

## Standardvertragsklauseln

Für die Zwecke von Artikel 28 Absatz 3 der Verordnung 2016/679 (DSGVO)

Zwischen

[NAME]  
Ust-IdNr: [CVR-NO]  
[ANSCHRIFT]  
"[POSTLEITZAHL UND STADT]"  
[LAND]

(die Datenverantwortliche)

und

FrontRead - Institut für Lesen und Lernen GmbH  
Ust-IdNr: DE 302510031  
Friedrich-Ebert-Damm 111  
22047 Hamburg  
Deutschland

(der Auftragsverarbeiter)

jeweils eine „Partei“; zusammen „die Parteien“

HABEN die folgenden Vertragsklauseln (die Klauseln) VEREINBART, um die Anforderungen der DSGVO zu erfüllen und den Schutz der Rechte der betroffenen Person zu gewährleisten.

**Inhalt**

1. Präambel.....	2
2. Die Rechte und Pflichten der Datenverantwortlichen.....	3
3. Der Auftragsverarbeiter handelt weisungsgemäß .....	3
4. Vertraulichkeit.....	3
5. Sicherheit der Verarbeitung .....	4
6. Einsatz von Unterauftragsverarbeitenden .....	5
7. Übermittlung von Daten in Drittländer oder an internationale Organisationen	6
8. Unterstützung der Datenverantwortlichen .....	7
9. Meldung von Verletzungen des Schutzes personenbezogener Daten .....	8
10. Löschung und Rückgabe von Daten.....	9
11. Prüfung und Inspektion .....	9
12. Die Absprache der Parteien über sonstige Bedingungen .....	9
13. Beginn und Kündigung .....	9
14. Kontaktpersonen/Kontaktstellen für die Datenverantwortliche und den Auftragsverarbeiter.....	10
Anlage A Informationen über die Verarbeitung.....	12
Anlage B Genehmigte Unterauftragsverarbeitende.....	13
Anlage C Anweisung hinsichtlich der Verwendung von personenbezogenen Daten.....	14

1. In diesen Vertragsklauseln (den Klauseln) sind die Rechte und Pflichten der Datenverantwortlichen und des Auftragsverarbeiters bei der Verarbeitung personenbezogener Daten im Auftrag der Datenverantwortlichen niedergelegt.
2. Die Klauseln sollen sicherstellen, dass die Parteien Artikel 28 Absatz 3 der Verordnung 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) einhalten.
3. Im Zusammenhang mit der Erbringung von FrontReads Lesetraining für Grund- und weiterführende Schulen, verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag des Datenverantwortlichen in Übereinstimmung mit den Klauseln.
4. Die Klauseln haben Vorrang vor etwaigen ähnlichen Bestimmungen, die in anderen Vereinbarungen zwischen den Parteien enthalten sind.
5. Vier Unterlagen liegen den Klauseln als Anlage bei und bilden einen festen Bestandteil derselben.
6. Anlage A enthält Einzelheiten über die Verarbeitung von personenbezogenen Daten, einschließlich des Zwecks und der Art der Verarbeitung, der Art von personenbezogenen Daten, der Kategorien von betroffenen Personen und der Dauer der Verarbeitung.
7. Anlage B enthält die Bedingungen der Verantwortlichen für den Einsatz von Unterauftragsverarbeitern seitens des Auftragsverarbeiters sowie eine Liste von durch die Datenverantwortliche zugelassenen Unterauftragsverarbeitenden.
8. Anlage C enthält die Anweisungen der Datenverantwortlichen hinsichtlich der Verarbeitung von personenbezogenen Daten und der vom Auftragsverarbeiter umzusetzenden Mindestsicherheitsmaßnahmen sowie dazu, wie Prüfungen des Auftragsverarbeiters und etwaiger Unterauftragsverarbeitenden durchzuführen sind.
9. Anlage D enthält Bestimmungen für andere Aktivitäten, die von den Klauseln nicht abgedeckt werden.
10. Die Klauseln werden zusammen mit den Anhängen von beiden Parteien in schriftlicher Form, einschließlich auf elektronischem Wege, gespeichert.
11. Die Klauseln befreien den Auftragsverarbeiter nicht von Pflichten, die Auftragsverarbeitenden gemäß der Datenschutz-Grundverordnung (DSGVO) oder anderen Rechtsvorschriften obliegen.

## 2. Die Rechte und Pflichten der Datenverantwortlichen

1. Die Datenverantwortliche trägt die Verantwortung für die Sicherstellung, dass die Verarbeitung personenbezogener Daten im Einklang mit der DSGVO (siehe Artikel 24 DSGVO), den einschlägigen Datenschutzbestimmungen der Union oder Mitgliedstaaten<sup>1</sup> und den Klauseln erfolgt.
2. Die Datenverantwortliche hat das Recht und die Pflicht, Entscheidungen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten zu treffen.
3. Die Datenverantwortliche trägt u. a. die Verantwortung für die Sicherstellung, dass die Verarbeitung personenbezogener Daten, mit der der Auftragsverarbeiter beauftragt wird, auf einer rechtlichen Grundlage erfolgt.

## 3. Der Auftragsverarbeiter handelt weisungsgemäß

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung der Datenverantwortlichen, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist. Derartige Weisungen gehen aus Anlagen A und C hervor. Nachfolgende Weisungen durch die Datenverantwortliche können auch während der Dauer der Verarbeitung personenbezogener Daten erfolgen. Solche Weisungen werden jedoch stets in schriftlicher Form, einschließlich auf elektronischem Wege, in Verbindung mit den Klauseln dokumentiert und gespeichert.
2. Der Auftragsverarbeiter informiert die Datenverantwortlichen unverzüglich, wenn von der Datenverantwortlichen erteilte Weisungen nach Ansicht des Auftragsverarbeiters gegen die DSGVO oder die einschlägigen Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

## 4. Vertraulichkeit

1. Der Auftragsverarbeiter gewährt nur Personen unter der Verantwortung des Auftragsverarbeiters, die sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und nur, wenn dies unbedingt erforderlich ist, Zugang zu personenbezogenen Daten, die im Auftrag der Datenverantwortlichen verarbeitet werden. Die Liste der Personen, denen Zugang gewährt wurde, ist in regelmäßigen Abständen zu überprüfen. Auf der Grundlage dieser Prüfung kann Zugang zu personenbezogenen Daten entzogen werden, wenn dieser Zugang nicht mehr erforderlich ist; diese Personen haben folglich keinen weiteren Zugang zu personenbezogenen Daten.
2. Nach Aufforderung durch die Datenverantwortliche weist der Auftragsverarbeiter nach, dass die betreffenden Personen unter der Verantwortung des Auftragsverarbeiters der oben genannten Verschwiegenheitspflicht unterliegen.

---

<sup>1</sup> Soweit in diesen Klauseln auf „Mitgliedstaaten“ Bezug genommen wird, ist dies als Bezugnahme auf „EWR-Mitgliedstaaten“ zu verstehen.  
Standardvertragsklauseln 2022

1. Gemäß Artikel 32 DSGVO treffen die Datenverantwortliche und der Auftragsverarbeiter 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 des Risikos für die persönlichen Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Die Datenverantwortliche evaluiert die mit der Verarbeitung einhergehenden Risiken für die Rechte und Freiheiten natürlicher Personen und ergreift Maßnahmen zur Minimierung dieser Risiken. Je nach ihrer Relevanz können die Maßnahmen Folgendes einschließen:

- a. die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
  - b. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
  - c. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
  - d. ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
2. Gemäß Artikel 32 DSGVO evaluiert auch der Auftragsverarbeiter – unabhängig von der Datenverantwortlichen – die mit der Verarbeitung einhergehenden Risiken für die Rechte und Freiheiten natürlicher Personen und ergreift Maßnahmen zur Minimierung dieser Risiken. Dazu gibt die Datenverantwortliche dem Auftragsverarbeiter alle Informationen, die zum Erkennen und Evaluieren derartiger Risiken notwendig sind.
  3. Ferner unterstützt der Auftragsverarbeiter die Datenverantwortliche bei der Gewährleistung der Einhaltung der Pflichten der Datenverantwortlichen gemäß Artikel 32 DSGVO, indem er die Datenverantwortliche zusammen mit allen anderen Informationen, die die Datenverantwortliche braucht, um ihre Pflicht gemäß Artikel 32 DSGVO zu erfüllen, u. a. Informationen über die technischen und organisatorischen Maßnahmen gibt, die vom Auftragsverarbeiter gemäß Artikel 32 DSGVO bereits umgesetzt worden sind.

