# Vertrag über die Verarbeitung personenbezogener Daten im Auftrag gemäß Art.28 DSGVO (Auftragsverarbeitungsvertrag)

zwischen

---

Verantwortlicher, im Folgenden „**Auftraggeber**“ genannt –

und

Clama Schulsoftware UG (haftungsbeschränkt)
Großer Burstah 46-48
20457 Hamburg

– Auftragsverarbeiter, im Folgenden „**Auftragnehmer**“ genannt –

– beide gemeinsam nachfolgend „**die Parteien**“ genannt –

## 1. Vertragsgegenstand

Im Rahmen der Erbringung der zwischen den Parteien bestehenden vertraglichen Leistungsbeziehungen zur Bereitstellung einer Software zur Gewaltprävention (nachfolgend „Hauptvertrag“ genannt) erhält der Auftragnehmer im gemäß des Hauptvertrags definierten Umfang (insb. Funktionen) Zugriff auf personenbezogene Daten, für welche der Auftraggeber datenschutzrechtlich verantwortlich ist oder welche der Auftraggeber gemäß Art. 28 Datenschutz-Grundverordnung verarbeitet (nachfolgend „**Auftraggeber-Daten**“ genannt, Datenschutz-Grundverordnung nachfolgend „**DSGVO**“).

Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien bei der Durchführung des Hauptvertrages im Hinblick auf den Umgang mit Auftraggeber-Daten.

## 2. Umfang der Beauftragung

2.1. Der Auftragnehmer verarbeitet Auftraggeber-Daten im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 28 Abs. 1 DSGVO (nachfolgend „**Auftragsverarbeitung**“ genannt). Der Auftraggeber bleibt Verantwortlicher im datenschutzrechtlichen Sinn.

2.2. Die Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer erfolgt in der Art, dem Umfang und zu dem Zweck wie in **Anlage 1** zu diesem Vertrag spezifiziert; die Verarbeitung betrifft die darin bezeichneten Arten personenbezogener Daten und Kategorien betroffener Personen. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.

2.3. Die Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer findet grundsätzlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union (EU) oder einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt.

## 3. Weisungsbefugnisse des Auftraggebers

3.1. Der Auftragnehmer verarbeitet die Auftraggeber-Daten gemäß den Weisungen des Auftraggebers, es sei denn der Auftragnehmer ist nach dem Unionsrecht oder dem Recht der Mitgliedsstaaten zur Verarbeitung verpflichtet, Art. 29 DSGVO. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen rechtzeitig vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.2. Die Weisungen des Auftraggebers sind grundsätzlich abschließend in den Bestimmungen dieses Vertrags festgelegt und dokumentiert. Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers, sie sind zu dokumentieren und die Übernahme etwa dadurch bedingter Mehrkosten des Auftragnehmers durch den Auftraggeber ist zu regeln.

3.3. Weisungen sollen im Regelfall von dem Weisungsberechtigten des Auftraggebers oder dessen Stellvertreter erteilt werden. Die Weisungsberechtigten und deren Stellvertreter sind in **Anlage 1** festgelegt.

3.4. Der Auftraggeber wird dem Auftragnehmer einen Wechsel in der Person des Weisungsberechtigten oder des Stellvertreters möglichst frühzeitig anzeigen.

3.5. Die von den Parteien vereinbarten Empfangsberechtigten für Weisungen auf Seiten des Auftragnehmers sind in **Anlage 1** bestimmt.

In dringenden Fällen darf der Auftraggeber aber auch jedem anderen Beschäftigten des Auftragnehmers entsprechende Weisungen erteilen, sofern weder der Empfangsberechtigte noch sein Stellvertreter für den Auftraggeber erreichbar waren.

3.6. Ein Wechsel in der Person des Empfangsberechtigten oder des Stellvertreters bzw. deren dauerhafte Verhinderung wird der Auftragnehmer dem Auftraggeber unter Benennung eines Vertreters mitteilen. Bis zum Zugang einer solchen Mitteilung beim Auftraggeber gelten die benannten Personen weiter als empfangsberechtigt für Weisungen des Auftraggebers.

3.7. Der Auftragnehmer gewährleistet, dass er die Auftraggeber-Daten im Einklang mit den Bestimmungen dieses Vertrags und den Weisungen des Auftraggebers verarbeitet. Ist der Auftragnehmer der begründeten Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, ist er nach einer entsprechenden Mitteilung an den Auftraggeber berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung in Textform durch den Auftraggeber auszusetzen. Die Parteien stimmen darin überein, dass die alleinige Verantwortung für die weisungsgemäße Verarbeitung der Auftraggeber-Daten beim Auftraggeber liegt.

