Vereinbarung zur Auftragsverarbeitung

(gemäß Art. 28 DSGVO)

zwischen

_____ Name der Schule _____ Straße und Hausnummer _____ PLZ und Ort	und	Snappet GmbH Altkönigstraße 7 61462 Königstein
(nachfolgend „**Auftraggeber**“ genannt)		(nachfolgend „**Auftragnehmer**“ genannt)

Inhalt

1. Gegenstand und Anwendungsbereich

1.1. **Gegenstand**. Der Auftragnehmer erbringt gegenüber dem Auftraggeber gemäß dem Softwarevertrag über die Nutzung der Snappet Lernplattform (nachfolgend "**Hauptvertrag**") Leistungen im Bereich Software as a Service. Der vorliegende Vertrag zur Auftragsverarbeitung (nachfolgend "**Vertrag**") regelt die Verarbeitung personenbezogener Daten, die der Auftragnehmer im Zusammenhang mit der Durchführung des Hauptvertrages für den Auftraggeber in dessen Auftrag verarbeitet. Die Begriffe „personenbezogene Daten“, „betroffene Person“ (nachfolgend „**Betroffener**“) und „Verarbeitung“ haben in diesem Vertrag die in Art. 4 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, nachfolgend „**DSGVO**“) beschriebene Bedeutung.

1.2. **Inhalt der Auftragsverarbeitung.** Gegenstand, Art und Zweck der Verarbeitung sowie die Art der im Auftrag verarbeiteten personenbezogenen Daten (nachfolgend „**Daten**“) sowie die Kategorien Betroffener sind in ANHANG 1 – EINZELHEITEN ZUR AUFTRAGSVERARBEITUNG geregelt.

1.3. **Anwendungsbereich.** Dieser Vertrag gilt nur, wenn und soweit es sich um personenbezogene Daten handelt, die Verarbeitung im Auftrag erfolgt und der Auftraggeber gemäß Art. 3 und 4 DSGVO mit der Verarbeitung der Daten den Bestimmungen der DSGVO unterliegt.

2. Pflichten des Auftraggebers

2.1. **Datenschutzrechtliche Verantwortlichkeit.** Der Auftraggeber bleibt im Verhältnis zwischen Auftraggeber und Auftragnehmer alleiniger Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Der Auftraggeber ist während der Vertragslaufzeit alleine verantwortlich für die Beurteilung der rechtlichen Zulässigkeit der im Rahmen des Auftragsverhältnisses durchzuführenden Verarbeitung durch den Auftragnehmer im Hinblick auf die Regelungen der DSGVO und anderer Vorschriften über den Datenschutz. Unterstützungspflichten des Auftragnehmers nach diesem Vertrag bleiben unberührt.

2.2. **Weisungen.** Der Auftraggeber wird, soweit erforderlich, im Rahmen des Vertragsgegenstands des Hauptvertrags Weisungen zum Umgang mit den Daten geben, insbesondere im Hinblick auf die Zwecke und wesentliche Mittel der Verarbeitung. Weisungen müssen schriftlich (E-Mail genügt) erfolgen und sind ausschließlich an die im ANHANG 1 – EINZELHEITEN ZUR AUFTRAGSVERARBEITUNG genannten Weisungsempfänger zu richten. Zu Weisungen auf Seiten des Auftraggebers sind ausschließlich die im ANHANG 1 – EINZELHEITEN ZUR AUFTRAGSVERARBEITUNG genannten weisungsbefugten Personen berechtigt. Änderungen bei den Weisungsempfängern und Weisungsbefugten teilen sich die Parteien unverzüglich mit (E-Mail genügt).

2.3. **Pflicht zur Freistellung.** Machen Dritte (einschließlich Betroffene oder Datenschutz-Aufsichtsbehörden) gegenüber dem Auftragnehmer Ansprüche bzw. Rechtsverletzungen geltend, die darauf beruhen, dass der Auftraggeber gegen seine Pflichten aus diesem Vertrag oder seine Pflichten aus der DSGVO verstoßen hat, so gilt Folgendes: Der Auftraggeber wird den Auftragnehmer von diesen Ansprüchen unverzüglich freistellen, den Auftragnehmer bei der Rechtsverteidigung angemessene Unterstützung bieten und den Auftragnehmer von den Kosten der Rechtsverteidigung freistellen. Voraussetzung für diese Freistellungspflicht ist, dass der Auftragnehmer den Auftraggeber über geltend gemachte Ansprüche unverzüglich schriftlich informiert, keine Anerkenntnisse oder gleichkommende Erklärungen abgibt und es dem Auftraggeber ermöglicht, auf Kosten des Auftraggebers - soweit möglich - alle gerichtlichen und außergerichtlichen Verhandlungen über die Ansprüche zu führen.

3. Pflichten des Auftragnehmers

3.1. **Weisungsgebundenheit.** Der Auftragnehmer verarbeitet die Daten nur auf dokumentierte Weisung des Auftraggebers hin, sofern der Auftragnehmer nicht durch das Recht der EU oder der EU-Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist. Im Falle einer solchen Verpflichtung teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Weisungen des Auftraggebers können sich auch auf die Übermittlung personenbezogener Daten in ein Land außerhalb des Europäischen Wirtschaftsraums beziehen, sofern dies durch diesen Vertrag nicht bereits festgelegt ist.

3.2. **Zweckbindung.** Der Auftragnehmer verarbeitet die Daten zu den in ANHANG 1 – EINZELHEITEN ZUR AUFTRAGSVERARBEITUNG genannten Zwecken und nach den Weisungen des Auftraggebers.

3.3. **Hinweispflicht.** Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn eine vom Auftraggeber erteilte Weisung nach Meinung des Auftragnehmers gegen die DSGVO oder gegen andere Datenschutzbestimmungen der EU oder desjenigen Mitgliedstaates verstößt, in dem der Auftragnehmer seinen Sitz hat. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Eine Pflicht zur rechtlichen Prüfung von Weisungen besteht für den Auftragnehmer nicht.

3.4. **Betroffenenrechte**. Machen Betroffene ihre Rechte auf Auskunft (Art. 15 DGSVO), Berichtigung (Art. 16 DSGVO), Löschung (Art. 17 DSGVO), Einschränkung der Verarbeitung (Art. 18 DSVO) oder Datenübertragbarkeit (Art. 20 DSGVO) geltend, erfüllt der Auftraggeber diese eigenständig und eigenverantwortlich. Gleiches gilt im Fall des Widerspruchs (Art. 21 DSGVO) oder Widerrufs von Einwilligungen. Ist dem Auftraggeber die Erfüllung von Betroffenenrechten unmöglich, so unterstützt der Auftragnehmer den Auftraggeber gemäß Ziffer 3.7. Für die Herausgabe und Löschung der Daten bei Vertragsende gilt vorrangig Ziffer 7. Anträge von Betroffenen leitet der Auftragnehmer an den Auftraggeber weiter.