Wenn es später nach dem Dafürhalten der Datenverantwortlichen für die Minimierung der erkannten Risiken erforderlich ist, dass der Auftragsverarbeiter zusätzlich zu den von ihm gemäß Artikel 32 DSGVO bereits ergriffenen weitere Maßnahmen ergreift, spezifiziert die Datenverantwortliche diese zusätzlichen zu ergreifenden Maßnahmen in Anlage C.

1. Zur Inanspruchnahme weiterer Auftragsverarbeitenden (eines/einer Unterauftragsverarbeiters/in) erfüllt der Auftragsverarbeiter die in Artikel 28 Absatz 2 und Absatz 4 DSGVO genannten Anforderungen.
2. Der/die Datenverarbeiter:in darf daher ohne vorherige ausdrückliche schriftliche Zustimmung keine Unterdatenverarbeitenden für die Erfüllung dieser Bestimmungen einsetzen. Ohne besondere schriftliche Genehmigung der Datenverantwortlichen nimmt der Auftragsverarbeiter daher keine weiteren Auftragsverarbeitenden (Unterauftragsverarbeiter:in) für die Erfüllung der Klauseln in Anspruch.
3. Der Auftragsverarbeiter nimmt Unterauftragsverarbeitende nur mit der besonderen vorherigen Genehmigung der Datenverantwortlichen in Anspruch. Der Auftragsverarbeiter muss die besondere Genehmigung mindestens 2 Monaten vor der Inanspruchnahme des/der betreffenden Unterauftragsverarbeiters/in beantragen. Die Liste von bereits von der Datenverantwortlichen genehmigten Unterauftragsverarbeitenden ist in Anlage B zu finden.
4. Wenn der Auftragsverarbeiter einen/eine Unterauftragsverarbeiter: in zur Durchführung spezifischer Verarbeitungsaktivitäten im Auftrag der Datenverantwortlichen in Anspruch nimmt, werden diesem/dieser Unterauftragsverarbeiter: in über einen Vertrag oder einen anderen Rechtsakt gemäß EU- oder Mitgliedstaatsrecht dieselben wie bereits in den Klauseln festgelegten Datenschutzpflichten auferlegt, insbesondere das Gewähren hinreichender Garantien über das Treffen geeigneter technischer und organisatorischer Maßnahmen, sodass die Verarbeitung die Anforderungen der Klauseln und der DSGVO erfüllt.

Der Auftragsverarbeiter trägt daher die Verantwortung, von dem/der Unterauftragsverarbeiter:in zu verlangen, dass dieser/diese zumindest die Pflichten erfüllt, denen der Auftragsverarbeiter gemäß den Klauseln und der DSGVO unterliegt.

5. Auf Anforderung der Datenverantwortlichen wird der Datenverantwortlichen eine Kopie einer derartigen Unterauftragsverarbeitervereinbarung und nachfolgender Änderungen vorgelegt, wodurch die Datenverantwortliche die Gelegenheit erhält zu gewährleisten, dass dem/der Unterauftragsverarbeiter:in dieselben Datenschutzpflichten, wie sie in den Klauseln niedergelegt sind, auferlegt werden. Klauseln im Zusammenhang mit geschäftlichen Themen, die keinen Einfluss auf den gesetzlichen Datenschutzhalt der Unterauftragsverarbeitervereinbarung haben, müssen der Datenverantwortlichen nicht vorgelegt werden.
6. Der Auftragsverarbeiter vereinbart eine Drittbegünstigtenklausel mit dem Unterauftragsverarbeitende, nach der die Datenverantwortliche im Falle des Konkurses des Auftragsverarbeiters ein Drittbegünstigter gemäß der Unterauftragsverarbeitervereinbarung ist und das Recht zur Durchsetzung der Vereinbarung gegen den vom Auftragsverarbeiter in Anspruch genom-

mene Unterauftragsverarbeitende hat, wodurch beispielsweise die Datenverantwortliche in der Lage ist, Unterauftragsverarbeitende zur Löschung oder Rückgabe der personenbezogenen Daten anzuweisen.

7. Wenn der/die Unterauftragsverarbeiter:in seine/ihre Datenschutzpflichten nicht erfüllt, haftet der Auftragsverarbeiter gegenüber der Datenverantwortlichen vollumfänglich für die Erfüllung der Pflichten des Unterauftragsverarbeitenden. Dies lässt die in der DSGVO, insbesondere in Artikeln 79 und 82 DSGVO, vorgesehenen Rechte der betroffenen Personen gegen die Datenverantwortliche und den Auftragsverarbeiter, einschließlich der Unterauftragsverarbeitenden, unberührt.

## **7. Übermittlung von Daten in Drittländer oder an internationale Organisationen**

1. Etwaige Übermittlungen von personenbezogenen Daten durch den Auftragsverarbeiter in Drittländer oder an internationale Organisationen erfolgen nur auf der Grundlage von dokumentierten Weisungen der Datenverantwortlichen und unter Einhaltung von Kapitel V DSGVO.
2. Falls gemäß EU- oder Mitgliedstaatsrecht, das für den Auftragsverarbeiter gilt, Übermittlungen in Drittländer oder an internationale Organisationen erforderlich sind, für deren Durchführung der Auftragsverarbeiter keine Weisung von der Datenverantwortlichen erhalten hat, setzt der Auftragsverarbeiter die Datenverantwortliche vor der Verarbeitung von dieser gesetzlichen Anforderung in Kenntnis, wenn diese Inkenntnissetzung nicht aus wichtigen Gründen des öffentlichen Interesses gemäß diesem Recht untersagt ist.
3. Ohne dokumentierte Weisungen von der Datenverantwortlichen ist dem Auftragsverarbeiter im Rahmen der Klauseln daher Folgendes nicht gestattet:
  - a. Übermitteln personenbezogener Daten an Datenverantwortliche oder Auftragsverarbeitende in einem Drittland oder in einer internationalen Organisation
  - b. Übertragen der Verarbeitung personenbezogener Daten an einen/eine Unterauftragsverarbeiter:in in einem Drittland
  - c. Veranlassen, dass die personenbezogenen Daten von Auftragsverarbeitenden in einem Drittland verarbeitet werden.
4. Die Weisungen der Datenverantwortlichen bezüglich der Übermittlung personenbezogener Daten in ein Drittland, gegebenenfalls einschließlich des Übermittlungs-Tools gemäß Kapitel V DSGVO, auf dem sie beruhen, sind in Anlage C.6 niedergelegt.
5. Die Klauseln dürfen nicht mit Standarddatenschutzklauseln im Sinne von Artikel 46 Absatz 2 Buchstabe c und Buchstabe d DSGVO verwechselt werden und die Parteien können sich nicht auf die Klauseln als ein Übermittlungs-Tool gemäß Kapitel V DSGVO berufen.

1. Angesichts der Art der Verarbeitung unterstützt der Auftragsverarbeiter die Datenverantwortliche nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Person nachzukommen.