## 4. Verantwortlichkeit des Auftraggebers

4.1. Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen im Verhältnis der Parteien zueinander allein verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund der Verarbeitung von Auftraggeber-Daten nach Maßgabe dieses Vertrages Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.

4.2. Dem Auftraggeber obliegt es, dem Auftragnehmer die Auftraggeber-Daten rechtzeitig zur Leistungserbringung nach dem Hauptvertrag zur Verfügung zu stellen und er ist verantwortlich für die Qualität der Auftraggeber-Daten. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

4.3. Der Auftraggeber hat dem Auftragnehmer auf Anforderung die in Art. 30 Abs. 2 DSGVO genannten Angaben zur Verfügung zu stellen, soweit sie dem Auftragnehmer nicht selbst vorliegen.

4.4. Ist der Auftragnehmer gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von Auftraggeber-Daten zu erteilen oder mit diesen Stellen anderweitig zusammenzuarbeiten, so ist der Auftraggeber verpflichtet, den Auftragnehmer auf erstes Anfordern bei der Erteilung solcher Auskünfte bzw. der Erfüllung anderweitiger Verpflichtungen zur Zusammenarbeit zu unterstützen.

## 5. Anforderungen an Personal

Der Auftragnehmer hat alle Personen, die Auftraggeber-Daten verarbeiten, bezüglich der Verarbeitung von Auftraggeber-Daten zur Vertraulichkeit zu verpflichten.

## 6. Sicherheit der Verarbeitung

6.1. Der Auftragnehmer wird die gemäß Art. 32 DSGVO erforderlichen, geeigneten technischen und organisatorischen Maßnahmen ergreifen, die unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Auftraggeber-Daten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeber-Daten zu gewährleisten.

Der Auftragnehmer wird insbesondere die in **Anlage 2** zu diesem Vertrag spezifizierten technischen und organisatorischen Maßnahmen ergreifen und gewährleisten, dass die Verarbeitung von Auftraggeber-Daten im Einklang mit diesen Maßnahmen durchgeführt wird.

6.2. Dem Auftragnehmer ist es gestattet, technische und organisatorische Maßnahmen während der Laufzeit des Vertrages zu ändern oder anzupassen, solange sie weiterhin den gesetzlichen Anforderungen genügen.

## 7. Inanspruchnahme weiterer Auftragsverarbeiter

7.1. Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung, weitere Auftragsverarbeiter hinsichtlich der Verarbeitung von Auftraggeber-Daten hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses hinzugezogenen weiteren Auftragsverarbeiter ergeben sich aus **Anlage 3**. Generell nicht genehmigungspflichtig sind Vertragsverhältnisse mit Dienstleistern, die die Prüfung oder Wartung von Datenverarbeitungsverfahren oder -anlagen durch andere Stellen oder andere Nebenleistungen zum Gegenstand haben, auch wenn dabei ein Zugriff auf Auftraggeber-Daten nicht ausgeschlossen werden kann, solange der Auftragnehmer angemessene Regelungen zum Schutz der Vertraulichkeit der Auftraggeber-Daten trifft.

7.2. Der Auftragnehmer wird den Auftraggeber vorab über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter informieren. Dem Auftraggeber steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines potentiellen weiteren Auftragsverarbeiters zu erheben. Soweit der Auftraggeber nicht innerhalb von 4 Wochen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Bis zum Ablauf der Einspruchsfrist wird der Auftragnehmer den weiteren Auftragsverarbeiter nicht einsetzen. Erhebt der Auftraggeber Einspruch, sind der Auftragnehmer sowie auch der Auftraggeber berechtigt, den Hauptvertrag und diesen Vertrag mit einer Frist von 3 Monaten zu kündigen.

Sofern der Hauptvertrag kürzere Fristen für eine ordentliche Kündigung vorsieht, sind diese kürzeren Kündigungsfristen auch hier anwendbar.

