstaat niedergelassen ist, aber nach Artikel 3 Absatz 2 der Verordnung (EU) 2016/679 in den räumlichen Anwendungsbereich dieser Verordnung fällt und einen Vertreter gemäß Artikel 27 Absatz 1 der Verordnung (EU) 2016/679 benannt hat: Die Aufsichtsbehörde des Mitgliedstaats, in dem der Vertreter nach Artikel 27 Absatz 1 der Verordnung (EU) 2016/679 niedergelassen ist, fungiert als zuständige Aufsichtsbehörde (entsprechend der Angabe in Anhang I.C).

Wenn der Datenexporteur nicht in einem EU-Mitgliedstaat niedergelassen ist, aber nach Artikel 3 Absatz 2 der Verordnung (EU) 2016/679 in den räumlichen Anwendungsbereich dieser Verordnung fällt, ohne jedoch einen Vertreter gemäß Artikel 27 Absatz 2 der Verordnung (EU) 2016/679 benennen zu müssen: Die Aufsichtsbehörde eines der Mitgliedstaaten, in denen die betroffenen Personen niedergelassen sind, deren personenbezogene Daten gemäß diesen Klauseln im Zusammenhang mit den ihnen angebotenen Waren oder Dienstleistungen übermittelt werden oder deren Verhalten beobachtet wird, fungiert als zuständige Aufsichtsbehörde (entsprechend der Angabe in Anhang I.C).

- 13.2. Der Datenimporteur erklärt sich damit einverstanden, sich der Zuständigkeit der zuständigen Aufsichtsbehörde zu unterwerfen und bei allen Verfahren, mit denen die Einhaltung dieser Klauseln sichergestellt werden soll, mit ihr zusammenzuarbeiten. Insbesondere erklärt sich der Datenimporteur damit einverstanden, Anfragen zu beantworten, sich Prüfungen zu unterziehen und

den von der Aufsichtsbehörde getroffenen Maßnahmen, darunter auch Abhilfemaßnahmen und Ausgleichsmaßnahmen, nachzukommen. Er bestätigt der Aufsichtsbehörde in schriftlicher Form, dass die erforderlichen Maßnahmen ergriffen wurden.

### **ABSCHNITT III - LOKALE RECHTSVORSCHRIFTEN UND PFLICHTEN IM FALLE DES ZUGANGS VON BEHÖRDEN ZU DEN DATEN**

#### **14. Klausel 14 - Lokale Rechtsvorschriften und Gepflogenheiten, die sich auf die Einhaltung der Klauseln auswirken**

- 14.1. Die Parteien sichern zu, keinen Grund zu der Annahme zu haben, dass die für die Verarbeitung personenbezogener Daten durch den Datenimporteur geltenden Rechtsvorschriften und Gepflogenheiten im Bestimmungsdrittland, einschließlich Anforderungen zur Offenlegung personenbezogener Daten oder Maßnahmen, die öffentlichen Behörden den Zugang zu diesen Daten gestatten, den Datenimporteur an der Erfüllung seiner Pflichten gemäß diesen Klauseln hindern. Dies basiert auf dem Verständnis, dass Rechtsvorschriften und Gepflogenheiten, die den Wesensgehalt der Grundrechte und Grundfreiheiten achten und nicht über Maßnahmen hinausgehen, die in einer demokratischen Gesellschaft notwendig und verhältnismäßig sind, um eines der in Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 aufgeführten Ziele sicherzustellen, nicht im Widerspruch zu diesen Klauseln stehen.
- 14.2. Die Parteien erklären, dass sie hinsichtlich der Zusicherung in Buchstabe a insbesondere die folgenden Aspekte gebührend berücksichtigt haben:
  - 14.2.1. die besonderen Umstände der Übermittlung, einschließlich der Länge der Verarbeitungskette, der Anzahl der beteiligten Akteure und der verwendeten Übertragungskanäle, beabsichtigte Datenweiterleitungen, die Art des Empfängers, den Zweck der Verarbeitung, die Kategorien und das Format der übermittelten personenbezogenen Daten, den Wirtschaftszweig, in dem die Übertragung erfolgt, den Speicherort der übermittelten Daten;
  - 14.2.2. die angesichts der besonderen Umstände der Übermittlung relevanten Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes (einschließlich solcher, die die Offenlegung von Daten gegenüber Behörden vorschreiben oder den Zugang von Behörden zu diesen Daten gestatten) sowie die geltenden Beschränkungen und Garantien<sup>4</sup>;
  - 14.2.3. alle relevanten vertraglichen, technischen oder organisatorischen Garantien, die zur Ergänzung der Garantien gemäß diesen Klauseln eingerichtet wurden, einschließlich Maßnahmen, die während der Übermittlung und bei der Verarbeitung personenbezogener Daten im Bestimmungsland angewandt werden.

---

<sup>4</sup> Zur Ermittlung der Auswirkungen derartiger Rechtsvorschriften und Gepflogenheiten auf die Einhaltung dieser Klauseln können in die Gesamtbeurteilung verschiedene Elemente einfließen. Diese Elemente können einschlägige und dokumentierte praktische Erfahrungen im Hinblick darauf umfassen, ob es bereits früher Ersuchen um Offenlegung seitens Behörden gab, die einen hinreichend repräsentativen Zeitrahmen abdecken, oder ob es solche Ersuchen nicht gab. Dies betrifft insbesondere interne Aufzeichnungen oder sonstige Belege, die fortlaufend mit gebührender Sorgfalt erstellt und von leitender Ebene bestätigt wurden, sofern diese Informationen rechtmäßig an Dritte weitergegeben werden können. Sofern anhand dieser praktischen Erfahrungen der Schluss gezogen wird, dass dem Datenimporteur die Einhaltung dieser Klauseln nicht unmöglich ist, muss dies durch weitere relevante objektive Elemente untermauert werden; den Parteien obliegt die sorgfältige Prüfung, ob alle diese Elemente ausreichend zuverlässig und repräsentativ sind, um die getroffene Schlussfolgerung zu bekräftigen. Insbesondere müssen die Parteien berücksichtigen, ob ihre praktische Erfahrung durch öffentlich verfügbare oder anderweitig zugängliche zuverlässige Informationen über das Vorhandensein oder Nicht-Vorhandensein von Ersuchen innerhalb desselben Wirtschaftszweigs und/oder über die Anwendung der Rechtsvorschriften in der Praxis, wie Rechtsprechung und Berichte unabhängiger Aufsichtsgremien, erhärtet und nicht widerlegt wird.

- 14.3. Der Datenimporteur versichert, dass er sich im Rahmen der Beurteilung nach Klausel 14.2 nach besten Kräften bemüht hat, dem Datenexporteur sachdienliche Informationen zur Verfügung zu stellen, und erklärt sich damit einverstanden, dass er mit dem Datenexporteur weiterhin zusammenarbeiten wird, um die Einhaltung dieser Klauseln zu gewährleisten.
- 14.4. Die Parteien erklären sich damit einverstanden, die Beurteilung nach Klausel 14.2 zu dokumentieren und sie der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.
- 14.5. Der Datenimporteur erklärt sich damit einverstanden, während der Laufzeit des Vertrags den Datenexporteur unverzüglich zu benachrichtigen, wenn er nach Zustimmung zu diesen Klauseln Grund zu der Annahme hat, dass für ihn Rechtsvorschriften oder Gepflogenheiten gelten, die nicht mit den Anforderungen in Klausel 14.1 im Einklang stehen; hierunter fällt auch eine Änderung der Rechtsvorschriften des Drittlandes oder eine Maßnahme (z. B. ein Offenlegungsersuchen), die sich auf eine nicht mit den Anforderungen in Klausel 14.1 im Einklang stehende Anwendung dieser Rechtsvorschriften in der Praxis bezieht.
- 14.6. Nach einer Benachrichtigung gemäß Klausel 14.5 oder wenn der Datenexporteur anderweitig Grund zu der Annahme hat, dass der Datenimporteur seinen Pflichten gemäß diesen Klauseln nicht mehr nachkommen kann, ermittelt der Datenexporteur unverzüglich geeignete Maßnahmen (z. B. technische oder organisatorische Maßnahmen zur Gewährleistung der Sicherheit und Vertraulichkeit), die der Datenexporteur und/oder der Datenimporteur ergreifen müssen, um Abhilfe zu schaffen. Der Datenexporteur setzt die Datenübermittlung aus, wenn er der Auffassung ist, dass keine geeigneten Garantien für eine derartige Übermittlung gewährleistet werden können, oder wenn er von der dafür zuständigen Aufsichtsbehörde dazu angewiesen wird. In diesem Fall ist der Datenexporteur berechtigt, den Vertrag zu kündigen, soweit es um die Verarbeitung personenbezogener Daten gemäß diesen Klauseln geht. Sind mehr als zwei Parteien an dem Vertrag beteiligt, so kann der Datenexporteur von diesem Kündigungsrecht nur gegenüber der verantwortlichen Partei Gebrauch machen, sofern die Parteien nichts anderes vereinbart haben. Wird der Vertrag gemäß dieser Klausel gekündigt, finden Klausel 16.4 und 16.5 Anwendung.