Dazu gehört, dass der Auftragsverarbeiter die Datenverantwortliche nach Möglichkeit bei der Einhaltung von Folgendem unterstützt:

- a. dem Recht, unterrichtet zu werden, wenn personenbezogene Daten von der betroffenen Person erhoben werden
  - b. dem Recht, unterrichtet zu werden, wenn personenbezogene Daten nicht bei der betroffenen Person erhoben wurden
  - c. dem Auskunftsrecht der betroffenen Person
  - d. dem Recht auf Berichtigung
  - e. dem Recht auf Löschung („Recht auf Vergessenwerden“)
  - f. dem Recht auf Einschränkung der Verarbeitung
  - g. der Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung
  - h. dem Recht auf Datenübertragbarkeit
  - i. dem Recht auf Widerspruch
  - j. dem Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden
2. Zusätzlich zu der Pflicht des Auftragsverarbeiters, die Datenverantwortliche gemäß Klausel 6.4 zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen die Datenverantwortliche nach Möglichkeit bei der Einhaltung von Folgendem:
    - a. der Pflicht der Datenverantwortlichen, die Aufsichtsbehörde 72 Stunden von der Verletzung des Schutzes personenbezogener Daten unverzüglich und, falls möglich, binnen höchstens 72 Stunden, nachdem ihm die Verletzung bekannt wurde, zu unterrichten, es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen;
    - b. der Pflicht der Datenverantwortlichen, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt;
    - c. der Pflicht der Datenverantwortlichen, eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen (eine Datenschutz-Folgenabschätzung);



- d. der Pflicht der Datenverantwortlichen, vor der Verarbeitung die Datenschutzbehörde zu konsultieren, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern die Datenverantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.
3. Die Parteien legen in Anlage C die geeigneten technischen und organisatorischen Maßnahmen, durch die der Auftragsverarbeiter die Datenverantwortliche zu unterstützen verpflichtet ist, sowie den Gegenstand und Umfang der erforderlichen Unterstützung fest. Dies gilt für die in Klauseln 9.1 und 9.2 vorgesehenen Verpflichtungen.

## **9. Meldung von Verletzungen des Schutzes personenbezogener Daten**

1. Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Auftragsverarbeiter der Datenverantwortlichen die Verletzung des Schutzes personenbezogener Daten unverzüglich, nachdem ihm die Verletzung bekannt wurde.
2. Die Meldung des Auftragsverarbeiters an die Datenverantwortliche erfolgt nach Möglichkeit innerhalb von 12, nachdem dem Auftragsverarbeiter die Verletzung des Schutzes personenbezogener Daten bekannt wurde, damit die Datenverantwortliche ihrer Pflicht nachkommen kann, die zuständige Aufsichtsbehörde von der Verletzung des Schutzes personenbezogener Daten zu unterrichten, siehe Artikel 33 DSGVO.
3. Gemäß Klausel 9 Absatz 2 Buchstabe a unterstützt der Auftragsverarbeiter die Datenverantwortliche dabei, die zuständige Aufsichtsbehörde von der Verletzung des Schutzes personenbezogener Daten zu unterrichten, das heißt, dass der Auftragsverarbeiter die Erlangung der unten aufgeführten Informationen, die gemäß Artikel 33 Absatz 3 DSGVO in der Mitteilung der Datenverantwortlichen an die zuständige Aufsichtsbehörde angegeben werden müssen, unterstützen muss:
  - a. die Art der personenbezogenen Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
  - b. die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
  - c. die von der Datenverantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.
4. In Anlage D legen die Parteien alle Elemente fest, die der Auftragsverarbeiter zur Verfügung stellen muss, wenn er die Datenverantwortliche bei der Meldung einer Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde unterstützt.

1. Nach Beendigung der Verarbeitung personenbezogener Daten ist der/die Datenverarbeiter:in verpflichtet, alle personenbezogenen Daten, die im Auftrag der für die Datenverarbeitung Verantwortlichen verarbeitet wurden, zu löschen und der Datenverantwortlichen zu bescheinigen, dass dies erfolgt ist, es sei denn, das EU-Recht oder das nationale Recht der Mitgliedstaaten schreibt die Speicherung der personenbezogenen Daten vor.
2. Gemäß den folgenden Rechtsvorschriften der EU oder der Mitgliedstaaten, die für den Auftragsverarbeiter gelten, ist die Speicherung personenbezogener Daten nach Abschluss der Erbringung der Verarbeitungsleistungen in Bezug auf personenbezogene Daten vorgeschrieben:
  - a. [...]

Der Auftragsverarbeiter verpflichtet sich, die Daten ausschließlich zu den Zwecken und für die Dauer, die in diesen Rechtsvorschriften vorgesehen sind, und strikt unter den dafür geltenden Bedingungen zu verarbeiten.

## 11. Prüfung und Inspektion

1. Der Auftragsverarbeiter stellt der Datenverantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Artikel 28 und den Klauseln niedergelegten Pflichten zur Verfügung und ermöglicht und trägt zu Überprüfungen – einschließlich Inspektionen – bei, die von der Datenverantwortlichen oder einem anderen von diesen beauftragten Prüfenden durchgeführt werden.
2. Die Verfahren, die für Prüfungen, einschließlich Inspektionen, des Auftragsverarbeiters und Unterauftragsverarbeitenden durch die Datenverantwortliche gelten, sind in den Anhängen C.7. und C.6. genauer angegeben.
3. Der Auftragsverarbeiter muss den Aufsichtsbehörden, die gemäß geltendem Recht Zugang zu den Einrichtungen der Datenverantwortlichen und des Auftragsverarbeiters haben, oder Vertretenden, die im Auftrag dieser Aufsichtsbehörden handeln, gegen Vorlage von entsprechenden Ausweispapieren Zugang zu den physischen Einrichtungen des Auftragsverarbeiters gewähren.

## 12. Die Absprache der Parteien über sonstige Bedingungen

1. Die Parteien können andere Klauseln über die Erbringung der Verarbeitungsleistungen in Bezug auf personenbezogene Daten vereinbaren, in denen z. B. Haftung festgelegt wird, solange diese weder mittelbar noch unmittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Person und den durch die DSGVO gewährten Schutz beschneiden.

## 13. Beginn und Kündigung

1. Die Klauseln sind ab dem Datum der Unterzeichnung durch beide Parteien wirksam.

2. Beide Parteien haben das Recht, die Neuaushandlung der Klauseln zu fordern, wenn Gesetzesänderungen oder Unzweckmäßigkeit der Klauseln Anlass zu einer derartigen Neuaushandlung geben.
3. Die Klauseln gelten während der Dauer der Erbringung der Verarbeitungsleistungen in Bezug auf personenbezogene Daten. Während der Dauer der Erbringung der Verarbeitungsleistungen in Bezug auf personenbezogene Daten können die Klauseln nur gekündigt werden, wenn andere, für die Erbringung von Verarbeitungsleistungen in Bezug auf personenbezogene Daten geltende Klauseln zwischen den Parteien vereinbart worden sind.
4. Wenn die Erbringung von Verarbeitungsleistungen in Bezug auf personenbezogene Daten beendet ist und die personenbezogenen Daten gemäß Klausel 11.1 und Anlage C.4 gelöscht oder der Datenverantwortlichen zurückgegeben worden sind, können die Klauseln von beiden Parteien schriftlich gekündigt werden.
5. Unterschrift

Im Auftrag der Datenverantwortlichen

Name	[NAME]
Position	[POSITION]
Datum	[DATUM]
E-mail	
Unterschrift	[UNTERSCHRIFT]

Im Auftrag des Auftragsverarbeiters

Name	André Mücke
Position	[POSITION]
Datum	[DATUM]
Email	
Unterschrift	[UNTERSCHRIFT]

#### 14. Kontaktpersonen/Kontaktstellen für die Datenverantwortliche und den Auftragsverarbeiter

1. Die Parteien können sich gegenseitig über die folgenden Kontaktpersonen/Kontaktstellen kontaktieren:
2. Die Parteien haben die Pflicht, sich kontinuierlich gegenseitig über Änderungen in Bezug auf Kontaktpersonen/Kontaktstellen zu unterrichten.

Name	[NAME]
Position	[POSITION]
Telefon	[TELEFON]
E-Mail	[E-MAIL]

Name	[NAME]
Position	[POSITION]
Telefon	[TELEFON]
E-Mail	[E-MAIL]

**A.1. Der Zweck der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag der Datenverantwortlichen ist:**

Der Zweck der Verarbeitung personenbezogener Daten durch den/die Datenverarbeiter:in im Auftrag der Stadtverwaltung besteht darin, der für die Datenverarbeitung Verantwortlichen die Nutzung der FrontRead-Plattform zu ermöglichen, die Eigentum des Datenverarbeiters ist und von diesem verwaltet wird, um Informationen über die Schüler:innen und Lehrer:innen der für die Datenverarbeitung Verantwortlichen zu sammeln und zu verarbeiten.