7.3. Der Vertrag zwischen dem Auftragnehmer und dem weiteren Auftragsverarbeiter muss letzterem dieselben Pflichten auferlegen, wie sie dem Auftragnehmer kraft dieses Vertrages obliegen. Die Parteien stimmen überein, dass diese Anforderung erfüllt ist, wenn der Vertrag ein diesem Vertrag entsprechendes Schutzniveau aufweist bzw. dem weiteren Auftragsverarbeiter die in Art. 28 Abs. 3 DSGVO festgelegten Pflichten auferlegt sind.

## 8. Rechte der betroffenen Personen

8.1. Der Auftragnehmer wird den Auftraggeber mit technischen und organisatorischen Maßnahmen im Rahmen des Zumutbaren dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.

8.2. Soweit eine betroffene Person einen Antrag auf Wahrnehmung der ihr zustehenden Rechte unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen zeitnah an den Auftraggeber weiterleiten.

8.3. Der Auftragnehmer wird dem Auftraggeber Informationen über die gespeicherten Auftraggeber-Daten, die Empfänger von Auftraggeber-Daten, an die der Auftragnehmer sie auftragsgemäß weitergibt, und den Zweck der Speicherung mitteilen, sofern dem Auftraggeber diese Informationen nicht selbst vorliegen oder er sie sich selbst beschaffen kann.

8.4. Der Auftragnehmer wird es dem Auftraggeber ermöglichen, Auftraggeber-Daten zu berichtigen, zu löschen oder ihre weitere Verarbeitung einzuschränken oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Einschränkung der weiteren Verarbeitung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.

8.5. Soweit die betroffene Person gegenüber dem Auftraggeber ein Recht auf Datenübertragbarkeit bezüglich der Auftraggeber-Daten nach Art. 20 DGVO besitzt, wird der Auftragnehmer den Auftraggeber bei der Bereitstellung der Auftraggeber-Daten in einem gängigen und maschinenlesbaren Format unterstützen, wenn der Auftraggeber sich die Daten nicht anderweitig beschaffen kann.

## 9. Mitteilungs- und Unterstützungspflichten des Auftragnehmers

9.1. Soweit den Auftraggeber eine gesetzliche Melde- oder Benachrichtigungspflicht wegen einer Verletzung des Schutzes von Auftraggeber-Daten (insbesondere nach Art. 33, 34 DSGVO) trifft, wird der Auftragnehmer den Auftraggeber zeitnah über etwaige meldepflichtige Ereignisse in seinem Verantwortungsbereich informieren. Der Auftragnehmer wird den Auftraggeber bei der Erfüllung der Melde- und Benachrichtigungspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen unterstützen.

9.2. Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei etwa vom Auftraggeber durchzuführenden Datenschutz-Folgenabschätzungen und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO unterstützen. Gleiches gilt bei etwaigen notwendigen Unterstützungshandlungen gemäß Art. 32 DSGVO. Eine Kostenerstattung ist ausgeschlossen, wenn die Unterstützung wegen eines Gesetzes- oder Vertragsverstoßes des Auftragnehmers erforderlich wurde.

## 10. Datenlöschung und -rückgabe

10.1. Der Auftragnehmer wird mit Beendigung der Erbringung der Verarbeitungsleistungen alle Auftraggeber-Daten löschen, sofern nicht gesetzlich eine Verpflichtung des Auftragnehmers zur weiteren Speicherung der Auftraggeber-Daten besteht.

10.2. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung von Auftraggeber-Daten dienen, dürfen durch den Auftragnehmer auch nach Vertragsende aufbewahrt werden, sofern sichergestellt ist, dass diese keine personenbezogenen Daten enthalten.

## 11. Nachweise und Überprüfungen

11.1. Der Auftragnehmer wird dem Auftraggeber auf dessen Anforderung alle erforderlichen und beim Auftragnehmer vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem Vertrag zur Verfügung stellen.

11.2. Der Auftraggeber ist berechtigt, den Auftragnehmer bezüglich der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, zu überprüfen; einschließlich durch Inspektionen.

11.3. Zur Durchführung von Inspektionen nach Ziff. 11.2. ist der Auftraggeber berechtigt, im Rahmen der üblichen Geschäftszeiten (montags bis freitags von 10 bis 18 Uhr) nach rechtzeitiger Vorankündigung, gemäß Ziff. 11.5., ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers die Geschäftsräume des Auftragnehmers zu betreten, in denen Auftraggeber-Daten verarbeitet werden. Die Vorankündigung ist entbehrlich, sofern eine Kontrolle ohne vorherige Anmeldung erforderlich erscheint, weil andernfalls der Kontrollzweck gefährdet wäre.