## **15. Klausel 15 - Pflichten des Datenimporteurs im Falle des Zugangs von Behörden zu den Daten**

### **15.1. Benachrichtigung**

- 15.1.1. Der Datenimporteur erklärt sich damit einverstanden, den Datenexporteur und, soweit möglich, die betroffene Person (gegebenenfalls mit Unterstützung des Datenexporteurs) unverzüglich zu benachrichtigen
  - 15.1.1.1. wenn er von einer Behörde, einschließlich Justizbehörden, ein nach den Rechtsvorschriften des Bestimmungslandes rechtlich bindendes Ersuchen um Offenlegung personenbezogener Daten erhält, die gemäß diesen Klauseln übermittelt werden (diese Benachrichtigung muss Informationen über die angeforderten personenbezogenen Daten, die ersuchende Behörde, die Rechtsgrundlage des Ersuchens und die mitgeteilte Antwort enthalten), oder
  - 15.1.1.3. wenn er Kenntnis davon erlangt, dass eine Behörde nach den Rechtsvorschriften des Bestimmungslandes direkten Zugang zu personenbezogenen Daten hat, die

gemäß diesen Klauseln übermittelt wurden; diese Benachrichtigung muss alle dem Datenimporteur verfügbaren Informationen enthalten.

- 15.1.2. Ist es dem Datenimporteur gemäß den Rechtsvorschriften des Bestimmungslandes untersagt, den Datenexporteur und/oder die betroffene Person zu benachrichtigen, so erklärt sich der Datenimporteur einverstanden, sich nach besten Kräften um eine Aufhebung des Verbots zu bemühen, damit möglichst viele Informationen so schnell wie möglich mitgeteilt werden können. Der Datenimporteur verpflichtet sich, seine Anstrengungen zu dokumentieren, um diese auf Verlangen des Datenexporteurs nachweisen zu können.
- 15.1.3. Soweit dies nach den Rechtsvorschriften des Bestimmungslandes zulässig ist, erklärt sich der Datenimporteur bereit, dem Datenexporteur während der Vertragslaufzeit in regelmäßigen Abständen möglichst viele sachdienliche Informationen über die eingegangenen Ersuchen zur Verfügung zu stellen (insbesondere Anzahl der Ersuchen, Art der angeforderten Daten, ersuchende Behörde(n), ob Ersuchen angefochten wurden und das Ergebnis solcher Anfechtungen usw.).
- 15.1.4. Der Datenimporteur erklärt sich damit einverstanden, die Informationen gemäß den Klauseln 15.1.1 bis 15.1.3 während der Vertragslaufzeit aufzubewahren und der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.
- 15.1.5. Die Klauseln 15.1.1. bis 15.1.3 gelten unbeschadet der Pflicht des Datenimporteurs gemäß Klausel 14.5 und Klausel 16, den Datenexporteur unverzüglich zu informieren, wenn er diese Klauseln nicht einhalten kann.
- 15.2. Überprüfung der Rechtmäßigkeit und Datenminimierung
- 15.2.1. Der Datenimporteur erklärt sich damit einverstanden, die Rechtmäßigkeit des Offenlegungsersuchens zu überprüfen, insbesondere ob das Ersuchen im Rahmen der Befugnisse liegt, die der ersuchenden Behörde übertragen wurden, und das Ersuchen anzufechten, wenn er nach sorgfältiger Beurteilung zu dem Schluss kommt, dass hinreichende Gründe zu der Annahme bestehen, dass das Ersuchen nach den Rechtsvorschriften des Bestimmungslandes, gemäß geltenden völkerrechtlichen Verpflichtungen und nach den Grundsätzen der Völkercourtoisie rechtswidrig ist. Unter den genannten Bedingungen sind vom Datenimporteur mögliche Rechtsmittel einzulegen. Bei der Anfechtung eines Ersuchens erwirkt der Datenimporteur einstweilige Maßnahmen, um die Wirkung des Ersuchens auszusetzen, bis die zuständige Justizbehörde über dessen Begründetheit entschieden hat. Er legt die angeforderten personenbezogenen Daten erst offen, wenn dies nach den geltenden Verfahrensregeln erforderlich ist. Diese Anforderungen gelten unbeschadet der Pflichten des Datenimporteurs gemäß Klausel 14.5.
- 15.2.2. Der Datenimporteur erklärt sich damit einverstanden, seine rechtliche Beurteilung und eine etwaige Anfechtung des Offenlegungsersuchens zu dokumentieren und diese Unterlagen dem Datenexporteur zur Verfügung zu stellen, soweit dies nach den Rechtsvorschriften des Bestimmungslandes zulässig ist. Auf Anfrage stellt er diese Unterlagen auch der zuständigen Aufsichtsbehörde zur Verfügung.

- 15.2.3. Der Datenimporteur erklärt sich damit einverstanden, bei der Beantwortung eines Offenlegungsersuchens auf der Grundlage einer vernünftigen Auslegung des Ersuchens die zulässige Mindestmenge an Informationen bereitzustellen.

#### **ABSCHNITT IV - SCHLUSSBESTIMMUNGEN**

##### **16. Klausel 16 - Verstöße gegen die Klauseln und Beendigung des Vertrags**

- 16.1. Der Datenimporteur unterrichtet den Datenexporteur unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.
- 16.2. Verstößt der Datenimporteur gegen diese Klauseln oder kann er diese Klauseln nicht einhalten, setzt der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur aus, bis der Verstoß beseitigt oder der Vertrag beendet ist. Dies gilt unbeschadet von Klausel 14.6.
- 16.3. Der Datenexporteur ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn
- 16.3.1. der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur gemäß Klausel 16.2 ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb einer einmonatigen Aussetzung, wiederhergestellt wurde,
- 16.3.2. der Datenimporteur in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder
- 16.3.3. der Datenimporteur einer verbindlichen Entscheidung eines zuständigen Gerichts oder einer zuständigen Aufsichtsbehörde, die seine Pflichten gemäß diesen Klauseln zum Gegenstand hat, nicht nachkommt.

In diesen Fällen unterrichtet der Datenexporteur die zuständige Aufsichtsbehörde über derartige Verstöße. Sind mehr als zwei Parteien an dem Vertrag beteiligt, so kann der Datenexporteur von diesem Kündigungsrecht nur gegenüber der verantwortlichen Partei Gebrauch machen, sofern die Parteien nichts anderes vereinbart haben.