**A.2. Die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag der Datenverantwortlichen bezieht sich hauptsächlich auf (die Art der Verarbeitung):**

Die Verarbeitung personenbezogener Daten durch den/die Datenverarbeiter:in im Auftrag der Stadtverwaltung besteht in erster Linie darin, dass der/die Datenverarbeiter:in der für die Datenverarbeitung Verantwortlichen die FrontRead-Plattform zur Verfügung stellt und dabei personenbezogene Daten über die Schüler:innen und Lehrer:innen der für die Datenverarbeitung Verantwortlichen auf den Servern des Unternehmens speichert.

**A.3. Die Verarbeitung bezieht sich auf die folgenden Arten personenbezogener Daten über betroffene Personen:**

Die Verarbeitung umfasst die folgenden Arten von allgemeinen personenbezogenen Daten:

1. Name
2. Benutzername
3. Rolle (Schüler:innen oder Lehrer:innen)
4. E-Mail-Adresse auf Lehrer:innen

**A.4. Zu der Verarbeitung gehören die folgenden Kategorien von betroffenen Personen:**

- A. Lehrer:innen
- B. Schüler:innen

**A.5. Die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag der Datenverantwortlichen kann erfolgen, wenn die Klauseln wirksam werden. Die Verarbeitung hat die folgende Dauer:**

Die Dauer der Verarbeitung der personenbezogenen Daten durch den Auftragsverarbeiter im Auftrag der Stadtverwaltung ist so lange, wie der Auftragsverarbeiter im Besitz der personenbezogenen Daten ist oder anderweitig personenbezogene Daten für die Stadtverwaltung verarbeitet, je nachdem, was später eintritt.

**B.1. Zugelassene Unterauftragsverarbeitende**

Bei Gültigkeitsbeginn der Klauseln genehmigt die Datenverantwortliche die Auftragsvergabe an die folgenden Unterauftragsverarbeitenden:

NAME	CVR	ANSCHRIFT	BESCHREIBUNG DER VERARBEITUNG
SE Cloud Factory	35393692	Vestergade 4, 6800 Varde, Dänemark	Se Cloud Factory hoster Fron- tReads serverpark

Bei Beginn der Klauseln genehmigt die Datenverantwortliche den Einsatz der oben genannten Unterauftragsverarbeiter für die für diese Partei beschriebene Verarbeitung. Ohne die ausdrückliche schriftliche Genehmigung der Datenverantwortlichen ist der Auftragsverarbeiter nicht berechtigt, einen/eine Unterauftragsverarbeiter:in mit einer von der vereinbarten „verschiedenen“ Verarbeitung oder anderen Unterauftragsverarbeitenden mit der Durchführung der beschriebenen Verarbeitung zu beauftragen.

**B.2. Vorherige Mitteilung für die Genehmigung von Unterauftragsverarbeitenden**

Im Falle eines Wechsels der Unterauftragsnehmenden muss die Gemeinde mindestens 30 Tage im Voraus informiert werden.

## C.1. Der Gegenstand der/Die Anweisung hinsichtlich der Verarbeitung

Die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag der Datenverantwortlichen erfolgt durch den Auftragsverarbeiter, der Folgendes durchführt:

- Wir geben der Lehrkraft Zugang, damit sie sich bei unserem System anmelden kann. Die Lehrkraft erlaubt dann ihren Schüler:innen, sich in das System einzuloggen.

FrontReads Produkt beruht auf der Kenntnis ausgewählter persönlicher Informationen über den Benutzer und den Administrator. Diese Informationen sind nicht sensibel und beschränken sich auf die Kenntnis der personenbezogenen Daten von;

- Benutzername und Passwort
  - a. Dient zur Authentifizierung bei der Anmeldung
- Name
  - b. Wird verwendet, um sie im Verwaltungsmodul zu identifizieren
- Ob die Person ein:e *Schüler:in*, ein *Mitarbeiter* oder ein *Externer* ist
  - c. Wird verwendet, um festzustellen, ob Sie über Verwaltungsrechte im Verwaltungsmodul verfügen sollten.

### C.1.1 Kategorisierung der Behandlung

Die von FrontRead erhobenen und gespeicherten personenbezogenen Daten fallen nicht unter die Definition der "sensiblen" personenbezogenen Daten gemäß Artikel 9 Absatz 1 der DSGVO.

### C.1.2 Relevanz der Behandlung

FrontRead hat den Benutzernamen und den Namen direkt in der Datenbank, und Sie können anhand der Verwaltungsrechte sehen, ob der Benutzer ein:e Schüler:in oder ein:e Mitarbeiter:in ist. Darüber hinaus speichert FrontRead nur Daten, die zeigen, wie weit die Benutzenden in seinem FrontRead-Prozess ist und wie der Fortschritt in diesem Prozess ist.

Nachstehend finden Sie eine Liste der Daten, auf die FrontRead Zugriff hat und die es speichert;

1. Benutzergruppe (manuell von einem Administrator benannt, oft nach der Klassenstufe und dem Klassennamen benannt, z. B. 7. a)
2. Welches Textpaket die Lehrkraft den Schülern:innen gegeben hat (was einen Eindruck davon vermitteln kann, ob sie starke oder schwache Leser sind)
3. Anzahl der Wörter pro Minute, die Nutzende lesen (Lesegeschwindigkeit)
4. Wie viel sich ihre Lesegeschwindigkeit seit Beginn des Programms verbessert hat
5. Wie viele richtige Antworten sie in abgeschlossenen und nicht abgeschlossenen Übungen hatten
6. Wie oft sie die Leseübungen durchlaufen haben

## C.2. Sicherheit der Verarbeitung

Bei dem Sicherheitsniveau muss Folgendes berücksichtigt werden:

C.2.1. Das Sicherheitsniveau muss der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den unterschiedlich wahrscheinlichen und schwerwiegenden Risiken für die Rechte und Freiheiten natürlicher Personen Rechnung tragen.

#### C.2.1.1. **Allgemeine Sicherheitsmaßnahmen**

Der/die Datenverarbeiter:in unterhält ein formelles, gut umgesetztes und professionelles Informationssicherheitsmanagementsystem, das sich auf die gesetzlichen Anforderungen und die gute Praxis der Datenverarbeitung stützt. Der Verarbeiter hat angemessene und den Tatsachen entsprechende interne Richtlinien und Vorschriften zu erstellen und anzuwenden. Darüber hinaus unterhält der Auftragsverarbeiter Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der von ihm zum Schutz der personenbezogenen Daten getroffenen technischen und organisatorischen Maßnahmen.

#### C.2.1.2 **Inputdatenmaterial mit personenbezogenen Daten**

In Übereinstimmung mit den Empfehlungen der Datenschutzbehörde, verarbeitet FrontRead Inputdatenmaterial von autorisierten Funktionen. Wenn Inputdaten anfallen, die nicht mehr für die angegebenen Zwecke verwendet werden, müssen diese Inputdaten gelöscht oder vernichtet werden. Dies geschieht durch eine Softwareentwicklerfunktion. Dabei sorgt die Funktion des Softwareentwicklers gleichzeitig dafür, dass die eingegebenen Daten gemäß den Empfehlungen der Datenschutzbehörde vernichtet werden.

FrontRead verwendet je nach den Benutzenden unterschiedliche personenbezogene Daten und spezifiziert so die Benutzertypen *Lehrer:in* und *Schüler:in* an einer Einrichtung. Für Benutzende, die entweder Lehrkräfte oder Schüler:innen an einer Einrichtung sind, müssen Inputdaten verwendet werden, die den Namen und den Benutzertyp enthalten. Für andere Benutzer:innen ist die Eingabe des Namens und der E-Mail-Adresse des/der Benutzenden erforderlich.

Die Daten, die FrontRead sammelt, sind notwendig, um aufschlussreiche und valide Ergebnisse für den Nutzenden zu generieren. Eingabedaten werden nur von den autorisierten Funktionen von FrontRead verarbeitet, einschließlich der Softwareentwickler- und Supportfunktionen.

#### C.2.1.3 **Outputdatenmaterial mit personenbezogenen Daten**

In Übereinstimmung mit den Empfehlungen der Datenschutzbehörde werden das Outputdatenmaterial von FrontRead nur von Personen genutzt, die mit den Zwecken, für die die Verarbeitung der personenbezogenen Daten erfolgt, befasst sind. Diese Personen haben die Funktionen Softwareentwickler, Vertrieb und Support.