11.4. Der Auftragnehmer ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Überprüfungszwecke sind, zu erhalten.

11.5. Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Überprüfung zusammenhängenden Umstände zu informieren. Der Auftraggeber darf eine Überprüfung pro Kalenderjahr durchführen. Weitere Überprüfungen erfolgen gegen Kostenerstattung und nach Abstimmung mit dem Auftragnehmer. Die Kostentragungspflicht des Auftraggebers entfällt, wenn die Kontrolle wegen eines Gesetzes- oder Vertragsverstoßes des Auftragnehmers erforderlich wurde.

11.6. Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Überprüfung, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund von dieser Ziff. 11 dieses Vertrags gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber ihm die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen unmittelbaren Wettbewerber des Auftragnehmers mit der Kontrolle beauftragen.

11.7. Der Auftraggeber ist berechtigt, die Kontrollhandlungen nach dieser Ziff. 11. selbst oder durch einen zur Geheimhaltung verpflichteten Bevollmächtigten vorzunehmen. Der Auftragnehmer ist verpflichtet, die Kontrollhandlungen eines solchen Bevollmächtigten in derselben Weise zu dulden und zu unterstützen wie Kontrollen durch den Auftraggeber.

11.8. Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der Pflichten nach diesem Vertrage anstatt durch eine Inspektion auch durch die Vorlage eines geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit – z.B. nach BSI-Grundschutz – („Prüfungsbericht“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

## 12. Vertragsdauer und Kündigung

Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Die Regelungen zur ordentlichen Kündigung des Hauptvertrags gelten entsprechend. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

## 13. Haftung und Vertragsstrafe

Für die Haftung des Auftragnehmers nach diesem Vertrag gelten die Haftungsausschlüsse und -begrenzungen gemäß dem Hauptvertrag. Soweit Dritte Ansprüche gegen den Auftragnehmer geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftraggebers gegen diesen Vertrag oder gegen eine seiner Pflichten als datenschutzrechtlich Verantwortlicher haben, stellt der Auftraggeber den Auftragnehmer von diesen Ansprüchen auf erstes Anfordern frei.

## 14. Schlussbestimmungen

14.1. Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und den Anforderungen des Art. 28 DSGVO am besten gerecht wird.

14.2. Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrags vor.

14.3. Jede Änderung dieses Vertrages bedarf einer ausdrücklichen schriftlichen Vereinbarung zwischen den Parteien. Textform genügt nicht, es sei denn diese ist in bestimmten Regelungen dieses Vertrags ausdrücklich erlaubt.

| | |
|---|---|
| Ort / Datum | Ort / Datum |
| Auftraggeber | Auftragnehmer |

**Anlagen:**

**Anlage 1:** Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen, Kontaktdaten

**Anlage 2:** Technische und organisatorische Maßnahmen

**Anlage 3:** Genehmigte Unterauftragnehmer

**Anlage 1:**

**Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen, Kontaktdaten**

1. **Art der Leistung** (Mehrauswahl möglich)

   Bereitstellung und Betrieb einer Gewaltpräventionsplattform als Software as a Service (SaaS)

2. **Gegenstand und Umfang der Datenverarbeitung**

   Zur Leistungserbringung nach dem Hauptvertrag und den zugehörigen Leistungsvereinbarungen führt der Auftragnehmer die nachfolgend beschriebene Verarbeitung von Auftraggeber-Daten durch:

   - ☐ Speicherung von Auftraggeber-Daten zur Bereitstellung der Software-Funktionen
   - ☐ anlassbezogener Zugriff auf Auftraggeber-Daten zu Supportzwecken auf Weisung des Auftraggebers

   Der Umfang der Datenverarbeitung richtet sich nach dem Umfang der vom Auftraggeber in die Software eingegebenen Auftraggeber-Daten.