- 16.4. Personenbezogene Daten, die vor Beendigung des Vertrags gemäß 16.3 übermittelt wurden, müssen nach Wahl des Datenexporteurs unverzüglich an diesen zurückgegeben oder vollständig gelöscht werden. Dies gilt gleichermaßen für alle Kopien der Daten. Der Datenimporteur bescheinigt dem Datenexporteur die Löschung. Bis zur Löschung oder Rückgabe der Daten stellt der Datenimporteur weiterhin die Einhaltung dieser Klauseln sicher. Falls für den Datenimporteur lokale Rechtsvorschriften gelten, die ihm die Rückgabe oder Löschung der übermittelten personenbezogenen Daten untersagen, sichert der Datenimporteur zu, dass er die Einhaltung dieser Klauseln auch weiterhin gewährleistet und diese Daten nur in dem Umfang und so lange verarbeitet, wie dies gemäß den betreffenden lokalen Rechtsvorschriften erforderlich ist.
- 16.5. Jede Partei kann ihre Zustimmung widerrufen, durch diese Klauseln gebunden zu sein, wenn i) die Europäische Kommission einen Beschluss nach Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 erlässt, der sich auf die Übermittlung personenbezogener Daten bezieht, für die diese Klauseln gelten, oder ii) die Verordnung (EU) 2016/679 Teil des Rechtsrahmens des Landes wird,



an das die personenbezogenen Daten übermittelt werden. Dies gilt unbeschadet anderer Verpflichtungen, die für die betreffende Verarbeitung gemäß der Verordnung (EU) 2016/679 gelten.

**17. Klausel 17 - Anwendbares Recht**

Diese Klauseln unterliegen dem Recht des EU-Mitgliedstaats, in dem der Datenexporteur niedergelassen ist. Wenn dieses Recht keine Rechte als Drittbegünstigte zulässt, unterliegen diese Klauseln dem Recht eines anderen EU-Mitgliedstaats, das Rechte als Drittbegünstigte zulässt. Die Parteien vereinbaren, dass dies das Recht von [REDACTED] ist.

**18. Klausel 18 - Gerichtsstand und Zuständigkeit**

- 18.1. Streitigkeiten, die sich aus diesen Klauseln ergeben, werden von den Gerichten eines EU-Mitgliedstaats beigelegt.
- 18.2. Die Parteien vereinbaren, dass dies die Gerichte von [REDACTED] sind.
- 18.3. Eine betroffene Person kann Klage gegen den Datenexporteur und/oder den Datenimporteur auch vor den Gerichten des Mitgliedstaats erheben, in dem sie ihren gewöhnlichen Aufenthaltsort hat.
- 18.4. Die Parteien erklären sich damit einverstanden, sich der Zuständigkeit dieser Gerichte zu unterwerfen



## **B. BESCHREIBUNG DER DATENÜBERMITTLUNG**

### **Kategorien betroffener Personen, deren personenbezogene Daten übermittelt werden**

- Endnutzer
- Kundenmitarbeiter

### **Kategorien der übermittelten personenbezogenen Daten**

#### **1. Der Endnutzer**

- Direkte identifizierende Informationen (z. B. Name, E-Mail-Adresse)
- Alle von den Endnutzern des Dienstes gelieferten personenbezogenen Daten
- Anwendungstechnik Metadaten
  - IP-Adressen, Verwendung von Cookies, usw.
- Statistik der Anwendungsnutzung
  - Metadaten zur Benutzerinteraktion mit der Anwendung
  - Andere Beurteilungsdaten - vom Lehrer, der die Klasse leitet, festgelegt
- Erfasste Online-Kommunikation (E-Mails, Blogeinträge)
- Provider/App zugewiesene Schülern-ID-Nummer
- Schülern-App Benutzername
- Antworten der Schüler auf Umfragen oder Fragebögen
- Von Schülern erstellte Inhalte: Texte, Bilder usw. - alles, was in der Unterrichtsdatei des Lehrers gespeichert ist
- Microsoft Single Sign-On
- Google Single Sign-On
- Region für die Datenspeicherung (USA oder EU)
- Google Analytics (anonym)
- MixPanel-Analytics (anonym)

#### **2. Der Kundenmitarbeiter**

- Name der Organisation
- E-Mail
- Telefon
- Adresse
- Erforderliche Bestellinformationen: Produkt, Menge, Preis und Steuer, Lieferung

**Übermittelte 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 Auftragsverarbeiter untersagt dem für die Verarbeitung Verantwortlichen hiermit ausdrücklich, ihm besondere Kategorien personenbezogener Daten zu übermitteln.

**Häufigkeit der Übermittlung (z. B. ob die Daten einmalig oder kontinuierlich übermittelt werden)**

Kontinuierlich während der Nutzung des Dienstes.

### **Art der Verarbeitung**

Der Auftragsverarbeiter wird die folgenden grundlegenden Verarbeitungstätigkeiten durchführen:

- Verarbeitung zur Erbringung des Dienstes in Übereinstimmung mit den AV-Bedingungen;
- die Verarbeitung zur Durchführung von Schritten, die für die Erbringung des Dienstes erforderlich sind; und
- die Verarbeitung zur Befolgung sonstiger angemessener Anweisungen des für die Verarbeitung Verantwortlichen (z. B. per E-Mail), die mit den Bedingungen der AV-Bedingungen übereinstimmen.

### **Zweck(e) der Datenübermittlung und Weiterverarbeitung**

Der Auftragsverarbeiter verarbeitet personenbezogene Daten, die an SMART Learning Suite übermittelt, dort gespeichert oder über SMART Learning Suite gesendet werden, um den Dienst und die damit verbundene technische Unterstützung in Übereinstimmung mit dieser AVV bereitzustellen.

**Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer**

Während der gesamten Laufzeit des Leistungsvertrags sowie für den Zeitraum nach Ablauf der Laufzeit bis zur Löschung der personenbezogenen Daten durch den Auftragsverarbeiter gemäß geltendem Recht oder auf Verlangen des für die Verarbeitung Verantwortlichen (Antrag auf Datenlöschung).

### **C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE**

Angabe der zuständigen Aufsichtsbehörde(n) gemäß Klausel 13

Verantwortlicher, bitte geben Sie hier die Aufsichtsbehörde Ihres Landes an:

---

*\*Hinweis: Wenn der für die Verarbeitung Verantwortliche als Datenexporteur fungiert und in einem EU-Mitgliedstaat ansässig ist, fungiert die Aufsichtsbehörde, die dafür zuständig ist, die Einhaltung der Verordnung (EU) 2016/679 durch den Datenexporteur in Bezug auf die Datenübermittlung zu gewährleisten, wie hier angegeben, als zuständige Aufsichtsbehörde.*

## ANHANG II - TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

### TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH TECHNISCHER UND ORGANISATORISCHER MASSNAHMEN ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

Beschreibung der von dem/den Datenimporteur(en) ergriffenen technischen und organisatorischen Maßnahmen (einschließlich aller relevanten Zertifizierungen) zur Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen

Die Vertragsparteien vereinbaren die Durchführung der folgenden Kategorien von Maßnahmen. Die Einzelheiten der einzelnen Maßnahmen sind auf Anfrage erhältlich.