FrontRead verarbeitet Daten in Form der Ergebnisse, die der/die Nutzende durch die Nutzung der Lösung erzielt. FrontRead verwendet Ausgabedaten, um den betreffenden Nutzenden einen Einblick in die von einem/einer bestimmten Nutzer:in erzielten Ergebnisse zu geben.

Outputdaten sind auf dem mit der FrontRead-Plattform verknüpften Verwaltungsmodul "Partner" verfügbar, zu dem alle Nutzer:innen und Administrierende Zugang haben, wenn auch nicht alle gleichberechtigt (siehe Abschnitt "Autorisierung und Zugangskontrolle").



Nur der Bereich Softwareentwicklung und Support von FrontRead hat direkten Zugriff auf alle Outputdaten, die in einer Datenbank gespeichert sind. Die Outputdaten dürfen nicht lokal auf dem Computer eines FrontRead-Mitarbeitenden gespeichert oder protokolliert werden.

Wenn die Daten nicht mehr benötigt werden und für FrontRead nicht mehr relevant sind, werden sie aus der FrontRead-Datenbank gelöscht.

C.2.2. Der/die Datenverarbeiter:in ist dann berechtigt und verpflichtet, über die technischen und organisatorischen Sicherheitsmaßnahmen zu entscheiden, die er ergreift, um das erforderliche (und vereinbarte) Sicherheitsniveau herzustellen.

C.2.3. Der/die Datenverarbeiter:in muss jedoch - in jedem Fall und mindestens - die folgenden mit der Stadtverwaltung vereinbarten Maßnahmen durchführen.

### **Anonymisierung und Verschlüsselung von personenbezogenen Daten**

Der/die Datenverarbeiter:in muss geeignete technische und organisatorische Maßnahmen ergreifen, um die Anonymisierung der personenbezogenen Daten zu gewährleisten, insbesondere wenn die Identifizierung der betroffenen Person(en) nicht mehr erforderlich ist.

Um die oben genannten Anforderungen zu erfüllen, hat der/die Datenverarbeiter:in insbesondere Folgendes umgesetzt:

Gemäß Artikel 5 Absatz 1 Buchstabe e der Datenschutzverordnung verarbeitet FrontRead personenbezogene Daten auf der Grundlage des Prinzips der "Beschränkung der Aufbewahrung".

FrontRead bewahrt personenbezogene Daten auf, bis der für die Datenverantwortlichen den Vertrag mit FrontRead kündigt und/oder wenn die für die Datenverantwortliche FrontRead auffordert, die Daten zu löschen.

Darüber hinaus können die Daten der Lernenden gelöscht werden, wenn der Schüler:in die Schule wechselt und die für die Datenverarbeitung Verantwortliche nicht mehr für die Daten der Lernenden zuständig ist bzw. keine Rechte mehr daran hat. Es liegt in der Verantwortung der für die Datenverarbeitung Verantwortlichen, diese Daten zu löschen.

Die Löschungsroutine muss aktiviert werden, wenn der/die Schüler:in die Schule in der Gemeinde verlässt und/oder in eine Schule in einer anderen Gemeinde wechselt. Wünscht die Gemeinde, dass die Schüler:innendaten gelöscht werden, wenn ein/ eine Schüler:in in eine andere Schule innerhalb der Gemeinde wechselt, so muss dies in einer gesonderten Vereinbarung festgehalten werden.

Der/die Datenverarbeiter:in muss geeignete technische und organisatorische Maßnahmen ergreifen, um sicherzustellen, dass personenbezogene Daten verschlüsselt werden, wenn und soweit dies erforderlich ist, insbesondere auch im Zusammenhang mit der Übermittlung über offene Netze und/oder externe Kommunikationsverbindungen, siehe auch unten unter "Schutz personenbezogener Daten bei der Übermittlung".

Um die oben genannten Anforderungen zu erfüllen, hat der/die Datenverarbeiter:in insbesondere Folgendes umgesetzt:

Der Zugriff auf FrontRead erfolgt über eine Anmeldung im Portal und ist über TSL/SSL verschlüsselt.

Wenn Sie FrontRead für Schüler:in und Lehrer:in verwenden, müssen diese angemeldet sein, um auf die Anwendung und die Daten zugreifen zu können.

### **Sicherung der variierenden Vertraulichkeit, Integrität, Verfügbarkeit und Robustheit des Systems**

Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass bei der Verarbeitung personenbezogener Daten eine angemessene Vertraulichkeit gewahrt bleibt, auch in Bezug auf den Systemzugang und den physischen Zugang zu den Verarbeitungsorten.

Im Hinblick auf die Erfüllung der oben genannten Anforderungen, hat der/die Datenverarbeiter:in insbesondere Folgendes umgesetzt:

In Übereinstimmung mit den Empfehlungen der Datenschutzbehörde legt FrontRead organisatorische Regeln fest, um sicherzustellen, dass sie den oben genannten Empfehlungen und den tatsächlichen Gegebenheiten des Unternehmens entsprechen.

Die organisatorischen Aspekte werden anhand der Rollenverteilung im Unternehmen beschrieben, und die Datenzugriffsrechte der einzelnen Rollen werden erläutert (siehe unten).

<b>Funktion</b>	<b>Adm. Type</b>	<b>Recht</b>
Vorstand	Unter Administrator	Einsicht in alle mit der FrontRead-Plattform verbundenen Benutzenden
Verkauf	Unter Administrator	Einsicht in alle mit der FrontRead-Plattform verbundenen Benutzenden
Kundendienst	Super Administrator	Vollständiger Zugang zu allen gespeicherten personenbezogenen Daten
Entwicklung	Super Administrator	Vollständiger Zugang zu allen gespeicherten personenbezogenen Daten
Marketing	Unter Administrator	Einsicht in alle mit der FrontRead-Plattform verbundenen Benutzenden

*Figur 1*

Durch die in Figur 1 dargestellte Verteilung der Rechte wird die Anzahl der Mitarbeitenden, die unnötigen Zugang zu allen personenbezogenen Daten haben, geregelt. Es wird also festgestellt, dass gemäß der Rechteverteilung in Figur 1 nur relevante und notwendige Rollen vollen Zugriff auf personenbezogene Daten in FrontRead haben.

Der Auftragsverarbeiter ergreift geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass bei der Verarbeitung personenbezogener Daten eine angemessene **Integrität** gewahrt bleibt; dazu gehört auch die Gewährleistung der Zuverlässigkeit und Richtigkeit der personenbezogenen Daten.

Um die oben genannten Anforderungen zu erfüllen, hat der/die Datenverarbeiter:in insbesondere Folgendes umgesetzt:

FrontRead beschränkt den Zugriff auf die persönlichen Daten der Nutzenden auf ein Minimum, diese Aufgabe wird von der Softwareentwicklung- und Supportfunktion übernommen.

FrontRead fungiert als *Super Administrator* und hat dadurch Zugriff auf alle zugänglichen Daten der FrontRead-Plattform. Die Funktion des Super Administrierenden bei FrontRead ist hier auf die Funktionen Softwareentwicklung und Support beschränkt.

Benutzende von FrontRead Produkten haben administrativen Zugriff auf einen vordefinierten Datensatz, der von der Rolle des Benutzenden abhängt. Nachstehend finden Sie eine Übersicht über den skalierten Datenzugriff.

<b>Adm. Thema</b>	<b>Adm. Type</b>	<b>Recht</b>
FrontRead ApS	Super Administrator:in	Vollständiger Zugang zu allen gespeicherten personenbezogenen Daten
Gemeinden	Partner Administrator:in	Einblick in alle mit dem Partner verbundenen Institutionen
Institutionen	Institution Administrator:in	Einblick in alle Teams der Institution
Lehrkraftoder Fachbereitsleiter	Institution Administrator:in	Einblick in alle Teams der Institution
Benutzende und Schüler:innen	User:in	Einblick in eigene Daten

*Figur 2*

Nur FrontRead als *Super Administrator* kann Unteradministratierende anlegen. Dies kann durch eine Vereinbarung zwischen 1) FrontRead und 2) der im Rahmenvertrag benannten Kontaktperson geschehen, woraufhin FrontRead eine benannte Person als Administrator:in einrichtet. Damit wird die von der Datenschutzbehörde empfohlene gesetzliche Anforderung an die *Autorisierung* und *Zugangskontrolle* erfüllt.