3. **Ort der Daten*speicherung*** durch den Auftragnehmer oder einen Unterauftragsverarbeiter

   - ☐ Bundesrepublik Deutschland
   - ☐ Sonstiges Land innerhalb der EU oder des EWR:
     - Frankreich

4. **Ort des Daten*zugriffs*** durch den Auftragnehmer oder einen Unterauftragsverarbeiter (Mehrauswahl möglich)

   - ☐ Aus der Bundesrepublik Deutschland heraus
   - ☐ Aus einem sonstigen Land innerhalb der EU oder des EWR heraus:

     Frankreich

5. **Kategorien von Betroffenen**

   - ☐ Mitarbeiter des Auftraggebers
   - ☐ Minderjährige Personen

6. **Kategorien von Auftraggeber-Daten**

   Die nachfolgend genannten Kategorien umfassen alle Datenkategorien, die in der Software verarbeitet werden können. Der konkrete Umfang richtet sich jedoch nach den vom Auftraggeber genutzten Funktionen gemäß des Hauptvertrags und der zugehörigen Leistungsvereinbarungen (siehe Ziff. 2. dieser **Anlage 1**) und kann daher weniger als die nachfolgend genannten Datenkategorien beinhalten. Mögliche verarbeitet Kategorien von Auftraggeber-Daten sind:

- **Personenstammdaten**, d.h. personenbezogene Daten eines Betroffenen, die nicht Vertragsstammdaten, demnach nicht vertragsbezogen sind, und auch keine Nutzerdaten sind (Nutzeraccount) hier
  - **Mitarbeiter des Auftraggebers, die nicht selbst Nutzer sind**
    - Name,
    - Vorname
    - Dienstliche E-Mail-Adresse
    - Unterschrift
  - **Schüler**
    - Vorname
    - Nachname
    - Weitere u.a. bei Umfragen erhobene, vom Auftraggeber vorgegebene personenbezogene Daten
- **„User generated content“,** d.h. Inhalte (Dokumente, Äußerungen etc.), die Betroffene willentlich und wissentlich selbst erzeugt haben

## 7. Weisungsberechtigte und Vertreter

| **Auftraggeber** | |
|---|---|
| Weisungsberechtigte/r | Name:<br>Vorname:<br>Bezeichnung:<br>E-Mail: |
| Stellvertreter/in | Name:<br>Vorname:<br>Bezeichnung:<br>E-Mail: |
| **Auftragnehmer** | |
| Empfangsberechtigte/r | Name: Baalmann<br>Vorname: Jannis<br>Bezeichnung: CTO |
| Stellvertreter/in | Name:<br>Vorname:<br>Bezeichnung:<br>E-Mail: |

Weiteres ergibt sich aus der Leistungsbeschreibung des Hauptvertrags und den hierauf basierenden Leistungsvereinbarungen.

**Anlage 2:**

**Technische und organisatorische Maßnahmen (TOM)**

**i.S.d. Art. 32 DSGVO**

Gemäß Art. 32 DS-GVO sind geeignete technische und organisatorische Maßnahmen, unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen, seitens des Verantwortlichen und der Auftragsverarbeiter zu treffen.

Der Auftragnehmer als Auftragsverarbeiter wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien, geeignet sind.

Zur Erfüllung der gesetzlichen Anforderungen sind in Art. 32 DS-GVO verschiedene Anforderungen/Kontrollen definiert. Der Auftragnehmer sowie seine Unterauftragnehmer (**Anlage 3**) setzen die Anforderungen in ihrem jeweiligen Einflussbereich (Kennzeichnung in Klammern) in Bezug auf diese Vereinbarung wie folgt um:

## 1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. b DSGVO

### 1.1. Zutrittskontrolle

*Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.*

Es existieren folgende Maßnahmen zur Zutrittskontrolle:

- ☐ **Technische Maßnahmen**
  - Automatisches Zugangskontrollsystem (UA Petabite)
  - Chipkarten / Transpondersysteme (UA Petabite)
  - Manuelles Schließsystem (Auftragnehmer, UA Petabite)
  - Schließsystem mit Codesperre (UA Petabite)
  - Türen mit Knauf Außenseite (Auftragnehmer, UA Petabite)
  - Videoüberwachung der Eingänge (UA Petabite)
- ☐ **Organisatorische Maßnahmen**
  - Schlüsselregelung / Liste (Auftragnehmer, UA Petabite)
  - Empfang / Rezeption / Pförtner (UA Petabite)
  - Besucherbuch (UA Petabite)
  - Mitarbeiter-/Besucherausweise (UA Petabite)
  - Auswahl von Infrastructure-as-a-Service-Providern mit ISO 27001 Konformität (UA Petabite)

## 1.2. Zugangskontrolle

*Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.*

*Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten" Passworts).*

Es existieren folgende Maßnahmen zur Zugangskontrolle:

