Vereinbarung über die Auftragsdatenverarbeitung
iSd Art 28 DSGVO

(Version vom 19.08.2026)

zwischen

Teachino FlexCo
Schwedenplatz 2/22
1010 Wien
Österreich
(im Folgenden der "**AUFTRAGSVERARBEITER**")

und der

_____
_____
_____
_____
_____

(im Folgenden die "**VERANTWORTLICHE**")

1. Die Vertragsparteien

1.1. Die VERANTWORTLICHE ist Verantwortliche im Sinne des Art. 4. Z. 7 der Datenschutz-Grundverordnung (VO [EU] 2016/679 – "DSGVO") hinsichtlich jeglicher Informationen, die sich auf identifizierte oder identifizierbare natürliche Personen im Sinne des Art. 4. Z. 1 DSGVO ("personenbezogene Daten") beziehen, die an den AUFTRAGSVERARBEITER im Rahmen der unter Punkt 2. genannten zu erbringenden Tätigkeiten überlassen werden.

1.2. Der AUFTRAGSVERARBEITER ist als Auftragsverarbeiter im Sinne des Art. 4. Z. 8 DSGVO für die VERANTWORTLICHE tätig.

2. Gegenstand, Art und Zweck der Verarbeitung

2.1. Der AUFTRAGSVERARBEITER wurde von der VERANTWORTLICHEN mit der Bereitstellung, dem Betrieb und dem Support einer Software zur Vorbereitung, Durchführung und Dokumentation des Unterrichts beauftragt und verarbeitet zu diesem Zweck personenbezogene Daten im Auftrag des VERANTWORTLICHEN.

3. Dauer der Verarbeitung

3.1. Die Verarbeitung erfolgt, solange der AUFTRAGSVERARBEITER personenbezogene Daten im Auftrag der VERANTWORTLICHEN verarbeitet oder solche Daten gespeichert hält. Die Beendigung der zugrunde liegenden Lizenzvereinbarung beendet die Auftragsverarbeitung nicht automatisch.

4. Art und Zweck der Verarbeitung, Kategorien von Betroffenen

4.1. Die gegenständlich vom AUFTRAGSVERARBEITER zu erbringenden Verarbeitungsvorgänge beziehen sich auf die Bereitstellung, den Betrieb und den Support einer Software zur Vorbereitung und Durchführung des Unterrichts.

4.2. Die Art der personenbezogenen Daten, die im Auftrag der VERANTWORTLICHEN verarbeitet werden dürfen, sowie die Kategorien der betroffenen Personen und die Zwecke der Datenverarbeitung sind in **Anlage A** beschrieben.

5. Pflichten des Auftragsverarbeiters

5.1. Der AUFTRAGSVERARBEITER verarbeitet personenbezogene Daten ausschließlich im Rahmen dieser Vereinbarung oder wie von der VERANTWORTLICHEN angewiesen, es sei denn, der AUFTRAGSVERARBEITER ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Er hat sämtliche Handlungen zu unterlassen, die seiner Position als AUFTRAGSVERARBEITER widersprechen. Er hat die sich aus dem anwendbaren Recht ergebenden Pflichten sorgfältig einzuhalten, insbesondere jene aus der DSGVO und dem Datenschutzgesetz idgF.

5.2. Der AUFTRAGSVERARBEITER verpflichtet sich, personenbezogene Daten ausschließlich im Rahmen der dokumentierten Weisungen der VERANTWORTLICHEN zu verwenden und ausschließlich der VERANTWORTLICHEN zurückzugeben oder nur nach deren Weisung an Dritte zu übermitteln. Das Verwenden der personenbezogenen Daten für eigene Zwecke des AUFTRAGSVERARBEITERS bedarf einer vorherigen schriftlichen Genehmigung durch die VERANTWORTLICHE. Ausgenommen hiervon sind Datenverarbeitungen, zu welchen der AUFTRAGSVERARBEITER gesetzlich verpflichtet ist; in einem solchen Fall teilt der AUFTRAGSVERARBEITER der VERANTWORTLICHEN diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Ist der AUFTRAGSVERARBEITER der Ansicht, dass eine Weisung der VERANTWORTLICHEN gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt, so teilt ihr der AUFTRAGSVERARBEITER dies mit. Die VERANTWORTLICHE hat dem AUFTRAGSVERARBEITER anschließend mitzuteilen, ob er an der Weisung festhält. Nachträgliche Weisungen können von der VERANTWORTLICHEN während der gesamten Dauer der Vereinbarung erteilt werden. Diese sind stets schriftlich, auch elektronisch, im Zusammenhang mit dieser Vereinbarung zu dokumentieren und aufzubewahren.

5.3. Der AUFTRAGSVERARBEITER verarbeitet die personenbezogenen Daten nach dem Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO und daher nur soweit, als dies zum Erbringen der unter Punkt 2. genannten Arbeiten erforderlich ist. Darüber hinaus verpflichtet sich der AUFTRAGSVERARBEITER ein nach Art 30 Abs 2 DSGVO erforderliches Verzeichnis von Verarbeitungstätigkeiten zu führen. Dieses Verzeichnis ist der gegenständlichen Vereinbarung über die Auftragsdatenverarbeitung als **Anlage A** angefügt. Ein Löschkonzept ist als **Anlage B** angefügt.