3.5. **Datengeheimnis.** Der Auftragnehmer gewährleistet, dass sich die beim Auftragnehmer zur Verarbeitung der Daten befugte Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

3.6. **Meldepflicht.** Wenn dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten im Sinne des Art. 4 Nr. 12 DSGVO im Rahmen der Auftragsverarbeitung bekannt wird, und die Daten des Auftraggebers hiervon betroffen sind, meldet der Auftragnehmer dies dem Auftraggeber unverzüglich.

3.7. **Unterstützungspflicht.** Der Auftragnehmer wird den Auftraggeber angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen

dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Art. 12 - 23 DSGVO genannten Rechte der Betroffenen nachzukommen. Stellt der Auftragnehmer dem Auftraggeber eine Software bereit, gilt klarstellend: Eine Pflicht des Auftragnehmers die Software so bereitzustellen, dass Betroffenenrechte unter der DSGVO mittels integrierter Funktionen durch den Auftragnehmer selbst erfüllt werden können besteht nicht. Der Auftragnehmer wird unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Auftraggeber zudem bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten (Datensicherheit, Meldepflichten bei Datenpannen, Datenschutzfolgenabschätzung und Konsultation von Datenschutzbehörden) unterstützen.

3.8. **Datensicherheit.** Der Auftragnehmer trifft in seinem Verantwortungsbereich alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen. Für die Festlegung und Zuleitung der ggf. vom Auftraggeber gewünschten Zugangsdaten an Angehörige des Auftraggebers ist ausschließlich der Auftraggeber verantwortlich. Die bei Vertragsbeginn vom Auftragnehmer getroffenen Maßnahmen sind im ANHANG 3 – TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN ZUR DATENSICHERHEIT beschrieben. Der Auftragnehmer ist verpflichtet, diese auf ihre Angemessenheit hin zu prüfen und im Falle von Bedenken, diese dem Auftraggeber unverzüglich mitzuteilen. Der Auftragnehmer ist berechtigt, die Maßnahmen den jeweiligen Anforderungen entsprechend anzupassen, sofern hierdurch das Datenschutzniveau insgesamt nicht abgesenkt wird. Änderungen sind vom Auftragnehmer zu dokumentieren.

3.9. **Anfragen von Aufsichtsbehörden.** Anfragen von Aufsichtsbehörden (Art. 31 DSGVO) in Bezug auf eigenständige Pflichten des Auftragnehmers aus der DSGVO (vgl. Art. 30, 32, 44 ff. Abs. 1 DSGVO) beantwortet der Auftragnehmer eigenständig und informiert den Auftraggeber nur, soweit die Sache unmittelbare rechtliche Auswirkungen auf den Auftraggeber hat.

4. Kontrollrechte des Auftraggebers

4.1. **Kontrollen.** Der Auftraggeber ist in Bezug auf die Daten berechtigt, die Einhaltung

a) der gesetzlichen Vorschriften über den Datenschutz,

b) der Vereinbarungen dieses Vertrages, und

c) der Weisungen des Auftraggebers

beim Auftragnehmer in Benehmen mit dem Auftragnehmer zu kontrollieren. Kontrollen in den Betriebsstätten des Auftragnehmers muss der Auftraggeber rechtzeitig vorher ankündigen. Kontrollen sind zu den üblichen Geschäftszeiten und ohne wesentliche Beeinträchtigung des Geschäftsbetriebs des Auftragnehmers durchzuführen.

4.2. **Nachweis der Einhaltung des Art. 28 DSGVO.** Der Auftragnehmer wird dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung stellen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung hierzu die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

4.3. **Nachweis genereller Maßnahmen**. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann nach Wahl des Auftragnehmers auch erfolgen durch

a) die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO,

b) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO, und

c) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren),

d) eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz, ISO 27001).

Die Verarbeitung von Daten in Privatwohnungen ist gestattet. Auch dort werden die datenschutzrechtlichen Vorschriften eingehalten.

4.4. **Schutzwürdige Interessen des Auftragnehmers.** Soweit durch Kontrollen Betriebs- und Geschäftsgeheimnisse des Auftragnehmers offenbart oder geistiges Eigentum des Auftragnehmers gefährdet werden kann oder die Interessen des Auftragnehmers in ähnlicher Weise beeinträchtigt werden können, hat der Auftraggeber die Kontrollen durch einen

fachkundigen und unabhängigen Dritten vornehmen zu lassen, der sich gegenüber dem Auftragnehmer vorab schriftlich zur Verschwiegenheit verpflichtet.

5. Unter-Auftragsverarbeiter

5.1. **Genehmigungserfordernis**. Der Auftragnehmer darf seinerseits weitere Auftragsverarbeiter (nachfolgend „**Unter-Auftragsverarbeiter**“) nur nach vorheriger schriftlicher Genehmigung des Auftraggebers (E-Mail genügt) einschalten. Die Genehmigung kann sich auf konkrete Unternehmen beziehen (nachfolgend „**Einzel-Genehmigung**“) oder allgemein für eine Gruppe oder Art von Unternehmen erteilt werden (nachfolgend „**General-Genehmigung**“).

5.2. **Erteilte Genehmigungen**. Der Auftraggeber genehmigt hiermit die in ANHANG 2 – GENEHMIGTE UNTER-AUFTRAGSVERARBEITER genannten Unter-Auftragsverarbeiter.

5.3. **Information und Widerspruch bei General-Genehmigungen**. Im Fall einer General-Genehmigung gilt:

a) Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Ersetzung eines bestehenden oder Hinzuziehung eines neuen Unter-Auftragsverarbeiters (Änderung) mit einer angemessenen Vorfrist, in der Regel mindestens vier Wochen. Die Information kann per E-Mail an den in ANHANG 1 – EINZELHEITEN ZUR AUFTRAGSVERARBEITUNG genannten Weisungsberechtigten des Auftraggebers erfolgen.

b) Der Auftraggeber hat das Recht, der Änderung des Unter-Auftragsverarbeiters schriftlich (E-Mail genügt) zu widersprechen. Im Falle eines Widerspruchs steht dem Auftragnehmer das Recht zu, diesen Vertrag und den Hauptvertrag außerordentlich mit Wirkung zum geplanten Inkrafttreten der Änderung außerordentlich zu kündigen (E-Mail genügt). Etwaig vorausbezahlte Vergütungen für den Zeitraum nach Wirksamwerden der Kündigung hat der Auftragnehmer dem Auftraggeber zu erstatten.

5.4. **Vereinbarungen mit Unter-Auftragsverarbeitern.** Der Auftragnehmer wird Unter-Auftragsverarbeitern entsprechende Datenschutzpflichten auferlegen wie sie in diesem Vertrag festgelegt sind.