1. Der Auftragsverarbeiter sollte über eine strukturierte Organisation verfügen, in der die Aufgaben und Zuständigkeiten der verschiedenen Mitarbeiter in Bezug auf Sicherheitsinformationen klar definiert sind.
2. Der Auftragsverarbeiter bietet regelmäßig Kurse an, um das Bewusstsein für widerstandsfähige Informationssysteme zu schärfen.
3. Der Auftragsverarbeiter sollte über Routinen und Funktionen verfügen, um Informationen, die einen Bezug zur Leistung haben, dauerhaft zu löschen und zu vernichten.
4. Der Auftragsverarbeiter hat eine Risikobewertung des Systems vorgenommen und Messungen durchgeführt, um etwaige Fehler in diesem System zu ermitteln.
5. Die Anforderungen des Verantwortlichen an die Verarbeitung von Informationen sind zu übernehmen. Werden solche Anforderungen nicht formuliert, muss der Auftragsverarbeiter in der Lage sein, die für ihn geltenden Routinen darzulegen.
6. Die Benutzer sind mit persönlichen und eindeutigen Benutzeridentitäten auszustatten, sodass anonyme Gastkonten nicht verwendet werden dürfen. Weitere Informationen finden Sie im Leitfaden für die Vertrauensstufe 1 (LoA1).
7. Der Auftragsverarbeiter muss eine vereinbarte Routine einhalten, die es dem Verantwortlichen ermöglicht, bestimmte Rechte zu genehmigen.
8. Der Auftragsverarbeiter verwendet persönliche und nachvollziehbare Benutzeridentitäten für Konten mit umfassenderen Rechten, die zur Verwaltung des Systems eingesetzt werden.
9. Der Auftragsverarbeiter muss über ein System verfügen, mit dem Passwörter verteilt und zurückgesetzt werden können, ohne dass das Passwort an Unbefugte weitergegeben wird. Weitere Informationen finden Sie im Leitfaden für die Vertrauensstufe 1 (LoA1).
10. Das Berechtigungssystem protokolliert Informationen darüber, wann ein Benutzer angelegt oder entfernt wird.
11. Der Auftragsverarbeiter muss über eine Routine zum Entfernen von Benutzeridentitäten aus dem System verfügen.
12. Der Auftragsverarbeiter muss Regeln für die für den Umgang mit Authentifizierungsinformationen verantwortliche Person festgelegt haben.

13. Nur Informationen oder Dienste, die öffentlich sind, dürfen in dem System und jeder anderen zugehörigen Infrastruktur, die keiner Authentifizierung unterzogen wurde, verfügbar sein.
14. Das System sollte zur Authentifizierung Passwörter oder etwas anderes verwenden, das eine höhere Sicherheitsstufe bietet. Es sollten Regeln dafür aufgestellt werden, wie ein Passwort im System und von einem Benutzer gehandhabt werden darf. Weitere Informationen finden Sie im Leitfaden für die Vertrauensstufe 1 (LoA1).
15. Die so genannte data hall muss mindestens die Schutzstufe 2 erfüllen (entsprechend dem „Datenraum“, der in der schwedischen Katastrophenschutzbehörde „Guidance for physical security information in the it-room“ genannt wird).
16. Der Auftragsverarbeiter muss über Routinen verfügen, die sicherstellen, dass nur befugtes Personal physischen Zugang zur so genannten Datenhalle hat.
17. Der Auftragsverarbeiter sollte über verschiedene Funktionen, Prozesse und Routinen verfügen, um die Leistung zu überwachen und Prognosen zu erstellen.
18. Der Auftragsverarbeiter sollte die Teile, die in der Lieferung enthalten sind, vor Beschädigungen schützen.
19. Der Auftragsverarbeiter sollte über Routinen und Funktionen für die Sicherung und Wiederherstellung von Informationen entsprechend den mit dem Verantwortlichen vereinbarten Anforderungen an die Zugänglichkeit verfügen. Backups sollten auf die gleiche Weise geschützt werden wie die ursprünglichen Informationen und separat aufbewahrt werden.
20. Log-in-Funktionen sollten für sicherheitsrelevante Ereignisse zur Verfügung stehen, insbesondere für fehlerhafte Log-ins, jede Änderung einer Berechtigung, unerlaubte Verbindungen und Verstöße gegen Berechtigungen.
21. Der Auftragsverarbeiter schützt Log-in-Funktionen und Log-Tools vor Manipulationen und unbefugtem Zugriff, auch durch Mitarbeiter des Auftragsverarbeiters.
22. Das System und die zugehörige Infrastruktur sollten dieselbe Zeitsynchronisation verwenden wie die Zeitquelle, d. h. UTC+0.
23. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über technische Schwachstellen in den gelieferten Komponenten. Gefundene Schwachstellen sind unverzüglich zu beseitigen.
24. Der Verantwortliche wird auf Anfrage über jeden Informationsaustausch mit anderen Systemen außerhalb der Kundenumgebung informiert.
25. Der Auftragsverarbeiter hat Grundsätze und Methoden für die Entwicklung sicherer Systeme festgelegt und dokumentiert und stellt diese dem Verantwortlichen vor.
26. Der Auftragsverarbeiter hat Richtlinien für ein Informationssystem, die er im Rahmen seiner Entwicklungsprozesse einhält.
27. Die hier genannten Verantwortlichkeiten des Auftragsverarbeiters gelten für alle Unterauftragsverarbeiter. Dem Verantwortlichen ist auf Anfrage mitzuteilen, welcher Unterauftragsverarbeiter eingesetzt wird.

28. Der Auftragsverarbeiter sollte über Routinen für die Meldung, Eskalation und Behandlung von Sicherheitsereignissen oder Vorfällen verfügen.
29. Der Auftragsverarbeiter arbeitet bei der Behandlung von Schwachstellen, Sicherheitsereignissen oder Zwischenfällen mit einer vom Verantwortlichen benannten Stelle zusammen.
30. Der Auftragsverarbeiter wird sich gemeinsam mit dem Verantwortlichen ständig darum bemühen, dass bei der Lieferung alle relevanten Gesetze, Vorschriften und Regeln, die für den Betrieb des Verantwortlichen gelten, eingehalten werden.
31. Bei der Verarbeitung personenbezogener Daten muss der Verantwortliche mit dem Auftragsverarbeiter eine Auftragsverarbeitungsvereinbarung abschließen, bevor der Vertrag wirksam wird.
32. Der Auftragsverarbeiter muss eine Genehmigung einholen, bevor die im System enthaltenen Informationen (Texte, Bilder usw.) in einem anderen Zusammenhang wiederverwendet werden.

### ANHANG III - UNTERAUFTRAGSVERARBEITER

LISTE DER UNTERAUFTRAGSVERARBEITER (Quelle: <https://www.smarttech.com/legal/lumio-privacy>)

Der Verantwortliche hat die Anspruchnahme folgender Unterauftragsverarbeiter genehmigt:

#### GÄSTE

##### Selbst gewählter Anzeigename für Gäste

Art: **Anonym**

Wo      Wer      Daten & Zweck

Kanada      SMART Technologies ULC      Für die Grundfunktionalität erforderlich. Der Anzeigename wird in der Lektion oder Aktivität eines Lehrers aufgezeichnet, wenn der Benutzer teilnimmt.

[SLS Terms \(SLS Allgemeine Geschäftsbedingungen\)](#)

[GDPR – EG Adequacy Decision \(Angemessenheitsbeschluss der EU Kommission\)](#)

USA/  
Deutschland      Amazon Web Services, Inc.      Für die Speicherung erforderlich. Wir bieten sowohl eine amerikanische als auch eine europäische Datenspeicherungsoption an.

[AWS Privacy \(Häufig gestellte Fragen zum Datenschutz\)](#)

[AWS GDPR \(Datenschutz-Grundverordnung\) Zentrum\)](#)

USA/  
Belgien      Firebase (Google LLC)      Erforderlich für die Grundfunktionalität (Firebase ist eine Backend-as-a-Service (BaaS) Cloud-Computing-Lösung, die wir für die (vorübergehende) automatisierte Computerverarbeitung in Echtzeit verwenden).

[Firebase Privacy \(Datenschutz und Sicherheit in Firebase\)](#)

[Firebase GDPR \(Datenschutz\)](#)

##### Von Gästen erstellte Inhalte

Art: **Anonym**

Wo      Wer      Daten & Zweck

Kanada      SMART Technologies ULC      Fakultativ (*wird in der Unterrichtsstunde des Lehrers gespeichert*).