In Übereinstimmung mit dem Erlass von der Sicherheit, Kapitel 2, § 10, verarbeitet FrontRead Inputdatenmaterial von autorisierten Funktionen. Werden die eingegebenen Inputdaten nicht mehr für die angegebenen Zwecke verwendet, müssen sie gelöscht oder vernichtet werden. Dies geschieht durch eine Softwareentwicklungsfunktion gemäß der DSGVO, Kapitel 2, § 10, Absatz 2. Auf diese Weise stellt die Funktion der Softwareentwickelnden auch sicher, dass die eingegebenen Daten gemäß Artikel 10 Absatz 3 der DSGVO vernichtet werden.

FrontRead verwendet je nach den Nutzenden unterschiedliche personenbezogene Daten. So werden die Benutzertypen Schüler:in und Lehrer:in angegeben. Für Benutzende, die entweder ein:e Lehrer:in oder ein:e Schüler:in an einer Einrichtung sind, müssen Inputdaten verwendet werden, die den Namen und den Benutzertyp enthalten.

Die Daten, die FrontRead sammelt, sind notwendig, um aufschlussreiche und valide Ergebnisse für alle Nutzenden zu generieren.

Die Inputdaten werden ausschließlich von den autorisierten Funktionen von FrontRead verarbeitet, einschließlich der Softwareentwicklung und Supportfunktionen gemäß der DSGVO, Kapitel 2, Abschnitt 10.

Der/die Datenverarbeiter:in muss geeignete technische und organisatorische Maßnahmen ergreifen, um die ständige Verfügbarkeit der personenbezogenen Daten zu gewährleisten, auch bei physischen und technischen Zwischenfällen (siehe unten "Wiederherstellung der personenbezogenen Daten").

Um die oben genannten Anforderungen zu erfüllen, hat der/die Datenverarbeiter:in insbesondere Folgendes umgesetzt:

### **Wiederherstellung von personenbezogenen Daten**

Der Auftragsverarbeiter ergreift geeignete technische und organisatorische Maßnahmen, um die rechtzeitige Wiederherstellung des Zugangs zu den personenbezogenen Daten bei physischen Vorfällen (Stromausfall, Brand, Überschwemmung, Blitzschlag usw.) und/oder technischen Vorfällen (Systemausfall, DoS usw.) sicherzustellen, einschließlich Notfallplänen, Verfahren usw.

Um die oben genannten Anforderungen zu erfüllen, hat der/die Datenverarbeiter:in insbesondere Folgendes umgesetzt:

FrontRead hat das Server-Hosting an SE Cloud Factory ausgelagert, um eine angemessene Sicherheit gegen physische Zwischenfälle im Zusammenhang mit dem Betrieb des Systems zu gewährleisten.

Darüber hinaus hat FrontRead einen BCP (Business Continuity Plan) entwickelt, in dem beschrieben wird, wie mit kritischen Vorfällen umgegangen werden soll.

Das FrontRead-Backup-Verfahren stellt sicher, dass im Falle eines Absturzes, eines Fehlers oder eines anderen Ereignisses ausreichende Möglichkeiten zur Wiederherstellung der Applikation und der Daten vorhanden sind.

### **Zugang zu personenbezogenen Daten durch das Internet**

Der/die Datenverarbeiter:in muss durch geeignete technische und organisatorische Maßnahmen sicherstellen, dass die personenbezogenen Daten u. a. gegen unbefugten Zugriff und/oder Manipulation geschützt sind, wenn und soweit sie über das Internet abgerufen werden, siehe auch oben unter "Anonymisierung und Verschlüsselung".

Um die oben genannten Anforderungen zu erfüllen, hat der/die Datenverarbeiter:in insbesondere Folgendes umgesetzt:

Der Zugriff auf FrontRead erfolgt über ein direktes Login in das Portal und ist somit durch die von FrontRead implementierte Verschlüsselung und Sicherheit (TSL/SSL) geschützt.

Wenn Sie FrontRead für Schüler:in und Lehrer:in verwenden, müssen diese angemeldet sein, um auf die Anwendung und die Daten zugreifen zu können.

Gemäß Abschnitt 13 der DSGVO werden die Daten von FrontRead ausschließlich von Personen verwendet, die mit den Zwecken befasst sind, für die die personenbezogenen Daten verarbeitet werden. Diese Personen haben die Funktionen der Softwareentwicklung, des Vertriebs und des Supports.

FrontRead verarbeitet Daten in Form von Ergebnissen, die Nutzende durch die Verwendung des Produkts erhalten. FrontRead verwendet Outputdaten, um relevanten Nutzenden einen Einblick in die von einer bestimmten nutzenden Person erzielten Ergebnisse zu geben.

Die Outputdaten sind auf dem mit der FrontRead-Plattform verknüpften Verwaltungsmodul "Partner" verfügbar, zu dem alle Nutzenden und Administrierende Zugang haben, wenn auch nicht alle gleichberechtigt (siehe Abschnitt "Autorisierung und Zugangskontrolle").

Nur die Softwareentwicklung und die Supportfunktionen von FrontRead haben direkten Zugriff auf alle Outputdaten, die in einer Datenbank gespeichert sind.

Wenn die Daten nicht mehr benötigt werden und für FrontRead nicht mehr relevant sind, werden sie aus der FrontRead-Datenbank gelöscht.

### **Schutz personenbezogener Daten bei der Übermittlung**

Der/die Datenverarbeiter:in muss durch geeignete technische und organisatorische Maßnahmen sicherstellen, dass die personenbezogenen Daten bei der Übermittlung verschlüsselt oder anderweitig geschützt werden, u. a. gegen unbefugten Zugriff und/oder Manipulation, siehe auch oben unter "Anonymisierung und Verschlüsselung".

Um die oben genannten Anforderungen zu erfüllen, hat der/die Datenverarbeiter:in insbesondere Folgendes umgesetzt:

Der Zugriff auf FrontRead erfolgt über ein direktes Login in das Portal und ist somit durch die von FrontRead implementierte Verschlüsselung und Sicherheit (TSL/SSL) geschützt.

Wenn Sie FrontRead für Schüler:in und Lehrer:in verwenden, müssen diese angemeldet sein, um auf die Anwendung und die Daten zugreifen zu können.

FrontRead hat für eine erzwungene Verschlüsselung (TSL/SSL) zwischen dem Benutzer und der Applikation durch den Hosting-Anbieter gesorgt.

### **Schutz der personenbezogenen Daten während der Speicherung**

Der/die Datenverarbeiter:in ergreift geeignete technische und organisatorische Maßnahmen, um den Schutz personenbezogener Daten u. a. gegen unbefugten Zugriff und/oder Manipulation zu gewährleisten, solange die Daten bei ihm gespeichert sind.

Um die oben genannten Anforderungen zu erfüllen, hat der/die Datenverarbeiter:in insbesondere Folgendes umgesetzt:

FrontRead legt die Verantwortung für die Verarbeitung und Vernichtung von Eingangs- und Ausgangsdaten und die Nutzung von Computerausrüstung auf der Grundlage der DSGVO, Kapitel 2, § 5 fest.

FrontRead verarbeitet Input- und Outputdatenmaterial in Übereinstimmung mit der DSGVO, Kapitel 2, § 10 und § 13.

Die Inputdaten werden ausschließlich von den autorisierten Funktionen von FrontRead verarbeitet, einschließlich der Softwareentwicklerfunktion und der Supportfunktion gemäß der DSGVO, Kapitel 2, Abschnitt 10 (siehe Abschnitt 3).

Die Outputdaten sind auf dem Verwaltungsmodul Partner verfügbar, das mit der FrontRead-Anwendung (FrontReads-Plattform, Anm. d. Red.) verbunden ist und zu dem alle angeschlossenen Benutzenden und Administrierenden Zugang haben. Allerdings hat nicht jeder den gleichen Zugang (siehe Abschnitt "Berechtigung und Zugangskontrolle").

FrontRead verarbeitet Daten in Form von Ergebnissen, die Nutzende durch die Verwendung des Produkts erzielen. Nur die Softwareentwicklung und der Support von FrontRead haben direkten Zugriff auf alle gespeicherten personenbezogenen Daten, die in einer Datenbank gespeichert sind.