6. Vergütung

6.1. **Gesonderte Vergütung**. Die Leistungen des Auftragnehmers nach diesem Vertrag sind mit der im Hauptvertrag vereinbarten Vergütung abgegolten, jedoch mit folgenden Ausnahmen:

a) Den durch die Erfüllung der Unterstützungspflichten nach den Ziffern 3.4 und 3.7 verursachten Aufwand hat der Auftraggeber dem Auftragnehmer zu ersetzen.

b) Geht der Inhalt von Weisungen des Auftraggebers über dasjenige hinaus, was der Auftragnehmer dem Auftraggeber gemäß dem Hauptvertrag und dessen Leistungsbeschreibung explizit schuldet, hat der Auftraggeber die entsprechenden Aufwände dem Auftragnehmer gesondert zu vergüten.

c) Durch Kontrollen (insbesondere gemäß Ziffer 4.1) entstehende Aufwände wird der Auftraggeber dem Auftragnehmer erstatten, ausgenommen Aufwände im Rahmen des Nachweises genereller Maßnahmen nach Ziffer 4.3.

Die Vergütungspflicht entfällt wenn und soweit der Aufwand durch eine schuldhafte Pflichtverletzung des Auftragnehmers verursacht wurde.

6.2. **Arbeitszeit und Vorschüsse.** Die Aufwände nach Ziffer 6.1 umfassen neben Fremdkosten (z.B. Reisekosten) auch eine Vergütung der Arbeitszeit des vom Auftragnehmer in Anspruch genommenen Personals. Hierbei gilt ein Stundensatz von € 90,- (netto). Der Auftragnehmer kann bei umfangreicheren Arbeiten einen angemessenen Vorschuss vom Auftraggeber verlangen. Für Aufwände bis zu 5 Stunden pro Kalenderjahr entfällt die gesonderte Vergütung (Inklusivleistung). Der Auftragnehmer wird den Auftraggeber vorab informieren, wenn nach dieser Ziffer zusätzliche Aufwände entstehen.

7. Rückgabe und Löschung der Daten bei Vertragsende

7.1. **Rückgabe.** Der Auftraggeber kann bei Vertragsende die Rückgabe der Daten verlangen. Die Rückgabe der Daten erfolgt, indem der Auftraggeber die Exportfunktion der Software soweit vorhanden nutzt. Die Rückgabe erfolgt dabei in dem von der Exportfunktion vorgegebenen Format. Eine vorherige Herausgabe oder eine Herausgabe in einem anderen Format bedarf

einer gesonderten Vereinbarung und Vergütung.

7.2. **Löschung**. Am Ende der Laufzeit dieses Vertrages wird der Auftragnehmer auf die erste schriftliche Anweisung des Auftraggebers hin die Daten des Auftraggebers von seinen Datenträgern löschen und Unterlagen mit Daten bei sich vernichten (jeweils einschließlich Sicherungskopien), soweit der Auftragnehmer nicht durch das Recht der EU oder des Mitgliedsstaates, in dem er seinen Sitz hat, zur weiteren Speicherung verpflichtet ist. Soweit eine Löschung nur mit unverhältnismäßigem Aufwand möglich ist (z.B. in Archiven) kann eine vorübergehende Sperrung und endgültige Löschung im Rahmen des nächsten Löschturnus erfolgen. Sollte keine schriftliche Anweisung des Auftraggebers zur Löschung vorliegen und keine weitere Verpflichtung zur Speicherung bestehen, so bleiben die Daten 12 Monate nach Vertragsende verfügbar. 10 Monaten nach Vertragsende erhält der Auftraggeber eine Nachricht, dass die Daten nach 2 Monaten gelöscht werden, es sei denn es liegt ein Auftrag des Auftraggebers vor, die Daten darüber hinaus beim Auftragnehmer verfügbar zu halten.

8. Laufzeit

Die Laufzeit dieses Vertrages entspricht der Laufzeit des Hauptvertrages. Das Recht zur Kündigung aus wichtigem Grund bleibt unberührt.

9. Schlussbestimmungen

9.1. **Erklärungen und Mitteilungen**. Sämtliche Erklärungen und Mitteilungen nach diesem Vertrag können an die im ANHANG 1 – EINZELHEITEN ZUR AUFTRAGSVERARBEITUNG genannten Weisungsempfänger bzw. Weisungsberechtigten gerichtet werden und auch in Form von E-Mails erfolgen.

9.2. **Anwendbares Recht.** Auf diesen Vertrag findet ausschließlich deutsches Recht unter Ausschluss des UN Kaufrechts Anwendung.

9.3. **Gerichtsstand.** Ist der Auftraggeber Kaufmann, eine juristische Person des öffentlichen Rechts oder ein öffentlich-rechtliches Sondervermögen, so ist ausschließlicher Gerichtsstand derjenige beim Auftragnehmer. Der Auftragnehmer bleibt berechtigt, am Sitz des Auftraggebers zu klagen.

9.4. **Teilunwirksamkeit.** Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder werden, so wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. Statt der unwirksamen Bestimmung gilt dasjenige, was die Parteien nach dem ursprünglich angestrebten Zweck unter wirtschaftlicher Betrachtungsweise redlicherweise vereinbart hätten. Das Gleiche gilt im Falle einer Vertragslücke.

_____
Ort, Datum

Für den **Auftraggeber**	Für den **Auftragnehmer**
_____	_____
Name	Name
_____	_____
Position / Funktion	Position / Funktion
_____	_____
Unterschrift	Unterschrift

ANHANG 1 – EINZELHEITEN ZUR AUFTRAGSVERARBEITUNG

1. Gegenstand, Art und Zweck der Verarbeitung

Im Einklang mit dem Hauptvertrag über die Nutzung der Snappet Lernplattform nimmt der Auftragnehmer für den Auftraggeber die folgenden Verarbeitungen personenbezogener Daten vor:

STANDARDVERARBEITUNGEN:

1.1 Anlage der Nutzerkonten (Einrichtung)

Der Auftraggeber und die von ihr benannten Lehrkräfte („Koordinatoren“) erhalten Zugriff auf den Einrichtungsbereich der Snappet Lernplattform, die sogenannte „Einrichtung“.

In der Einrichtung kann der Koordinator die Klassen, Schüler (Betroffene) und Lehrkräfte (Betroffene) des Auftraggebers anlegen. Dies ist eine Voraussetzung, damit der Auftraggeber mit der Snappet Lernplattform arbeiten kann.

Der Koordinator ist dabei frei in der Wahl der Bezeichnungen für Klassen, Schüler und Lehrkräfte. Lehrkräfte benötigen eine E-Mail-Adresse, damit sie ihr individuelles Kennwort vertraulich festlegen können. Darüber hinaus kann der Koordinator in der Einrichtung festlegen, ob Lehrkräfte nur auf eine Klasse oder auf alle Klassen des Auftraggebers Zugriff haben.

1.2 Ermittlung und Bereitstellung der Lernergebnisse für den Schüler (Lernprogramm)

Der Auftraggeber und die von ihm gemäß Ziffer 1.1 angelegten Schüler (Betroffene) erhalten Zugriff auf den Bereich zum Bearbeiten von Aufgaben, das sogenannte „Lernprogramm“.