---

**Art:** Anonym

---

Wo	Wer	Daten & Zweck
		<a href="#">SLS Terms (SLS Allgemeine Geschäftsbedingungen)</a> <a href="#">GDPR – EG Adequacy Decision (Angemessenheitsbeschluss der EU Kommission)</a>
USA/ Deutschland	Amazon Web Services, Inc.	Für die Speicherung erforderlich. Wir bieten sowohl eine amerikanische als auch eine europäische Datenspeicherungsoption an.  <a href="#">AWS Privacy (Häufig gestellte Fragen zum Datenschutz)</a> <a href="#">AWS GDPR (Datenschutz-Grundverordnung (DSGVO) Zentrum)</a>
USA/ Belgien	Firebase (Google LLC)	Erforderlich für die Grundfunktionalität (Firebase ist eine Backend-as-a-Service (BaaS) Cloud-Computing-Lösung, die wir für die (vorübergehende) automatisierte Computerverarbeitung in Echtzeit verwenden).  <a href="#">Firebase Privacy (Datenschutz und Sicherheit in Firebase)</a> <a href="#">Firebase GDPR (Datenschutz)</a>

### Gast-Analyse

---

**Art:** Anonym

---

Wo	Wer	Daten & Zweck
Kana da	SMART Technolog ies ULC	Erforderlich für Produktverbesserung und Serviceüberwachung. Wir verwenden Mixpanel als unseren Auftragsverarbeiter für diese Zwecke.  <a href="#">SLS Terms (SLS Allgemeine Geschäftsbedingungen)</a> <a href="#">GDPR – EG Adequacy Decision (Angemessenheitsbeschluss der EU Kommission)</a>
USA	Mixpanel, Inc.	Erforderlich für Produktverbesserung und Serviceüberwachung. Mit Mixpanel können wir analysieren, wie unsere nicht identifizierten Nutzer mit Lumio interagieren. Es dient dazu, Trends zu erkennen, das allgemeine aggregierte Nutzungsverhalten zu verstehen und hilft uns, bessere Entscheidungen zu treffen, wie wir die Benutzerfreundlichkeit und die Funktionen unseres Produkts verbessern können. Diese Daten werden auch verwendet, um zu verfolgen, wie lange unsere Server brauchen, um Aktionen wie das Öffnen von Dateien abzuschließen, was uns hilft, den Zustand des Dienstes und die Up/Downtime zu messen.  <a href="#">Mixpanel Privacy (Datenschutzhinweise)</a> <a href="#">Mixpanel GDPR</a>

---

K.A. Drittanbieter Optionale Inhalte oder Aktivitäten, die ein Lehrer zu einer Lektion hinzufügt, wie z. B. er von YouTube oder andere eingebettete Inhalte, die ein Nutzer freiwillig hinzufügt. Wir  
Inhalten können nicht kontrollieren, welche Daten ein Dritter direkt sammelt, wenn ein Lehrer oder Schüler beschließt, diese in eine Lektion einzubinden. Für Premium-Inhalte, die SMART zur Verfügung stellt, melden wir jedoch nur die anonyme Nutzung an den Drittanbieter.

---

USA Sentry.io

- Lektions-ID (keine personenbezogenen Daten)
- Benutzer-ID und Sitzungs-IDs (gehasht und mit sog. Salt versehen zur Wahrung der Anonymität)
- Request header (Anwendung und Version, Plattform, Betriebssystem, Browser, Sprache, Datum und Uhrzeit)
- Bread crumbs (zuletzt besuchte Seiten und angeklickte Links)

Optionale Fehlerberichterstattung durch den Benutzer: Nachdem die automatische Fehlermeldung abgeschlossen ist, haben die Benutzer die Möglichkeit, ihren Namen, ihre E-Mail-Adresse und zusätzliche Informationen über den Fehler anzugeben. Die Benutzer werden auch gefragt, ob sie möchten, dass SMART sich mit ihnen in Verbindung setzt. Diese optionalen persönlichen Informationen werden in Salesforce (in den Vereinigten Staaten) gespeichert und an unser Kundendienstteam weitergegeben.

[Sentry Privacy](#)  
[Sentry GDPR](#)

---

USA Slack Technologies LLC

- Lektions-ID (keine personenbezogenen Daten)
- Benutzer-ID und Sitzungs-IDs (gehasht und gesalzen, um die Anonymität zu wahren)
- Request-Header (Anwendung und Version, Plattform, Betriebssystem, Browser, Sprache, Datum und Uhrzeit)
- Breadcrumbs (zuletzt besuchte Seiten und angeklickte Links)

Optionale Selbstfehlerberichterstattung: Nachdem die automatische Fehlerberichterstattung abgeschlossen ist, haben Benutzer die Möglichkeit, ihren Namen, ihre E-Mail-Adresse und zusätzliche Informationen zum Fehler anzugeben. Die Benutzer werden auch gefragt, ob sie möchten, dass SMART sich mit ihnen in Verbindung setzt. Diese optionalen personenbezogenen Daten werden in Salesforce (mit Sitz in den USA) gespeichert und über Sentry und Slack an unsere Kundensupport- und Entwicklungsteams weitergegeben.

[Slack Privacy](#)  
[Slack GDPR](#)

---

USA Splunk Inc. Erforderliche Metadaten, einschließlich Systemprotokolle und Leistung.

[Splunk Privacy](#)  
[Splunk GDPR](#)

---

**SCHÜLER / MINDERJÄHRIGE, ANGEMELDET**

### Schüler-Konto

**Art:** Identifizierbar

Wo	Wer	Daten & Zweck
Kanada	SMART Technologies ULC	Erforderliche Kontodaten für die Produktfunktionalität: Anzeigenname, vollständiger Name, E-Mail, öffentliches Profilbild, bevorzugte Sprache.  <a href="#">SLS Terms (SLS Allgemeine Geschäftsbedingungen)</a> <a href="#">GDPR – EG Adequacy Decision (Angemessenheitsbeschluss der EU Kommission)</a>
Global	Microsoft, Inc.	Erforderlich, wenn Sie Microsoft als Single-Sign-On-Anbieter (SSO) für den Zugriff auf Lumio verwenden. Microsoft stellt SMART die erforderlichen Kontodaten zur Verfügung.  <a href="#">Microsoft SSO</a> <a href="#">Microsoft Datenschutz</a> <a href="#">Microsoft GDPR</a>
Global	Google LLC	Erforderlich, wenn Sie Google als Single-Sign-On-Anbieter (SSO) für den Zugriff auf Lumio verwenden. Google versorgt SMART mit den erforderlichen Kontodaten.  <a href="#">Google SSO</a> <a href="#">Google Datenschutz</a> <a href="#">Google GDPR</a>
USA/ Deutschland	Amazon Web Services, Inc.	Für die Speicherung erforderlich. Wir bieten sowohl eine amerikanische als auch eine europäische Datenspeicherungsoption an.  <a href="#">AWS Privacy (Häufig gestellte Fragen zum Datenschutz)</a> <a href="#">AWS GPDR (Datenschutz-Grundverordnung (DSGVO) Zentrum)</a>

### Lumio als angemeldeter Schüler verwenden (von Schülern erstellte Inhalte)

**Art:** Pseudonymisiert

Wo	Wer	Daten & Zweck
Kanada	SMART Technologies ULC	Optional. Wenn Schüler an Live-Aktivitäten teilnehmen, bei denen sie Antworten geben oder von ihnen erstellte Inhalte hochladen, werden diese ihrem Konto zugeordnet.