Wenn die Daten nicht mehr benötigt werden und für FrontRead nicht mehr relevant sind, werden sie in der FrontRead-Datenbank gelöscht.

FrontRead nutzt die Computerausrüstung in erster Linie in den Räumlichkeiten des Unternehmens und in zweiter Linie an autorisierten PC-Arbeitsplätzen. Die Sicherheitsmaßnahmen am Standort von FrontRead berücksichtigen gängige Sicherheitspraktiken, einschließlich der Kontrolle der Schließung von Räumlichkeiten und der Verschlüsselung von Passwörtern.

Für den Fall, dass Mitarbeiter mit der Absicht, einen PC-Arbeitsplatz außerhalb der FrontReads-Website einzurichten, werden die Mitarbeitenden eine zu diesem Zweck erstellte Testdatenbank verwenden. Dadurch wird verhindert, dass die eigentliche persönliche Datenbank für unsichere Verbindungen zugänglich ist.

Die Heimarbeit erfolgt immer über einen vom Unternehmen autorisierten Computer, für den der Nutzer niemals entsprechende Passwörter auf anderen Computern erstellt oder speichert. Darüber hinaus müssen die mit dem Heimarbeitsplatz verbundenen Computer stets mit Antivirensoftware gemäß § 8 der DSGVO ausgestattet sein.

### **Physische Sicherung der Räumlichkeiten, in denen personenbezogene Daten verarbeitet werden**

Der/die Datenverarbeiter:in muss geeignete technische und organisatorische Maßnahmen ergreifen, um die physischen Räumlichkeiten, in denen die personenbezogenen Daten verarbeitet werden, unter anderem gegen unbefugten Zugang und/oder Manipulation zu schützen.

Um die oben genannten Anforderungen zu erfüllen, hat der/die Datenverarbeiter:in insbesondere Folgendes umgesetzt:

Am eigenen Standort von FrontRead ist während der Öffnungszeiten immer mindestens ein:e Mitarbeiter:in anwesend. Im umgekehrten Fall werden die Bürotüren verschlossen und die Fenster geschlossen gehalten. Außerhalb der Öffnungszeiten wird das gleiche Schließverfahren durchgeführt.

Um Einbrüche in die Computer von FrontReads zu verhindern, die sich in den Räumlichkeiten von FrontReads befinden, sind alle Computer mit verschlüsselten Passwörtern und Antivirenprogrammen ausgestattet.

### **Nutzung von Heim- und Fernarbeitsplätzen**

Der Auftragsverarbeiter ergreift geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass personenbezogene Daten unter anderem vor unbefugtem Zugriff und/oder Manipulation geschützt sind, wenn auf sie von Heim- und Fernarbeitsplätzen aus zugegriffen wird, und dass eine Verschlüsselung der Kommunikationsverbindungen und eine Authentifizierung der Personen, die von Heim- und Fernarbeitsplätzen aus auf personenbezogene Daten zugreifen, verwendet werden.

Um die oben genannten Anforderungen zu erfüllen, hat der/die Datenverarbeiter:in insbesondere Folgendes umgesetzt:

FrontRead verarbeitet personenbezogene Daten an Heimarbeitsplätzen in Übereinstimmung mit den Empfehlungen der Datenschutzbehörde zu Heimarbeitsplätzen. Diese Verarbeitung findet auf einem PC-Arbeitsplatz statt, der sich physisch außerhalb des Standorts von FrontRead befindet.

Für den Fall, dass Mitarbeitende mit der Absicht, einen PC-Arbeitsplatz außerhalb des FrontReads-Geländes einzurichten, wird der/die Mitarbeiter:in eine zu diesem Zweck erstellte Testdatenbank verwenden. Dadurch wird verhindert, dass die eigentliche persönliche Datenbank für unsichere Verbindungen zugänglich ist.

Die Heimarbeit erfolgt immer über einen vom Unternehmen autorisierten Computer, für den der/die Nutzer:in niemals entsprechende Passwörter auf anderen Computern erstellt oder speichert. Darüber hinaus müssen die zum Home Office gehörenden Computer stets mit einer Antiviren-Software gemäß den gesetzlichen Empfehlungen der Datenschutzbehörde ausgestattet sein.

### **Protokollierung**

Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass jeder Zugriff auf die personenbezogenen Daten so protokolliert wird, dass die Protokolldaten jederzeit verwendet werden können, um einen unbefugten Zugriff auf die personenbezogenen Daten und deren Missbrauch aufzudecken und so weit wie möglich zu verhindern.

Um die oben genannten Anforderungen zu erfüllen, hat der/die Datenverarbeiter:in insbesondere Folgendes umgesetzt:

In Übereinstimmung mit der DSGVO, Kapitel 3, Abschnitt 19, führt FrontRead eine automatische Aufzeichnung (Protokollierung) aller Verwendungen personenbezogener Daten durch.

FrontRead nutzt das Protokoll, um zu überwachen und zu analysieren, welche Elemente der Homepage genutzt werden und wie stark die einzelnen Elemente genutzt werden.

Gemäß der DSGVO, Kapitel 3, Artikel 19 Absatz 4, wird das Protokoll nicht gelöscht, da die darin enthaltenen Daten zu statistischen und wissenschaftlichen Forschungszwecken verarbeitet werden, wobei die Identifikationsdaten zuvor verschlüsselt wurden. FrontRead führt ein mechanisches Protokoll, das sowohl der Benutzenden als auch den Zeitpunkt der Bearbeitung enthält.

Die Protokollierung der Daten der FrontReads-Website erfolgt durch den/die Hosting-Anbieter:in der Website.

Die Protokollierung der persönlichen Daten von FrontReads über die FrontReads-Plattform erfolgt durch den Server der FrontReads-Hosting-Anbietenden.

### **Regelmäßige Prüfung, Bewertung und Evaluierung von Maßnahmen zur Gewährleistung der Sicherheit der Behandlung**

Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen, um eine regelmäßige Prüfung, Bewertung und Evaluierung der Effektivität der Sicherheitsmaßnahmen zu gewährleisten.

Um die oben genannten Anforderungen zu erfüllen, hat der/die Datenverarbeiter:in insbesondere Folgendes umgesetzt:

FrontRead hat Anweisungen für eine jährliche Überprüfung der Verfahren und Richtlinien erstellt und im BCP (Business Continuity Plan) dokumentiert, wie und wann die technische Einrichtung bewertet, getestet und gegebenenfalls aktualisiert wird.

### **C.3. Unterstützung der Datenverantwortlichen**

Insoweit dies im Rahmen des Umfangs und des Ausmaßes der unten angegebenen Unterstützung möglich ist, unterstützt der Auftragsverarbeiter die Datenverantwortliche gemäß Klausel 9.1 und 9.2 durch Umsetzung der folgenden technischen und organisatorischen Maßnahmen:

1. Der/die Datenverarbeiter:in unterstützt die Gemeinde, soweit möglich und unter Berücksichtigung der Art der Verarbeitung, durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung der Verpflichtung der Gemeinde, auf Anfragen zur Ausübung der Rechte der betroffenen Personen gemäß Kapitel III der DSGVO zu antworten.