Im Lernprogramm können Schüler die in der Snappet Lernplattform enthaltenen Aufgaben bearbeiten. Snappet erfasst, welche Aufgaben der Schüler bearbeitet hat, was seine Antworten waren und welche Ergebnisse er dabei erzielt hat. Die Ergebnisse werden systematisch zusammengestellt, sodass ein Einblick in die Leistung des Schülers ermöglicht wird. Diese Daten bieten dem Schüler einen Einblick in seinen Lernstand bezogen den jeweils relevanten Lehrplan.

1.3 Bereitstellung der Lernergebnisse von Schülern für die Lehrkräfte (Unterrichtsplaner)

Der Auftraggeber und die von ihm gemäß Ziffer 1.1 angelegten Lehrkräfte erhalten Zugriff auf den Auswertungsteil der Snappet Lernplattform, den sogenannten „Unterrichtsplaner“.

Im Unterrichtsplaner können die Lehrkräfte sehen, an welchen Lernzielen und Fachgebiete die einzelnen Schüler arbeiten, welche Aufgaben die einzelnen Schüler bearbeitet haben, was ihre Antworten waren und mit welchem Ergebnis die Schüler diese Aufgaben bearbeitet haben.

Darüber hinaus können die Lehrkräfte für die Klassen einzelne Fachgebiete, die von der Klasse zu bearbeitende Aufgaben enthalten, aktivieren und deaktivieren. Daneben können Lehrkräfte das Lernmaterial anpassen und gezielt bereitstellen (u.a. indem Aufgaben für einzelne oder alle Schüler sichtbar gemacht werden). Lehrkräfte können für einzelne Schüler bestimmte Funktionen ein- oder ausschalten, zum Beispiel die „Vorlesefunktion“.

1.4 Anlage einer Sicherheitskopie (Back-Up)

Die personenbezogenen Daten, die vom Auftragnehmer verarbeitet werden, werden über ein Back-Up gesichert. Fällt einer der Server des Auftragnehmers aus, besteht die Möglichkeit, nach einer Neuinstallation, die Snappet Lernplattform weiter zu nutzen, ohne dass die Lernergebnisse verloren gehen.

OPTIONALE VERARBEITUNGEN:

Die im folgenden genannten Verarbeitungen können durch den Auftraggeber zusätzlich aktiviert werden und bieten dem Auftraggeber umfangreiche zusätzliche Einsichten in die Lernergebnisse der Schüler. Diese zusätzlichen Einsichten stehen jedoch nur dann zur Verfügung, wenn der Auftraggeber die hier genannten Verarbeitungen in der Einrichtung aktiviert oder Snappet durch eine Weisung mit deren Aktivierung beauftragt.

1.5 Erstellung und eigenständige Verwendung von Übersichten über die Ergebnisse, die von Schülern je Aufgabe erzielt wurden, um beispielsweise die Schwierigkeiten der Aufgaben zu ermitteln. Die Übersichten, die keine individuell identifizierbaren Daten enthalten, werden von dem Auftraggeber für die Verwendung von Snappet auf Grundlage dieses Vertrags bereitgestellt.

Der Auftragnehmer erfasst wie unter obiger Ziffer 1.2 beschrieben die Bearbeitungen von Aufgaben durch die Schüler. Die Ergebnisse werden durch Snappet systematisch zusammengestellt. Snappet erstellt aus diesen Ergebnissen regelmäßig eine aggregierte Übersicht aller Antworten je Aufgabe. Diese Übersicht enthält alle bearbeiteten Aufgaben und ob die Aufgaben richtig oder falsch bearbeitet wurde.

1.6 Erstellung und Verwendung von Auswertung hinsichtlich der Lernstände, um beispielsweise an verschiedenen Stellen den Lernstand des Schülers mit einem Perzentilwert einzustufen. Nicht individuell identifizierbare Auswertungen hinsichtlich der Perzentilwerte werden Snappet hierzu von dem Auftraggeber für eine begrenzte unabhängige Verwendung bereitgestellt.

Der Auftragnehmer erfasst wie unter obiger Ziffer 1.2 beschrieben die Bearbeitungen von Aufgaben durch die Schüler. Die Ergebnisse werden durch Snappet systematisch zusammengestellt. Snappet erstellt für den Auftraggeber regelmäßig aus diesen Daten Profile der Schüler, die für jede Kompetenz, jedes Fach und alle Fächer pro Schüler den aktuellen Lernstand zeigt.

Die Daten des Schülers werden dabei mit der Gesamtheit aller Schüler von allen Auftraggebern verglichen, die Snappet nutzen und der hier genannten Verarbeitung zugestimmt haben. (Beispiel: „Schüler A ist in Kompetenz X besser als 52% aller Schüler aus der gleichen Klassenstufe.“) Entsprechend verwendet Snappet umgekehrt die Daten der Schüler des Auftraggebers zur Berechnung der aggregierten Gesamtheit, die allen Auftraggebern, die dieser Verarbeitung zugestimmt haben, für analoge Auswertungen in Schülerprofilen zur Verfügung gestellt werden. Snappet stellt dabei sicher, dass keine Daten von individuellen Schülern identifizierbar sind.

Snappet wird die unter Punkt 1.5 und 1.6 genannten optionalen Verarbeitungen nicht ausführen, ohne dass Snappet eine zuvor erteile Weisung durch den Auftraggeber vorliegt.

WEITERE VERARBEITUNG AUF WEISUNG:

1.7 Weitere Verarbeitungen auf Weisung

Neben den unter obigen Ziffern 1.1 bis 1.6 genannten Verarbeitungen kann der Auftraggeber weitere Verarbeitungen beim Auftragnehmer anfragen. Es gilt Ziffer 6 aus diesem Vertrag.

2. Art der personenbezogenen Daten

2.1. Personenbezogene Daten von Schülern des Auftraggebers

Beschreibung	Datenquelle	Begründung der Verarbeitung
Name (auch Nummern oder Kürzel möglich)	Festlegung durch Auftraggeber (Koordinator in der Einrichtung)	Identifizierung des Schülers durch die Lehrkraft im Rahmen von Auswertungen
Zugehörige Schule, Klassenstufe und Klassenbezeichnung	Festlegung durch Auftraggeber (Koordinator in der Einrichtung)	Zuordnung auf eine Lehrkraft und deren Auswertung in Klassenübersicht
Zugangsdaten mit Benutzername und Kennwort	Festlegung durch Auftraggeber (Lehrkraft im Unterrichtsplaner)	Steuerung des Zugriffs zur Lernplattform
Individuell oder klassenweise zugewiesene Aufgaben	Festlegung durch Auftraggeber (Lehrkraft im Unterrichtsplaner)	Ermöglicht der Lehrkraft eine durch sie gesteuerte und differenzierte Arbeitsweise
Bearbeitete Aufgaben mit Datum und Dauer sowie Inhalt und Ergebnis	Eingabe durch den Schüler (Lernprogramm)	Basis der im System erzeugten Auswertungen für die Lehrkraft und den Schüler
Lernstand als Perzentilwert je Kompetenz und aggregiert für die Fachbereiche (für 1.5/1.6)	Berechnung durch das System (optional)	Basis der im System erzeugten Auswertungen für die Lehrkraft und den Schüler