---

		<a href="#">SLS Terms (SLS Allgemeine Geschäftsbedingungen)</a> <a href="#">GDPR – EG Adequacy Decision (Angemessenheitsbeschluss der EU Kommission)</a>
USA/ Deutschland	Amazon Web Services, Inc.	Für die Speicherung erforderlich. Wir bieten sowohl eine amerikanische als auch eine europäische Datenspeicherungsoption an.  <a href="#">AWS Privacy (Häufig gestellte Fragen zum Datenschutz)</a> <a href="#">AWS GPDR (Datenschutz-Grundverordnung (DSGVO) Zentrum)</a>
USA/ Belgien	Firebase (Google LLC)	Erforderlich für die Grundfunktionalität (Firebase ist eine Backend-as-a-Service (BaaS) Cloud-Computing-Lösung, die wir für die (vorübergehende) automatisierte Computerverarbeitung in Echtzeit verwenden).  <a href="#">Firebase Privacy (Datenschutz und Sicherheit in Firebase)</a> <a href="#">Firebase GDPR (Datenschutz)</a>

### **Angemeldeter Schüler Analyse**

**Art: Pseudonymisiert**

---

<b>Wo</b>	<b>Wer</b>	<b>Daten &amp; Zweck</b>
Kana da	SMART Technologies ULC	Erforderlich für Produktverbesserung und Serviceüberwachung. Wir verwenden Mixpanel als unseren Auftragsverarbeiter für diese Zwecke.  <a href="#">SLS Terms (SLS Allgemeine Geschäftsbedingungen)</a> <a href="#">GDPR – EG Adequacy Decision (Angemessenheitsbeschluss der EU Kommission)</a>
USA	Mixpanel, Inc.	Erforderlich für Produktverbesserung und Serviceüberwachung. Mit Mixpanel können wir analysieren, wie unsere nicht identifizierten Nutzer mit Lumio interagieren. Es dient dazu, Trends zu erkennen, das allgemeine aggregierte Nutzungsverhalten zu verstehen und hilft uns, bessere Entscheidungen zu treffen, wie wir die Benutzerfreundlichkeit und die Funktionen unseres Produkts verbessern können. Diese Daten werden auch verwendet, um zu verfolgen, wie lange unsere Server brauchen, um Aktionen wie das Öffnen von Dateien abzuschließen, was uns hilft, den Zustand des Dienstes und die Up/Downtime zu messen.  <a href="#">Mixpanel Privacy (Datenschutzhinweise)</a> <a href="#">Mixpanel GDPR</a>
K.A.	Drittanbieter von Inhalten	Optionale Inhalte oder Aktivitäten, die ein Lehrer zu einer Lektion hinzufügen kann, wie z. B. YouTube-Inhalte oder andere eingebettete Inhalte, die ein Nutzer freiwillig hinzufügt. Wir können nicht kontrollieren, welche Daten ein Dritter direkt über den

---

Inhalt sammelt, wenn ein Lehrer oder Schüler beschließt, diesen in eine Lektion einzubinden. Bei Premium-Inhalten, die SMART zur Verfügung stellt, melden wir jedoch nur die anonyme Nutzung an den Drittanbieter.

---

- USA Sentry.io
- Lektions-ID (keine personenbezogenen Daten)
  - Benutzer-ID und Sitzungs-IDs (gehasht und gesalzen zur Wahrung der Anonymität)
  - Anfragekopf (Anwendung und Version, Plattform, Betriebssystem, Browser, Sprache, Datum und Uhrzeit)
  - Brotkrümel (zuletzt besuchte Seiten und angeklickte Links)

Optionale Fehlerberichterstattung durch den Benutzer: Nachdem die automatische Fehlermeldung abgeschlossen ist, haben die Benutzer die Möglichkeit, ihren Namen, ihre E-Mail-Adresse und zusätzliche Informationen über den Fehler anzugeben. Die Benutzer werden auch gefragt, ob sie möchten, dass SMART sich mit ihnen in Verbindung setzt. Diese optionalen persönlichen Informationen werden in Salesforce (in den Vereinigten Staaten) gespeichert und an unser Kundendienstteam weitergegeben.

[Sentry Privacy](#)  
[Sentry GDPR](#)

- 
- USA Slack Technologies LLC
- Lektions-ID (keine personenbezogenen Daten)
  - Benutzer-ID und Sitzungs-IDs (gehasht und gesalzen, um die Anonymität zu wahren)
  - Request-Header (Anwendung und Version, Plattform, Betriebssystem, Browser, Sprache, Datum und Uhrzeit)
  - Breadcrumbs (zuletzt besuchte Seiten und angeklickte Links)

Optionale Selbstfehlerberichterstattung: Nachdem die automatische Fehlerberichterstattung abgeschlossen ist, haben Benutzer die Möglichkeit, ihren Namen, ihre E-Mail-Adresse und zusätzliche Informationen zum Fehler anzugeben. Die Benutzer werden auch gefragt, ob sie möchten, dass SMART sich mit ihnen in Verbindung setzt. Diese optionalen personenbezogenen Daten werden in Salesforce (mit Sitz in den USA) gespeichert und über Sentry und Slack an unsere Kundensupport- und Entwicklungsteams weitergegeben.

[Slack Privacy](#)  
[Slack GDPR](#)

- 
- USA Splunk Inc.
- Erforderliche Metadaten, einschließlich Systemprotokolle und Leistung.
- [Splunk Privacy](#)  
[Splunk GDPR](#)

## LEHRER/ERWACHSENE, ANGEMELDET

### Lehrerkonto

**Art:** Identifizierbar

Wo	Wer	Daten & Zweck
Kanada	SMART Technologies ULC	Erforderliche Kontodetails: Anzeigenname, Name, E-Mail, öffentliches Profilbild, Sprachpräferenz. Erforderliche Einstellungen des Kontoprofils: Opt-Ins, Benutzertyp, Standort.  <a href="#">SLS Terms (SLS Allgemeine Geschäftsbedingungen)</a> <a href="#">GDPR – EG Adequacy Decision (Angemessenheitsbeschluss der EU Kommission)</a>
Global	Microsoft, Inc.	Erforderlich, wenn Sie Microsoft als Single-Sign-On-Anbieter (SSO) für den Zugriff auf Lumio verwenden. Microsoft stellt SMART die erforderlichen Kontodaten zur Verfügung.  <a href="#">Microsoft SSO</a> <a href="#">Microsoft Privacy</a> <a href="#">Microsoft GDPR</a>
Global	Google LLC	Erforderlich, wenn Sie Google als Single-Sign-On-Anbieter (SSO) für den Zugriff auf Lumio verwenden. Microsoft stellt SMART die erforderlichen Kontodaten zur Verfügung.  <a href="#">Google SSO</a> <a href="#">Google Datenschutz</a> <a href="#">Google GDPR</a>
USA/ Deutschland	Amazon Web Services, Inc.	Für die Speicherung erforderlich. Wir bieten sowohl eine amerikanische als auch eine europäische Datenspeicherungsoption an.  <a href="#">AWS Privacy (Häufig gestellte Fragen zum Datenschutz)</a> <a href="#">AWS GPDR (Datenschutz-Grundverordnung (DSGVO) Zentrum)</a>

### Lumio als angemeldete Lehrkraft verwenden (von Lehrkräften erstellte Inhalte)

**Art:** Identifizierbar

Wo	Wer	Daten & Zweck
Kanada	SMART Technologies ULC	Generierte Inhalte (von einer Lehrkraft erstellte Lektionen und Aktivitäten). Selbst gewählte Klassennamen.