Dies bedeutet, dass der/die Datenverarbeiter:in die Gemeinde so weit wie möglich dabei unterstützt, dass die Gemeinde die Einhaltung der Vorschriften zu gewährleisten:

- a. Die Informationspflicht bei der Erhebung personenbezogener Daten bei der betroffenen Person.
  - b. Die Informationspflicht, wenn personenbezogene Daten nicht bei der betroffenen Person erhoben wurden.
  - c. Das Recht auf Zugang.
  - d. Das Recht auf Berichtigung.
  - e. Das Recht auf Löschung ("Recht auf Vergessenwerden").
  - f. Das Recht auf Einschränkung der Verarbeitung.
  - g. Die Meldepflicht im Falle der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung.
  - h. Das Recht auf Widerspruch.
  - i. Das Recht, keiner Entscheidung unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung, einschließlich Profiling, beruht.
2. Zusätzlich zu der Verpflichtung der Datenverarbeitenden, die Gemeinde gemäß Ziffer 5.3 zu unterstützen, muss der/die Datenverarbeiter:in unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen die Gemeinde auch unterstützen:
    - a. Die Verpflichtung der Gemeinde, die Verletzung des Schutzes personenbezogener Daten unverzüglich und nach Möglichkeit innerhalb von 72 Stunden nach Kenntnisnahme der zuständigen Aufsichtsbehörde zu melden, es sei denn, die Verletzung des Schutzes personenbezogener Daten stellt wahrscheinlich kein Risiko für die Rechte oder Freiheiten natürlicher Personen dar.
    - b. Die Verpflichtung der Gemeinde, die betroffene Person unverzüglich über eine Verletzung des Schutzes personenbezogener Daten



zu benachrichtigen, wenn die Verletzung wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt

- c. Die Verpflichtung für die Gemeinde, vor der Verarbeitung eine Analyse der Auswirkungen der geplanten Verarbeitungstätigkeiten auf den Schutz personenbezogener Daten durchzuführen (Folgenabschätzung).
  - d. Die Verpflichtung der Gemeinde, vor der Verarbeitung die zuständige Aufsichtsbehörde, die Datenschutzbehörde, zu konsultieren, wenn eine Datenschutz-Folgenabschätzung ergibt, dass die Verarbeitung zu einem hohen Risiko führen würde, wenn der für die Datenverarbeitung Verantwortliche keine Maßnahmen zur Risikominderung trifft.
3. Die Parteien legen in Anhang C die erforderlichen technischen und organisatorischen Maßnahmen fest, mit denen der/die Datenverarbeiter:in die Stadtverwaltung unterstützt, sowie den Umfang und die Reichweite dieser Unterstützung. Dies gilt für die Verpflichtungen aus den Ziffern 8 und 9.

#### **C.4. Dauer der Speicherung/Löschungsverfahren**

Die personenbezogenen Daten werden so lange aufbewahrt, wie der/die Schüler:in in einer Einrichtung im Bereich des für die Datenverarbeitung Verantwortlichen (Grundschulen) eingeschrieben ist; danach müssen sie vom/von der Datenverarbeiter:in gelöscht werden.

Nach Beendigung des Dienstes zur Verarbeitung personenbezogener Daten löscht der/die Datenverarbeiter:in die personenbezogenen Daten entweder gemäß Bestimmung 11.1, es sei denn, die für die Datenverarbeitung Verantwortlichen haben nach Unterzeichnung dieser Bestimmungen seine ursprüngliche Wahl geändert. Solche Änderungen müssen dokumentiert und schriftlich, auch elektronisch, in Verbindung mit den Bestimmungen aufbewahrt werden.

#### **C.5. Verarbeitungsort**

Die Verarbeitung der personenbezogenen Daten gemäß den Klauseln kann ohne die vorherige schriftliche Genehmigung der Datenverantwortlichen nur an den folgenden Orten erfolgen:

Die Verarbeitung personenbezogener Daten, die unter die Bestimmungen fallen, darf nur mit vorheriger schriftlicher Zustimmung des für die Datenverarbeitung Verantwortlichen an anderen als den nachstehend genannten Orten erfolgen:

- FrontRead ApS, Åbogade 15, 8200 Aarhus N, Dänemark
  - Datenverarbeiter
- SE Cloud Factory, Vestergade 4, 6800 Varde, Dänemark
  - Unterdatenverarbeiter von FrontRead

C.5.2. Der Ort der Verarbeitung der von den Bestimmungen erfassten personenbezogenen Daten durch beauftragte Unterdatenverarbeitende zum Zeitpunkt des Inkrafttretens der Bestimmungen ergibt sich aus B.1.1 der Bestimmungen.

C.5.3. Jede Änderung des Ortes der Verarbeitung der unter die Bestimmungen fallenden personenbezogenen Daten durch den/die Datenverarbeiter:in sowie durch die von der Stadtverwaltung von Zeit zu Zeit zugelassene Unterdatenverarbeitende bedarf der vorherigen schriftlichen Zustimmung der Gemeinde.

## **C.6. Weisung zur Übermittlung personenbezogener Daten an Drittländer**

C.6.1. Der/die Datenverarbeiter:in darf die personenbezogenen Daten der Gemeinde nicht in Drittländer übermitteln.

C.6.2. Wenn die Gemeinde in diesem Reglement oder später keine dokumentierte Anweisung für die Übermittlung personenbezogener Daten in ein Drittland gibt, ist der/die Datenverarbeiter:in im Rahmen dieses Reglements nicht berechtigt, solche Übermittlungen vorzunehmen.

## **C.7. Verfahren für die Prüfungen, einschließlich Inspektionen, der vom Auftragsverarbeiter durchgeführten Verarbeitung von personenbezogenen Daten durch die Datenverantwortliche**

Der Auftragsverarbeiter holt jährlich auf eigene Kosten einen branchenweit anerkannten Bestätigungsvermerk eines unabhängigen Dritten über die Einhaltung der DSGVO, der Datenschutzbestimmungen anderer EU-Rechtsvorschriften oder des nationalen Rechts der Mitgliedstaaten und dieser Regeln durch den Auftragsverarbeiter ein. Die Erklärung bezieht sich auf die Verarbeitungstätigkeiten, die der Auftragsverarbeiter für die Gemeinde durchführt.

Der/die Datenverarbeiter:in verwendet den folgenden Standard: Einmal im Jahr erhält FrontRead eine unabhängige Erklärung von Lundgrens Advokater in Dänemark.

Die Erklärung des/der Rechnungsprüfenden ist dem für die Datenverarbeitung Verantwortlichen unverzüglich zur Kenntnisnahme zu übermitteln. Der/die für die Datenverarbeitung Verantwortliche kann den Rahmen und/oder die Methodik der Erklärung anfechten und in solchen Fällen eine neue Erklärung in einem anderen Rahmen und/oder mit einer anderen Methodik verlangen.

Die Erklärung des/der Rechnungsprüfenden wird dem/der für die Datenverarbeitung Verantwortlichen unverzüglich zur Kenntnisnahme zugeleitet. Der/die für die Datenverarbeitung Verantwortliche kann den Umfang und/oder die Methodik der Erklärung anfechten und in solchen Fällen eine neue Erklärung mit einem anderen Umfang und/oder einer anderen Methodik verlangen.

Auf der Grundlage der Ergebnisse der Erklärung ist der/die für die Datenverarbeitung Verantwortliche berechtigt, die Durchführung zusätzlicher Maßnahmen zu verlangen, um die Einhaltung der DSGVO, anderer Datenschutzbestimmungen des EU-Rechts oder des nationalen Rechts der Mitgliedstaaten und dieser Vorschriften sicherzustellen.

Darüber hinaus hat der/die für die Datenverarbeitung Verantwortliche oder die Vertretung des/der für die Datenverarbeitung Verantwortlichen das Recht, die Räumlichkeiten, in denen der/die datenverarbeitende Person personenbezogene Daten verarbeitet, einschließlich der Räumlichkeiten und Systeme, die für die oder

im Zusammenhang mit der Verarbeitung genutzt werden, zu inspizieren, auch physisch. Solche Inspektionen können immer dann durchgeführt werden, wenn der/die für die Datenverarbeitung Verantwortliche dies für notwendig erachtet.

### **C.8. Verfahren für die Prüfungen, einschließlich Inspektionen, der von Unterauftragsverarbeitern durchgeführten Verarbeitung von personenbezogenen Daten**

Wird die Verarbeitung personenbezogener Daten oder Teile davon ausgelagert, so stellt der/die Datenverarbeiter:in sicher, dass die Unterdatenverarbeitenden mindestens auf dem in Abschnitt C.7 beschriebenen Niveau überwacht wird, sofern nichts anderes bestimmt ist.

Der/die für die Datenverarbeitung Verantwortliche kann jederzeit den Nachweis verlangen, dass angemessene Folgemaßnahmen ergriffen wurden.

Auf der Grundlage der Ergebnisse der Erklärungen/Inspektionen ist der/die für die Datenverarbeitung Verantwortliche berechtigt, die Durchführung weiterer Maßnahmen zu verlangen, um die Einhaltung der DSGVO, anderer Datenschutz Erlässe des EU-Rechts oder des nationalen Rechts der Mitgliedstaaten und deren Vorschriften sicherzustellen.