2.2. Personenbezogene Daten von Lehrkräften des Auftraggebers

Beschreibung	Datenquelle	Begründung der Verarbeitung
Vorname und Name	Festlegung durch Auftraggeber (Koordinator in der Einrichtung)	Identifizierung der Lehrkraft durch den Auftrraggeber und bei Supportleistung durch Auftragnehmer
Zugehörige Schule, Klassenstufe und Klassenbezeichnung	Festlegung durch Auftraggeber (Koordinator in der Einrichtung)	Zuordnung einer Klasse zur Lehrkraft für die Steuerung und Auswertung in Klassenübersicht
Zugangsdaten mit Benutzername und Kennwort	Festlegung durch Auftraggeber (Lehrkraft individuell)	Steuerung des Zugriffs zur Lernplattform
E-Mail-Adresse und Telefonnummer	Festlegung durch Auftraggeber (Koordinator in der Einrichtung)	Kontaktdaten für Support-leistungen durch den Auftragnehmer

3. Kategorien betroffener Personen

- Schüler des Auftraggebers
- Lehrkräfte des Auftraggebers

4. Weisungsempfänger und Weisungsberechtigte

a) Weisungsempfänger beim Auftragnehmer

Weisungsempfänger beim Auftragnehmer Weisungsempfänger beim Auftragnehmer sind die Mitarbeiterinnen und Mitarbeiter der Kundenbetreuung des Auftragnehmers. Weisungen im Sinne dieses Vertrags sind per E-Mail an auftrag@snappet.de zu richten.

b) Weisungsberechtigte beim Auftraggeber

Weisungsberechtigt beim Auftraggeber sind die Schulleitung und alle Personen mit Zugang zur Einrichtung. Weisungsberechtigte Personen des Auftraggebers können durch eine Weisung im Sinne dieses Vertrags weitere weisungsberechtigte Personen benennen.

Weisungen per E-Mail sind nur von E-Mail-Adressen gültig, die vom Auftraggeber über die Einrichtung bei einer weisungsberechtigten Person hinterlegt wurden, oder von der offiziellen E-Mail-Adresse des Auftraggebers oder von einer E-Mail-Adresse die durch eine der vorgenannten durch eine Weisung im Sinne dieses Vertrags genannt wurden.

Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen.

5. Besondere Weisungen / Vereinbarungen

Keine.

ANHANG 2 – GENEHMIGTE UNTER-AUFTRAGSVERARBEITER

1. Einzel-Genehmigungen

Nr.	Firma, Anschrift, Land	Erbrachte Leistungen	Anmerkungen
1	Snappet B.V., Daalseplein 101, 3511 SK Utrecht, Niederlande	Alle in ANHANG 1 genannten Verarbeitungen	Snappet B.V. ist die Muttergesellschaft des Auftragnehmers.
2	Amazon Web Services Europe, Dublin, Irland	Hosting der Snappet Lernplattform	Unter-Auftragsverarbeiter von 1

ANHANG 3 – TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN ZUR DATENSICHERHEIT

Siehe separates Dokument.

Technische und organisatorische Maßnahmen zur Datensicherheit

gemäß Art. 32 DSGVO (als Auftragsverarbeiter)

Inhaltsverzeichnis

1. Gegenstand

Dieses Dokument beschreibt die durch Snappet GmbH getroffenen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten, soweit das Unternehmen als Auftragsverarbeiter handelt.

Snappet verarbeitet personenbezogenen Daten für seine Kunden (nachfolgend „Auftraggeber“) im Einklang mit dem Hauptvertrag über die Nutzung der Snappet Lernplattform (nachfolgend „Snappet-Plattform“). Angaben zu Gegenstand, Art und Zweck der Verarbeitung sind im Anhang 1 des Auftragsverarbeitungsvertrags dargestellt.

Die Verarbeitung im Auftrag erfolgt in erster Linie nicht direkt durch die Snappet GmbH, sondern durch die im Auftragsverarbeitungsvertrag Anhang 2 genannten Unter-Auftragsverarbeiter, insb. durch die zur Snappet Gruppe gehörende Snappet B.V. Nachfolgend werden die Snappet GmbH und die Unter-Auftragsverarbeiter einheitlich mit „Snappet“ bezeichnet.

2. Vertraulichkeit (Art 32 Abs. 1 lit. b) DSGVO)

Nachfolgend sind Maßnahmen dargestellt, die dem Schutz personenbezogener Daten vor unbefugter oder unbeabsichtigter Preisgabe dienen. Dies umfasst Schutz vor externen wie internen Angreifern sowie Schutz vor strukturellen Gefährdungen.

2.1 Zutrittskontrolle

Snappet hat die nachfolgenden Maßnahmen implementiert, um zu verhindern, dass Unbefugte Zutritt zu Systemen erhalten, mit denen personenbezogene Daten verarbeitet werden.

- **Einrichtungen:** Die eingesetzten Netzwerke (Rechenzentren, Server, Netzwerkausrüstungen und Host-Softwaresysteme zur Servicebereitstellung) sind an allen Standorten in unauffälligen Einrichtungen untergebracht.
- **Zutrittskontrollen:** Die Zutrittspunkte zur den Serverstandorten werden sowohl an der Grundstücksgrenze als auch an den Gebäuden mithilfe von elektronischen Zutrittskontrollen gesteuert und sind durch Vorrichtungen zur Einbruchmeldung gesichert, die bei gewaltsamem Öffnen oder Aufhalten der Türen einen Alarm ausgeben.
- **Besucherkontrolle:** Alle Besucher müssen am Empfang gültige Ausweisdokumente vorzeigen und sich eintragen. Sie werden von autorisierten Mitarbeitern begleitet.
- **Videoüberwachung:** Die Sicherheitsbereiche werden per Videokamera (CCTV) überwacht.
- **Sicherheitspersonal:** In den Rechenzentren wird rund um die Uhr geschultes Sicherheitspersonal beschäftigt, das in den und um die Gebäude herum stationiert sind.

2.2 Zugangskontrolle

Snappet hat die nachfolgenden Maßnahmen implementiert, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten benutzt werden können. (siehe auch 2.3)

- **Firewall-Richtlinien:** Firewall-Geräte sind so konfiguriert, dass sie den Zugriff auf die lokal erforderliche Umgebung beschränken und Begrenzungen von Rechenclustern einhalten. Firewall-Richtlinien (Konfigurationsdateien) werden automatisch alle 24 Stunden auf die Firewall-Geräte übertragen.
- **Personalkontrolle:** Der Zugriff auf das Netzwerk wird erst dann aktiviert, wenn von der Personalverwaltung ein aktiver Eintrag im HR-System erstellt wird. Der Systemzugriff wird binnen 24 Stunden nach Deaktivierung des Mitarbeitereintrags im HR-System aufgehoben.

- **Protokollierung von Zugangsdaten:** Jegliches Hinzufügen, Löschen oder Ändern von Nutzer-IDs, Anmeldedaten oder anderen identifizierenden Objekten werden protokolliert.