---

K.A.	Drittanbieter von Inhalten	Optionale Inhalte oder Aktivitäten, die ein Lehrer zu einer Lektion hinzufügen kann, wie z. B. YouTube-Inhalte oder andere eingebettete Inhalte, die ein Nutzer freiwillig hinzufügt. Wir können nicht kontrollieren, welche Daten ein Dritter direkt über den Inhalt sammelt, wenn ein Lehrer oder Schüler beschließt, diesen in eine Lektion einzubinden. Bei Premium-Inhalten, die SMART zur Verfügung stellt, melden wir jedoch nur die anonyme Nutzung an den Drittanbieter.
USA	Sentry.io	<ul style="list-style-type: none"><li>• Lektions-ID (keine personenbezogenen Daten)</li><li>• Benutzer-ID und Sitzungs-IDs (gehasht und gesalzen zur Wahrung der Anonymität)</li><li>• Anfragekopf (Anwendung und Version, Plattform, Betriebssystem, Browser, Sprache, Datum und Uhrzeit)</li><li>• Brotkrümel (zuletzt besuchte Seiten und angeklickte Links)</li></ul> <p>Optionale Fehlerberichterstattung durch den Benutzer: Nachdem die automatische Fehlermeldung abgeschlossen ist, haben die Benutzer die Möglichkeit, ihren Namen, ihre E-Mail-Adresse und zusätzliche Informationen über den Fehler anzugeben. Die Benutzer werden auch gefragt, ob sie möchten, dass SMART sich mit ihnen in Verbindung setzt. Diese optionalen persönlichen Informationen werden in Salesforce (in den Vereinigten Staaten) gespeichert und an unser Kundendienstteam weitergegeben.</p>
USA	Slack Technologies LLC	<ul style="list-style-type: none"><li>• Lektions-ID (keine personenbezogenen Daten)</li><li>• Benutzer-ID und Sitzungs-IDs (gehasht und gesalzen, um die Anonymität zu wahren)</li><li>• Request-Header (Anwendung und Version, Plattform, Betriebssystem, Browser, Sprache, Datum und Uhrzeit)</li><li>• Breadcrumbs (zuletzt besuchte Seiten und angeklickte Links)</li></ul> <p>Optionale Selbstfehlerberichterstattung: Nachdem die automatische Fehlerberichterstattung abgeschlossen ist, haben Benutzer die Möglichkeit, ihren Namen, ihre E-Mail-Adresse und zusätzliche Informationen zum Fehler anzugeben. Die Benutzer werden auch gefragt, ob sie möchten, dass SMART sich mit ihnen in Verbindung setzt. Diese optionalen personenbezogenen Daten werden in Salesforce (mit Sitz in den USA) gespeichert und über Sentry und Slack an unsere Kundensupport- und Entwicklungsteams weitergegeben.</p> <p><a href="#">Slack Privacy</a> <a href="#">Slack GDPR</a></p>
USA	Splunk Inc.	Erforderliche Metadaten, einschließlich Systemprotokolle und Leistung.  <a href="#">Splunk Privacy</a> <a href="#">Splunk GDPR</a>

---



## GESAMMELTE UND VERARBEITETE KUNDENDATEN

In diesem Abschnitt wird beschrieben, welche Daten von Kunden (Käufern, Interessenten und autorisierten Vertriebspartnern von SMART) erfasst, verarbeitet und weitergegeben werden. Sie können über unseren Kundendienst jederzeit die Löschung von Daten und Konten beantragen, aber wir müssen alle Daten, die für Käufe und Finanztransaktionen relevant sind, so lange aufbewahren, bis sie nach geltendem Recht nicht mehr erforderlich sind. Der Begriff „identifizierbar“, der in der nachstehenden Tabelle verwendet wird, bedeutet nicht unbedingt persönlich identifizierbare Informationen.

Wo	Wer	Rolle	Daten & Zweck	Typ
K.A.	Wiederverkäufer & SMARTs Regionalbüro	Verkäufer	Erforderliche Kontaktinformationen: Name des Unternehmens, E-Mail, Titel, Telefon, Adresse. Erforderliche Bestellinformationen: Produkt, Menge, Preis und Steuer, Lieferung. Erkundigen Sie sich bei Ihrem regionalen Händler nach den Datenschutzhinweisen.	Identifizierbar
Kanada	SMART Technologies ULC	Hersteller	Erforderliche Kontoinformationen: Name des Unternehmens, E-Mail, Titel, Telefon, Adresse, Wiederverkäufer, aktuelle Abonnements. Erforderliche Bestellinformationen: Produkt, Menge, Preis und Steuer, Lieferung. Erforderliche Admin-Portal-Informationen für die Lizenzbereitstellung: Lizenzen und Aktivierungen, Vor- und Nachnamen von Lehrern und Administratoren (kann eine Nicht-personenbezogene Daten-Version bereitstellen, um DSGVO einzuhalten) sowie E-Mail-Adressen und Klassennamen (kann eine Nicht-personenbezogene Daten-Version sein, um DSGVO einzuhalten).	Identifizierbar

Wo	Wer	Rolle	Daten & Zweck	Typ
			<a href="#">SLS Terms (SLS Allgemeine Geschäftsbedingungen)</a> <a href="#">GDPR – EG Adequacy Decision</a> <a href="#">(Angemessenheitsbeschluss der EU Kommission)</a>	
Kanada	Blue Ocean Contact Centers, Inc.	Unterstützung	<p>Optional. Blue Ocean ist ein Unterauftragnehmer, der Live-Support (Telefon, E-Mail und Web) anbietet. Zu den erfassten Informationen gehören der Name des Unternehmens, der Name des Anrufers (aus DSGVO-Gründen kann auch nur der Name des Unternehmens verwendet werden), die E-Mail-Adresse (aus DSGVO-Gründen kann auch eine Nicht- personenbezogene Daten -Version angegeben werden), der Titel, die Telefonnummer, die Adresse sowie eine Beschreibung des Problems und alle gemeinsamen Details, die zur Lösung des Problems beitragen. Anrufe werden aufgezeichnet.</p> <p> <a href="#">Blue Ocean Datenschutz</a>  <a href="#">GDPR – EG Adequacy Decision</a>  <a href="#">(Angemessenheitsbeschluss der EU Kommission)</a> </p>	Identifizierbar
USA/Deutschland	Amazon Web Services, Inc.	Verarbeitung, Back-Office	<p>Erforderlich für die Produktinfrastruktur, einschließlich des Hostings von Aufzeichnungen von Support-Anrufen.</p> <p> <a href="#">AWS-Datenschutz</a>  <a href="#">AWS GDPR</a> </p>	Identifizierbar

Wo	Wer	Rolle	Daten & Zweck	Typ
USA	Google, LLC.	Bearbeitung, Back-Office.	Fakultativ. Wird nur für die Bearbeitung von Supportformularen verwendet. Google-Formulare werden verwendet, wenn ein Käufer unseren Außendienst in Anspruch nimmt (z. B. bei Vor-Ort-Support).	Identifizierbar
			<a href="#">Google Datenschutz</a> <a href="#">Google GDPR</a>	
USA	Microsoft, Inc.	Verarbeitung, Back-Office	Erforderlich für unser ERP-System (Enterprise Resource Planning), eine Software zur Verwaltung der täglichen Geschäftsaktivitäten wie Buchhaltung, Beschaffung, Projektmanagement und Lieferkette, sowie für unser E-Mail-System, PowerBI® (Datenvisualisation) und SharePoint® (Dokumentenmanagement), sowie für alle anderen Standard-Microsoft-Office-Softwaretitel wie Word, Excel usw.	Identifizierbar
			<a href="#">Microsoft Datenschutz</a> <a href="#">Microsoft GDPR</a>	
USA	BigCommerce, Bestellung Inc.		Optional. Wird nur verwendet, wenn ein Kunde über unseren E-Commerce-Shop einkauft: Name des Kunden, E-Mail, Titel, Telefon, Adresse, gekauftes Produkt oder Dienstleistung und ob die Zahlung eingegangen ist.	Identifizierbar
			<a href="#">BigCommerce Datenschutz</a> <a href="#">BigCommerce GDPR</a>	

Wo	Wer	Rolle	Daten & Zweck	Typ
USA	Stripe, Inc. und Stripe Payments Europe, Ltd.	Bestellung	<p>Optional. Wird nur verwendet, wenn ein Kunde über unseren E-Commerce-Shop mit einer Kreditkarte einkauft: Name des Kunden, E-Mail, Titel, Telefon, Adresse, erworbenes Produkt oder Dienstleistung, Kreditkartendaten. Einwohner des Europäischen Wirtschaftsraums (EWR), des Vereinigten Königreichs und der Schweiz. Verantwortlich für die Erfassung und Verarbeitung personenbezogener Kreditkartendaten von Einwohnern des EWR, des Vereinigten Königreichs und der Schweiz ist Stripe Payments Europe, Ltd, ein in Irland eingetragenes Unternehmen mit Sitz in 1 Grand Canal Street Lower, Grand Canal Dock, Dublin. Um Ihre Rechte auszuüben, können Sie den Datenschutzbeauftragten über <a href="mailto:dpo@stripe.com">dpo@stripe.com</a> kontaktieren.</p> <p><a href="#">Stripe Datenschutz Streifen GDPR</a></p>	Identifizierbar
USA	Salesforce.com, Inc.	Bestellung, Marketing, Vertriebsunterstützung	<p>Erforderliche Bestellinformationen (Produkt, Menge, Preis und Steuer, Lieferung). Erforderlich für unser Kundenbeziehungsmanagement (CRM).</p> <p>Erforderlich, damit unsere autorisierten Distributoren und Wiederverkäufer mit SMART zusammenarbeiten</p>	Identifizierbar