- **Technische Maßnahmen**
  - Login mit Benutzername + Passwort (Auftragnehmer, UA Petabite)
  - Login mit biometrischen Daten (Auftragnehmer, UA Petabite)
  - Anti-Viren-Software Server (UA Petabite)
  - Anti-Virus-Software Clients (UA Petabite)
  - Firewall (UA Petabite)
  - Einsatz VPN bei Remote-Zugriffen (UA Petabite)
  - Verschlüsselung von Datenträgern (UA Petabite)
  - Automatische Desktopsperre (UA Petabite)
  - Verschlüsselung von Notebooks / Tablet (UA Petabite)
- **Organisatorische Maßnahmen**
  - Verwalten von Benutzerberechtigungen (Auftragnehmer)
  - Zentrale Passwortvergabe (UA Petabite)
  - Richtlinie „Sicheres Passwort" (Auftragnehmer, UA Petabite)
  - Allg. Richtlinie Datenschutz und / oder Sicherheit (Auftragnehmer, UA Petabite)
  - Auswahl von Infrastructure-as-a-Service-Providern mit ISO 27001 Konformität (UA Petabite)

Die Plattform selbst (gemäß Anlage 1 Ziff.1., bereitgestellt durch den Auftragnehmer) verfügt, sofern vom Auftraggeber aktiviert, als technische Maßnahme über

- 2-Faktor-Authentifizierung für Nutzer der Plattform

Details zu dieser Maßnahme und weiteren Merkmalen sind der Leistungsbeschreibung zur Plattform zu entnehmen.

## 1.3. Zugriffskontrolle

*Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.*

Es existieren folgende Maßnahmen zur Zugriffskontrolle:

- **Technische Maßnahmen**
  - Physische Löschung von Datenträgern (UA Petabite)
- **Organisatorische Maßnahmen**
  - Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte) mit minimaler Anzahl an Administratoren (Auftragnehmer, UA Petabite)
  - Verwaltung Benutzerrechte durch Administratoren (UA Petabite)

### 1.4. Trennungskontrolle

*Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.*

Es existieren folgende Maßnahmen zur Trennungskontrolle:

- **Technische Maßnahmen**
  - Trennung von Produktiv- und Testumgebung (Auftragnehmer, UA Petabite)
  - Mandantenfähigkeit relevanter Anwendungen (Auftragnehmer, UA Petabite)
- **Organisatorische Maßnahmen**
  - Steuerung über Berechtigungskonzept (UA Petabite)
  - Festlegung von Datenbankrechten (Auftragnehmer, UA Petabite)

### 1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

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

Es existieren folgende Maßnahmen zur Pseudonymisierung:

- **Technische Maßnahmen**
  - Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesichertem System (mögl. verschlüsselt) (UA Petabite)
- **Technische Maßnahmen**
  - Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren (Auftragnehmer, UA Petabite)

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

### 2.1. Weitergabekontrolle

*Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.*

Es existieren folgende Maßnahmen zur Weitergabekontrolle:

- **Technische Maßnahmen**
  - Bereitstellung über verschlüsselte Verbindungen wie sftp, https (Auftragnehmer, UA Petabite)
  - E-Mail-Verschlüsselung (S/MIME / PGP) (UA Petabite)
  - E-Mail-Signatur (S/MIME / PGP) (UA Petabite)
  - Einsatz von VPN (UA Petabite)
- **Organisatorische Maßnahmen**
  - Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen (Auftragnehmer, UA Petabite)
  - Weitergabe in anonymisierter oder pseudonymisierter Form (UA Petabite)

### 2.2. Eingabekontrolle

*Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.*

Es existieren folgende Maßnahmen zur Eingabekontrolle:

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) (UA Petabite)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts (Auftragnehmer, UA Petabite)
- Klare Zuständigkeiten für Löschungen (Auftragnehmer, UA Petabite)

## 3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

### 3.1. Verfügbarkeitskontrolle

*Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.*

Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle:

- **Technische Maßnahmen**
  - Feuer- und Rauchmeldeanlagen (UA Petabite)
  - Serverraum klimatisiert (UA Petabite)
  - USV (UA Petabite)
- **Organisatorische Maßnahmen**
  - Backup & Recovery-Konzept (ausformuliert) (Auftragnehmer, UA Petabite)
  - Kontrolle des Sicherungsvorgangs (Auftragnehmer, UA Petabite)
  - Getrennte Partitionen für Betriebssysteme und Daten (UA Petabite)