- **Passwortrichtlinie:** Erstmalige Passwörter werden stets in einer einmaligen Zeichenfolge erstellt und müssen nach der ersten Verwendung sofort geändert werden. Passwörter müssen alle 6 Monate geändert werden. Sie müssen hinreichend komplex sein hinsichtlich Länge, Komplexität und Veränderungsgrad. Es erfolgt eine automatische Sperrung bei mehrfacher falscher Eingabe.

2.3 Zugriffskontrolle

Snappet hat die nachfolgenden Maßnahmen implementiert, um zu sicherzustellen, dass die zur Benutzung von Datenverarbeitungssystemen berechtigten Nutzer nur auf solche Daten zugreifen können, für die sie berechtigt sind, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt kopiert, verändert oder gelöscht werden können.

- **Rollenbasiertes Zugriffsmodell:** Es wird ein rollenbasiertes Zugriffsmodell verwendet. Allen Nutzern wird für alle Systemkomponenten eine eindeutige ID zugewiesen. Es gilt das Prinzip der geringsten Rechte, nach dem den Nutzern lediglich die zur Erfüllung ihrer Aufgaben notwendigen Berechtigungen zur Verfügung gestellt werden.

- **Berechtigungsprüfungen:** Konto- und Zugriffsberechtigungen werden regelmäßig (mindestens alle 6 Monate) von zuständigen Mitarbeitern geprüft. Nutzerrechte werden widerrufen, sobald der Zweck für die Erteilung nicht mehr existiert ist.

- **Server-Admin-Zugriff**: Snappet-Mitarbeiter, die Zugriff auf das Hosting von Snappet per Managementkonsole / CLI / direkt über APIs benötigen, erhalten ein individuelles IAM-Nutzerkonto und benötigen für den Zugriff ein persönliches MFA-Gerät.

- **Root-Konto-Zugriff:** Der Root-Zugriff wird nicht für die tägliche Interaktion verwendet. Er ist auf eine eng begrenzte Gruppe an Mitarbeitern beschränkt, und nur über MFA-Geräte zugänglich.

- **Incident Response Plan (IRP):** Es besteht ein Incident Response Plan (IRP) für den Fall eines missbräuchlichem Zugriff. Er definiert die Verantwortlichkeiten und konkreten Maßnahmen zu allen kritischen Systemkomponenten.

2.4 Trennung

Snappet hat die nachfolgenden Maßnahmen implementiert, um zu sicherzustellen, dass personenbezogene Daten, die für unterschiedliche Auftraggeber oder für unterschiedliche Zwecke erhoben wurden, getrennt verarbeitet werden können.

- **Isolierte Hosting-Umgebung:** Das Hosting erfolgt in einer virtualisierten mandantenfähigen Umgebung, für die Sicherheitsverwaltungsprozesse und Sicherheitskontrollen bestehen. Die Systeme sind so ausgelegt, dass per Filterung über die Virtualisierungs-Software Hosting-Umgebungen der Zugriff auf physische Hosts oder Instanzen verweigert wird, die ihnen nicht zugeordnet sind. Der Hypervisor wird regelmäßig auf Schwachstellen sowie Angriffsvektoren von internen und externen Penetrationsteams geprüft und sorgt für eine robuste Isolierung.

- **Unternehmenssepariерung:** Das Hosting-Netzwerk ist mithilfe von Netzwerksicherheits- und Separierungsgeräten vom restlichen Firmennetzwerk getrennt. Entwickler und Administratoren im Firmennetzwerk, die zwecks Wartung Zugriff benötigen, benötigen eine ausdrückliche Genehmigung. Die Verbindung autorisierter Mitarbeiter zum Netzwerk erfolgt ausschließlich über einen Bastion oder VPN Host, der den Zugriff auf Netzwerkgeräte und

andere Cloud-Komponenten beschränkt und alle Aktivitäten zwecks Sicherheitsprüfung protokolliert. Der Zugriff auf diesen Host erfolgt für alle Benutzerkonten ausschließlich per Authentifizierungsmethode über öffentliche Schlüssel mit SSH.

- **Trennung von Systemen:** Für das Testen der Anwendung stehen Testsysteme zur Verfügung, die vom Produktivsystem getrennt sind. Es werden keine personenbezogenen Daten von Nutzern in Testsystemen eingesetzt. Auch Support-Systeme sind vom Produktivsystem der Auftragsverarbeitung getrennt. Berechtigungen werden auf Anwendungsebene vergeben.

- **Separierung von Inhalten:** Auf der Snappet-Plattform ist der Zugriff auf die Daten von Auftraggebern per rollenbasierter Sicherheit geschützt, sodass auf Daten anderer Auftraggeber nicht zugegriffen werden kann. Auftraggeber werden serverseitig mithilfe kryptographisch signierter Token mit einer ID als Claim identifiziert. So wird sichergestellt, dass Auftraggeber nur ihre eigenen Daten sehen können.

2.5 Verschlüsselung (Art 32 Abs. 1 lit. a) DSGVO)

Snappet hat die nachfolgenden Maßnahmen zur Verschlüsselung von Daten implementiert.

- **Übertragungsschutz:** Snappet verbindet sich via HTTPS mit Netzwerkzugangspunkten, die gegen unbefugtes Abhören, Manipulation und Nachrichtenfälschung schützen sollen. Jeglicher Zugriff auf das Snappet Hosting-Netzwerk wird über ein IPsec VPN (Virtual Private Network) -Gerät gesichert, mit dem ein verschlüsselter Tunnel zwischen der VPC des Hostinganbieters und den Snappet Zugangssystemen hergestellt wird.

- **Verschlüsselung der Netzwerkkommunikation:** Die Kommunikation im Netzwerk erfolgt ausschließlich per Authentifizierungsmethode über öffentliche Schlüssel mit SSH über einen Bastion-Host, der den Zugriff auf Netzwerkgeräte und andere Cloud-Komponenten beschränkt sowie jegliche Aktivitäten zwecks Sicherheitsprüfung protokolliert.

- **Verschlüsselung der Datenübertragung:** Die Datenübertragung zwischen dem Rechenzentrum und Clients/Anwendungen außerhalb des Netzwerks ist per TLS-Verschlüsselung geschützt. Dieser Verschlüsselungstyp wird stets durchgesetzt. Darin eingeschlossen ist der VPN-Zugriff auf Server innerhalb des Rechenzentrums, Client-Anwendungen an Standorten von Snappet sowie in die Snappet-Plattform integrierte externe Services.

- **TLS-Verschlüsselung:** Um zusätzliche Sicherheit zu gewährleisten, werden Anfrageübertragungen nur dann von Snappet akzeptiert, wenn Secure Sockets Layer (SSL) bzw. HTTPS/TLS verwendet wird. Alle Sendungen und Antworten werden mit TLS manipulationssicher verschlüsselt.

- **Festplattenverschlüsselung und Antiviren-Software:** Alle Geräte (z. B. Laptops, PCs) sind mit einer Festplattenverschlüsselung sowie Antivirus-Software ausgestattet, die E-Mail-Filter sowie Malware-Erkennung beinhaltet.