Wo	Wer	Rolle	Daten & Zweck	Typ
			<p>können. Grundlegende Kunden- und Kaufinformationen werden zwischen SMART und seinen autorisierten Vertriebshändlern und Wiederverkäufern ausgetauscht.</p> <p><a href="#">Salesforce Datenschutz</a> <a href="#">Vertriebsmitarbeiter GDPR</a></p>	
USA	HubSpot, Inc.	Marketing	<p>Optional. Wir verwenden HubSpot, ein Customer Relationship Management (CRM), für Personen, die sich ausdrücklich dafür entschieden haben, bestimmte Mitteilungen zu erhalten, z. B. Marketing, Schulungen, Nachrichten und Angebote von uns.</p> <p><a href="#">Hubspot Datenschutz</a> <a href="#">Hubspot GDPR</a></p>	Identifizierbar
USA	Mixpanel, Inc.	Überwachung	<p>Erforderlich für Produktverbesserung und Serviceüberwachung. Mixpanel ermöglicht es uns zu analysieren, wie unsere nicht identifizierten Nutzer mit Notebook interagieren. Es dient dazu, Trends zu erkennen, das allgemeine aggregierte Nutzungsverhalten zu verstehen und hilft uns, bessere Entscheidungen zu treffen, wie wir die Benutzerfreundlichkeit und die Funktionen unseres Produkts verbessern können. Diese Daten werden auch verwendet, um zu verfolgen, wie lange unsere Server</p>	Pseudonymisiert

Wo	Wer	Rolle	Daten & Zweck	Typ
			<p>brauchen, um Aktionen wie das Öffnen von Dateien abzuschließen, was uns hilft, den Zustand des Dienstes und die Up/Downtime zu messen.</p> <p><a href="#">Mixpanel Datenschutz</a> <a href="#">Mixpanel GDPR</a></p>	
USA	Gainsight, Inc.	Marketing	<p>Gilt nur für Kunden in den USA. Wir verwenden Gainsight, ein CRM-Tool (Customer Relationship Management), für E-Mail-Marketing (Name, E-Mail-Adresse, Unternehmensinformationen) an Einzelpersonen und Organisationen.</p> <p><a href="#">Gainsight Datenschutz</a></p>	Identifizierbar
Kanada	Call Miner	Unterstützen	<p>Optional. Verarbeitung für telefonische Interaktionen (Option zum Deaktivieren von Anrufaufzeichnungen), erforderlich für E-Mails. Call Miner ist ein Unterauftragsverarbeiter, der Omnichannel-Interaktionsanalysen auf Basis von KI und maschinellem Lernen bereitstellt. Call Miner analysiert Kundensupport-Interaktionen, einschließlich aufgezeichneter Anrufe und E-Mails, die vorübergehend in CallMiner gespeichert werden. Die Metadaten werden in CallMiner gespeichert, um die Kundenerfahrung zu analysieren und Trendinformationen zu den</p>	Identifizierbar

Wo	Wer	Rolle	Daten & Zweck	Typ
			Interaktionen zwischen Agent und Kunde zu erhalten.  <a href="#">Call Miner Privacy and Security</a>	
USA or Europe	Digital River	Ordnung	Optional. Online-Auftragsannahme (E-Commerce). Wird nur verwendet, wenn Einkäufe über unseren E-Commerce-Shop getätigt werden. SMART hat keinen Zugriff auf Kreditkarteninformationen, sondern nur auf Digital River.  <a href="#">Digital River Privacy</a> <a href="#">Digital River GDPR</a>	Identifizierbar
Kanada	Fivetran Inc	Verarbeitung, Backoffice	Erforderlicher Datenconnectordienst. Verschiebt Daten aus Systemanwendungen in Snowflake.  <a href="#">Fivetran Privacy</a> <a href="#">Fivetran Security</a>	Identifizierbare Konto- und Kaufinformationen
Vereinigtes Königreich	Kluster Enterprises Limited	Umsatzprognose	Erforderlich, um Analysen zu unseren Verkaufsdaten bereitzustellen.  <a href="#">Kluster Privacy</a> <a href="#">Kluster GDPR</a>	Identifizierbare Konto- und Kaufinformationen
USA	LinkedIn	Marketing	Erforderlich, wenn Sie sich für den Erhalt von Marketingmitteilungen entscheiden. Wird verwendet, um eine Lookalike Audience zu erstellen, die an SMART interessiert sein könnte, weil sie Personen ähnelt, die sich bereits ausdrücklich für den	Identifizierbare Konto- und Kaufinformationen

Wo	Wer	Rolle	Daten & Zweck	Typ
			<p>Erhalt bestimmter Mitteilungen entschieden haben, z. B. Marketing, SMART-Lösungen, Veranstaltungen und Sonderangebote.</p> <p><a href="#">LinkedIn Privacy</a> <a href="#">LinkedIn GDPR</a></p>	
USA	Meta Platforms, Inc.	Marketing	<p>Erforderlich, wenn Sie sich für den Erhalt von Marketingmitteilungen entscheiden. Wird verwendet, um eine Lookalike Audience zu erstellen, die an SMART interessiert sein könnte, weil sie Personen ähnelt, die sich bereits ausdrücklich für den Erhalt bestimmter Mitteilungen entschieden haben, z. B. Marketing, SMART-Lösungen, Veranstaltungen und Sonderangebote.</p> <p><a href="#">Meta Platforms Privacy</a></p>	Identifizierbare Kontaktinformationen
USA	Outreach Corporation	Marketing	<p>Erforderlich, wenn Sie sich für den Erhalt von Marketingmitteilungen entscheiden. Outreach wird verwendet, um unsere Kunden in Nordamerika zu kontaktieren, die sich ausdrücklich für den Erhalt bestimmter Mitteilungen wie Marketing, Schulungen, Neuigkeiten und Angebote von uns entschieden haben.</p>	Identifizierbare Konto- und Kaufinformationen



Wo	Wer	Rolle	Daten & Zweck	Typ
			Outreach bietet auch Analysen. <a href="#">Outreach Privacy</a> <a href="#">Outreach Security</a>	
Kanada	Sana Commerce	Ordnung	Nur erforderlich, wenn der Kunde Teile kauft. Bearbeiten Sie Bestellungen und Zahlungen (bei Verwendung von Sana Pay). <a href="#">Sana Privacy</a> <a href="#">Sana GDPR</a>	Identifizierbare Konto- und Kaufinformationen
USA	Sigma Computing, Inc.	Verarbeitung, Backoffice	Erforderlich für Webanwendungen, die internen Benutzern Snowflake-Daten (siehe unten) präsentieren. <a href="#">Sigma Privacy</a>	Identifizierbare Konto- und Kaufinformationen
Kanada	Snowflake, Inc.	Verarbeitung, Backoffice	Erforderlich. Snowflake aggregiert und zentralisiert die Kundendaten von SMART aus mehreren Quellen (Salesforce, Microsoft Dynamics, HubSpot, Oracle/OBIEE, Pivotal). Erforderlich für die Verarbeitung und das Backoffice. <a href="#">Snowflake Privacy</a> <a href="#">Snowflake Security</a>	Identifizierbare Konto- und Kaufinformationen