- Auswahl von sicheren Infrastructure-as-a-Service-Providern (ISO 27001-Konformität, Feuer- und Rauchmeldeanlagen, Feuerlöscher im Serverraum, Serverraum klimatisiert, USV) (UA Petabite)
- Vorgaben zur Konfiguration und Strukturierung gemieteter Infrastruktur (UA Petabite)

## 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

### 4.1. Datenschutz-Management

Es existieren folgende Maßnahmen zum Datenschutz-Management:

☐ **Technische Maßnahmen**

- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet…) (UA Petabite)
- Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12 (UA Petabite)

☐ **Organisatorische Maßnahmen**

- Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet (UA Petabite)
- Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich (Auftragnehmer, UA Petabite)
- Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach. (Auftragnehmer, UA Petabite)
- Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden. (Auftragnehmer, UA Petabite)

### 4.2. Incident-Response-Management

*Unterstützung bei der Reaktion auf Sicherheitsverletzungen*

Es existieren folgende Maßnahmen zum Incident-Response-Management:

☐ **Technische Maßnahmen**

- Einsatz von Firewall und regelmäßige Aktualisierung (UA Petabite)
- Einsatz von Spamfilter und regelmäßige Aktualisierung (UA Petabite)
- Einsatz von Virenscanner und regelmäßige Aktualisierung (Auftragnehmer, UA Petabite))

☐ **Organisatorische Maßnahmen**

- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde) (Auftragnehmer, UA Petabite)
- Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen (Auftragnehmer, UA Petabite)
- Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem (Auftragnehmer, UA Petabite)
- Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen (Auftragnehmer UA Petabite)

### 4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

*Privacy by design / Privacy by default*

Es existieren folgende Maßnahmen zu datenschutzfreundlichen Voreinstellungen:

- ☐ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind (Auftragnehmer, UA Petabite)

### 4.4. Auftragskontrolle (Outsourcing an Dritte)

*Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.*

Es existieren folgende Maßnahmen zur Auftragskontrolle:

- ☐ **Technische Maßnahmen**
  - Nur verschlüsselten Zugänge in alle Drittsysteme (UA Petabite)
- ☐ **Organisatorische Maßnahmen**
  - Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit, u.a. Prüfung der Dokumentation, Mitarbeiter sind zur Verschwiegenheit verpflichtet, Bereitstellung wirksamer Kontrollrechte) (Auftragnehmer, UA Petabite)
  - Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standard-Vertragsklauseln (Auftragnehmer, UA Petabite)
  - schriftliche Weisungen an den Auftragnehmer (Auftragnehmer)
  - Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis (Auftragnehmer)
  - Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer (Auftragnehmer)
  - Regelung zum Einsatz weiterer Subunternehmer (Auftragnehmer, UA Petabite)
  - Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags (Auftragnehmer, UA Petabite)
  - Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus (UA Petabite)

**Anlage 3:**

**Genehmigte Unterauftragnehmer**

| **Firma, Anschrift** | **Art und Zweck der Verarbeitung** | **Art der Daten** | **Kategorien der betroffenen Personen** |
|---|---|---|---|
| Petabite GmbH, Munstermannskamp 1, 21335 Lüneburg | ☐ Speicherung im Rahmen von Hosting-Dienstleistungen<br>☐ Möglicher Zugriff im Rahmen von IT- und IT-Security-Support-Dienstleistungen | ☐ **Personenstammdaten**, d.h. personenbezogene Daten eines Betroffenen, die nicht Vertragsstammdaten, demnach nicht vertragsbezogen sind, hier<br>○ **Mitarbeiter des Auftraggebers (Lehrer)**<br>▪ Name,<br>▪ Vorname<br>▪ Dienstliche E-Mail-Adresse<br>○ **Schüler**<br>▪ Vorname<br>▪ Nachname<br>☐ **Nutzungsdaten**, d.h. Informationen über Art, Umfang, Dauer und Zeitpunkt der Nutzung eines web-basierten Multimedia-Angebots (Webseiten, Videoangebote, etc.)<br>☐ **User-Account-Informationen**, d.h. z.B. Benutzername, Passwort, Rechteprofil, Organisationsinformationen, Rollen etc.<br>☐ **„User generated content“,** d.h. Inhalte (Dokumente, Äußerungen etc.), die Betroffene willentlich und wissentlich selbst erzeugt haben | ☐ Mitarbeiter des Auftraggebers<br>☐ Minderjährige Personen |