- **Verschlüsselung von Zugangsdaten:** Schlüssel und Geheimnisse für den Zugriff auf Ressourcen der Snappet-Plattform werden standardmäßig verschlüsselt. Die hierzu verwendeten Verschlüsselungs-Codes werden mithilfe des Schlüsselmanagements des Infrastrukturanbieters manipulationssicher gespeichert. Die Benutzerdaten für den Zugriff auf Systeme mit personenbezogenen Daten werden mithilfe von sicheren Hash-Algorithmen gespeichert.

2.6 Pseudonymisierung (Art 32 Abs. 1 lit. a) DSGVO)

Unter Pseudonymisierung versteht man das Ersetzen von Identifikationsmerkmalen wie z.B. eines Namens oder einer E-Mail-Adresse durch eine eindeutige Kennung, dem Pseudonym. Die Identifikationsmerkmale (und die Zuordnung zum Pseudonym) werden getrennt von den Inhaltsdaten aufbewahrt und besonders gesichert. Dadurch kann die Datensicherheit erhöht werden, weil z.B. bei einer unbefugten Offenbarung der Inhaltsdaten keine personenbezogenen Daten offenbart werden.

Snappet hat die nachfolgenden Maßnahmen implementiert, um eine Pseudonymisierung von personenbezogenen Daten zu ermöglichen.

- **Gegenstand, Art und Zweck der Verarbeitung:** Snappet verarbeitet personenbezogenen Daten im Einklang mit dem Hauptvertrag über die Nutzung der Snappet Lernplattform (nachfolgend „Snappet-Plattform“). Genaue Angaben zu Gegenstand, Art und Zweck der Verarbeitung sind im Auftragsverarbeitungsvertrag Anhang 1 dargestellt. Die personenbezogenen Daten beziehen sich auf Lehrer und Schüler des jeweiligen Auftraggebers. Die Daten der Lehrer beschränken sich auf die für den Zugriff auf die Snappet-Plattform erforderlichen Daten. Es gibt daher keine Inhaltsdaten. Die Daten der Schüler sind umfangreicher, da Lernstandprofile erstellt werden.
- **Pseudonymisierung für Daten von Schülern:** Die Identifikation der Schüler in der Snappet-Plattform kann potentiell durch die Daten Name und die zugehörige Schule bzw. Klasse erfolgen. Der Auftraggeber kann diese Daten beliebig festzulegen, beispielsweise kann durch die Verwendung von Nummern anstelle der Namen eine Pseudonymisierung erreicht werden. Die Identifikation ist dann nur durch den Auftraggeber möglich.
- **Aufklärung:** Snappet klärt über diese Option auf, und empfiehlt grundsätzlich eine Pseudonymisierung auf die oben beschriebene Weise. Wenn Snappet Klassen und Schüler voranlegt, wird hierfür eine pseudonymisierte numerische Lösung angewendet.
- **Prinzip der Datensparsamkeit:** Die in der Anwendung verarbeiteten personenbezogenen Daten sind nach dem Prinzip der Datensparsamkeit auf das notwendige Minimum reduziert. Sofern die Verarbeitung anonym erfolgen kann, wird auf den Personenbezug verzichtet.
- **Anonymisierung bei optionaler Verarbeitung:** Snappet setzt eine strikte Separierung von Daten (a) zur Standardverarbeitung und (b) zur optionalen Verarbeitung (siehe Anlage 1 des Auftragsverarbeitungsvertrags) durch. Anonymisierung und Aggregation werden automatisch für jede optionale Datenverarbeitung angewandt.

3. Integrität (Art 32 Abs. 1 lit. b) DSGVO)

Nachfolgend sind Maßnahmen dargestellt, die dazu dienen, personenbezogene Daten vollständig und richtig bereitzustellen. Die Maßnahmen zielen darauf ab, unzulässige Änderungen an den Daten zu erkennen und Verfahren zur Berichtigung vorzuhalten.

3.1 Eingabekontrolle

Snappet hat die nachfolgenden Maßnahmen implementiert, um nachträglich überprüfen und feststellen zu können, welche personenbezogenen Daten zu welcher Zeit und von wem in Verarbeitungssysteme eingegeben, geändert oder entfernt worden sind.

- **Tracking von API-Aufrufen:** API-Aufrufe zur Orchestrierung der Hosting-Umgebung werden mithilfe automatischer Webservice-Cloud-Trails überwacht.

- **Protokollierung und Überwachung prüffähiger Ereigniskategorien:** Prüffähige Ereigniskategorien werden in allen Systemen und Geräten des Hosting-Systems verwendet. Sicherheitsrelevante Ereignisse werden in Prüfprotokollen mit einem Satz Datenelemente („Wann“ (Zeitstempel), „Wo“ (Quelle), „Wer“ (Benutzername), „Was“ (Inhalt)) aufgezeichnet, um die notwendigen Analyseanforderungen zu unterstützen.
- **Nachverfolgbarkeit der Benutzeraktivität:** Entwickler und Administratoren, die zwecks Wartung Zugriff auf Cloud-Komponenten des Hostinganbieters haben müssen, benötigen hierfür spezielle Rechte. Die Authentifizierungsschritte für den Zugang zur Snappet Datenbank und den Managementschnittstellen sind nachverfolgbar.

3.2 Weitergabekontrolle

Snappet hat die nachfolgenden Maßnahmen implementiert, um sicher zu stellen, dass personenbezogenen Daten bei der elektronischen Übertragung oder beim Transport auf Datenträgern nicht unbefugt angezeigt, kopiert, verändert oder gelöscht werden können.

- **Prävention unbefugter Vervielfältigungen:** Die Maßnahmen zur Verhinderung der unerlaubten Vervielfältigung der physischen Speicherstruktur selbst sind in den Abschnitten 2.1 bis 2.5 oben aufgeführt. Zudem ist es verboten, persönliche elektronische Geräte und Wechseldatenträger mit den Informationssystemen des Netzwerks zu verbinden.
- **Vernichtung von Datenträger:** Wenn ein Datenträger das Ende seiner Lebensdauer erreicht hat, wird es mit einem speziellen Verfahren gemäß einheitlichen Richtlinien vernichtet, um einen unbefugten Zugriff auf Daten zu unterbinden. Alle Datenträger werden gemäß den Standardmethoden der Industrie sowie geltenden Datenschutzvorschriften entmagnetisiert und vernichtet.
- **Sichere Zugangspunkte:** Der Hostinganbieter verfügt über eine begrenzte Anzahl an Zugriffspunkten für die Cloud. Der Zugriff auf diese sogenannten API-Endpunkte erfolgt via HTTP (HTTPS), wodurch eine sichere Kommunikation mit Snappet aufgebaut wird.
- **Übertragungsschutz:** Snappet verbindet sich via HTTPS mit diesen Zugangspunkten, die gegen unbefugtes Abhören, Manipulation und Nachrichtenfälschung schützen sollen. Jeglicher Zugriff auf das Snappet Hosting-Netzwerk wird über ein IPsec VPN (Virtual Private Network) -Gerät gesichert, mit dem ein verschlüsselter Tunnel zwischen der VPC des Hostinganbieters und den Snappet Zugangssystemen hergestellt wird.
- **Verbindungen zum Netzwerk durch Mitarbeiter des Hostinganbieters:** Die Verbindung der Mitarbeiter zum Netzwerk erfolgt ausschließlich per Authentifizierungsmethode über öffentliche Schlüssel mit SSH über einen Bastion Host, der den Zugriff auf Netzwerkgeräte und andere Cloud-Komponenten beschränkt.
- **Manipulationsschutz:** Während der elektronischen Übertragung, des Transports oder der Aufzeichnung können ohne Autorisierung durch Snappet keinerlei Daten angezeigt, kopiert, geändert oder gelöscht werden; siehe dazu die Maßnahmen in den Abschnitten 2.2 und 2.3.
- **Endgeräte:** Daten von Auftraggebern sind ausschließlich über die Snappet-Plattform verfügbar und werden nicht auf Endgeräten des Auftraggebers gespeichert.

4. Verfügbarkeit (Art 32 Abs. 1 lit. b) DSGVO)

Nachfolgend sind Maßnahmen dargestellt, die sicherstellen, dass personenbezogene Daten dann zur Verfügung stehen, wenn sie benötigt werden. Dies umfasst auch Maßnahmen zur Wiederherstellung der Daten bei Verlust oder Vernichtung.

4.1 Insbesondere: Wiederherstellbarkeit nach Zwischenfall (Art 32 Abs. 1 lit. c) DSGVO)

Snappet hat die nachfolgenden Maßnahmen implementiert, um die Verfügbarkeit von personenbezogenen Daten nach einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

- **Feuerwarn- und Schutzsysteme:** In allen Rechenzentren sind automatische Feuerwarn- und Schutzsysteme installiert. Dazu wurden Rauchmelder in allen Umgebungen der Rechenzentren sowie Räumen mit mechanischer und elektrischer Infrastruktur, Kälteaggregaten und Generatorausrüstungen installiert.

- **Redundante Stromversorgungen:** Die Stromversorgungen der Rechenzentren sind redundant angelegt und können ohne jegliche Beeinträchtigung des Betriebs rund um die Uhr aufrechterhalten werden. USVs (unterbrechungsfreie Stromversorgungen) dienen als Notstromversorgung bei einem Ausfall der Hauptversorgung für kritische und wichtige Lasten in der Einrichtung. Generatoren stellen in den Rechenzentren Notstromversorgungen für die gesamte Einrichtung bereit.

- **Klima- und Temperatursteuerung:** Mithilfe von Personal und Systemen wird sichergestellt, dass sich Temperatur und Feuchtigkeit innerhalb der zulässigen Toleranzen bewegen.

- **Präventivwartung:** Es wird eine Präventivwartung durchgeführt, um einen kontinuierlichen Betrieb der Ausrüstungen sicherzustellen.

4.2 Insbesondere: Belastbarkeit (Art 32 Abs. 1 lit. b) DSGVO)

Snappet hat die nachfolgenden Maßnahmen implementiert, um datenverarbeitende Systeme widerstandsfähig zu machen, wenn nicht verhinderbare Störungen auf die Systeme einwirken.

- **Mehrere Verfügbarkeitszonen:** Daten werden stets auf mehreren Festplatten auf verschiedenen Servern gespeichert. Sicherungen werden immer in mehreren Verfügbarkeitszonen (Rechenzentren) angelegt. Jede von ihnen ist als unabhängige Ausfallzone konzipiert. Das bedeutet, dass die Verfügbarkeitszonen physisch voneinander getrennt. Alle Verfügbarkeitszonen sind redundant mit mehreren Tier-1-Transitprovidern verbunden.

- **Backup-Strategie für die Snappet-Plattform:** Es werden stündlich/täglich Sicherungen aller Daten durchgeführt. Dies ermöglicht eine einfache Wiederherstellung bei Integritätsproblemen.

- **Prüfung der Notfallpläne:** Die Notfallpläne werden regelmäßig von den Mitgliedern der Geschäftsführung sowie dem Prüfungsausschuss des Vorstandes geprüft.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art 32 Abs. 1 lit. d) DSGVO)

Snappet hat die nachfolgenden Verfahren implementiert zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

- **Rollen und Verantwortlichkeiten:** Der Datenschutzbeauftragte ist benannt. Verantwortliche für Datensicherheit, Auftragskontrolle und aktuelle Dokumentation der Verfahrensschritte sind definiert.

- **Datenschutzkonzept:** Ein Datenschutzkonzept insb. für Auftragsverarbeitung wurde aufgestellt einschließlich Richtlinien zum sicheren Umgang mit personenbezogenen Daten. Darin geregelt werden u.a. die Verantwortlichkeiten und Prozesse
    - zum Abschluss von Verträgen zur Auftragsverarbeitung einschließlich deren Prüfung,
    - bei der Einschaltung von Unter-Auftragsverarbeitern, einschließlich der Kontrolle und Vertragsprüfung,
    - zum Umgang mit Weisungen von Auftraggebern und zur Sicherstellung der Zweckbindung,
    - für den Umgang mit Anträgen von Betroffenen in Bezug auf Betroffenenrechte,
    - für die Führung eines Verzeichnisses der Verarbeitungstätigkeiten (als Auftragsverarbeiter),
    - zur Erkennung und Behandlung von Datenschutzvorfällen (Incident-Response-Management IRP).
- **Vertraulichkeitsverpflichtung:** Die mit personenbezogenen Daten befassten Mitarbeiter haben klar definierte Aufgaben und sind auf das Datengeheimnis verpflichtet.
- **Interne Kommunikation:** Verschiedene Methoden der internen Kommunikation wurden implementiert, um die Mitarbeiter dabei zu unterstützen, ihre Rollen und Zuständigkeiten besser zu verstehen und wichtige Ereignisse zeitnah zu melden. Dazu gehören Orientierungs- und Schulungsprogramme für neue Mitarbeiter sowie regelmäßige Management-Besprechungen in Bezug auf Aktualisierungen der geschäftlichen Performance sowie andere Themen.
- **Datenschutzfreundliche Voreinstellungen** (Art. 25 Abs. 2 DS-GVO)**:** Jede Hardware und Software durchläuft im Rahmen der Investitionsplanung ein Genehmigungsverfahren. Software und Änderungen sind dokumentiert. Die im Hauptvertrag (Anlage 1 Punkt 1) geschilderte optionale Verarbeitung ist als Voreinstellung deaktiviert, und wird nur nach ausdrücklicher Zustimmung des jeweiligen Auftraggebers aktiviert.
- **Compliance-Programme:** Die IT-Infrastruktur des Hostinganbieters wird gemäß den Best Practices in Sachen Sicherheit sowie einer Vielfalt an IT-Sicherheitsstandards konzipiert und verwaltet, darunter: SOC 1 (früher SAS 70), SOC 2, SOC 3 und FedRAMP, PCI DSS Level 1, ISO 27001.