5.4. Der AUFTRAGSVERARBEITER erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten oder potentiell zugriffsberechtigten Personen vor Aufnahme ihrer Tätigkeit zur Wahrung des Datengeheimnisses i.S.d. Art. 28 Abs. 3 lit. b DSGVO, und aller relevanter Datenschutzgesetze verpflichtet hat. Insbesondere bleibt die Verschwiegenheitspflicht der mit der Datenverarbeitung beauftragten Personen auch nach Beenden ihrer Tätigkeit und Ausscheiden beim AUFTRAGSVERARBEITER aufrecht.

5.5. Der AUFTRAGSVERARBEITER trägt für die technischen und organisatorischen Voraussetzungen Vorsorge, sodass die VERANTWORTLICHE die Rechte der Betroffenen, insbesondere die Bestimmungen des Art. 13 und 14 DSGVO (Informationspflicht), Art. 15 DSGVO (Auskunftsrecht), Art. 16 und 17 DSGVO (Recht auf Richtigstellung und Löschung), Art. 18 DSGVO (Recht auf Einschränkung der Verarbeitung), Art. 20 DSGVO (Recht auf

Datenübertragbarkeit) und Art. 21 DSGVO, (Recht auf Widerspruch) gegenüber einer betroffenen Person innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt der VERANTWORTLICHEN alle dafür notwendigen Informationen.

5.6. Der AUFTRAGSVERARBEITER erklärt rechtsverbindlich, einen Datenschutzbeauftragten zu benennen, sofern er dazu nach Art. 37 DSGVO verpflichtet ist. In diesem Fall werden dessen Kontaktdaten der VERANTWORTLICHEN mitgeteilt. Der AUFTRAGSVERARBEITER teilt der VERANTWORTLICHEN auch einen Wechsel des Datenschutzbeauftragten unverzüglich mit.

5.7. Der AUFTRAGSVERARBEITER ist verpflichtet, allfällige Anfragen oder Aufforderungen der zuständigen Datenschutzbehörde ("DSB") oder anderer zuständiger Behörden Folge zu leisten und die internen Verarbeitungsvorgänge entsprechend anzupassen. Die Pflicht besteht unabhängig davon, ob solche Anfragen oder Aufforderungen direkt durch die Behörde erteilt werden oder über die VERANTWORTLICHE an den AUFTRAGSVERARBEITER herangetragen werden. Der AUFTRAGSVERARBEITER wird die VERANTWORTLICHE von derartigen Anfragen oder Aufforderungen der Datenschutzbehörde unverzüglich informieren.

5.8. Im Zusammenhang mit den in diesem Vertrag genannten Arbeiten kooperiert der AUFTRAGSVERARBEITER im größtmöglichen Umfang mit den zuständigen Behörden und der VERANTWORTLICHEN, insbesondere bei der Erstellung des Verzeichnisses der Verarbeitungsvorgänge (Art. 30 DSGVO), bei Datenschutz-Folgeabschätzungen (Art. 35 DSGVO) und vorherigen Konsultationen der Aufsichtsbehörde (Art. 36 DSGVO).

5.9. Die VERANTWORTLICHE wird hinsichtlich der Verarbeitung der überlassenen Daten das Recht der Einsichtnahme und Kontrolle der Datenverarbeitungseinrichtungen eingeräumt. Die VERANTWORTLICHE wird die Einsichtnahme und Kontrolle vorab ankündigen und unter größtmöglicher Schonung des Geschäftsbetriebs des AUFTRAGSVERARBEITERS durchführen. Der AUFTRAGSVERARBEITER verpflichtet sich gemäß Art. 28 Abs 3 lit. h DSGVO, der VERANTWORTLICHEN jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind. Die Parteien stellen der zuständigen Aufsichtsbehörde die Ergebnisse von Prüfungen auf Anfrage zur Verfügung.

6. Sub-Auftragsverarbeiter

6.1. Der AUFTRAGSVERARBEITER ist berechtigt, die im **Anlage C** angeführten Subdienstleister zum Wahrnehmen der vertragsgegenständlichen Aufgaben zu beauftragen. Werden neue Subdienstleister hinzugefügt, muss der AUFTRAGSVERARBEITER den VERANTWORTLICHEN mit einer Vorlaufzeit von 4 Wochen informieren. Spricht der VERANTWORTLICHE innerhalb dieser Frist keinen Widerspruch aus, darf der Subdienstleister beauftragt werden. Jedenfalls hat der AUFTRAGSVERARBEITER sicherzustellen, dass die Heranziehung des Subdienstleisters das Erfüllen der Vorgaben des gegenständlichen Vertrags zu keinem Zeitpunkt gefährdet.

6.2. Sub-Auftragsverarbeiter außerhalb des EWR darf der AUFTRAGSVERARBEITER beauftragen, wenn (i) diese in einem Drittland niedergelassen sind, das über ein von der EU-Kommission mit Beschluss akzeptiertes angemessenes Datenschutzniveau verfügt (Angemessenheitsbeschluss) oder (ii) mit diesen die EU-Standardvertragsklauseln bzw diesen gleichgestellte durch die EU-Kommission erlassene Vertragsschablonen als geeignete Garantien im Sinne des Art. 46 Abs. 2 lit. c und d DSGVO vereinbart wurden.

6.3. In jedem Fall bleibt der AUFTRAGSVERARBEITER der VERANTWORTLICHEN vollumfänglich für die Leistungserbringung durch den hinzugezogenen Sub-Auftragsverarbeiter, ihre Verpflichtungen und das Erfüllen der ihr zugewiesenen Aufgaben verantwortlich. Außerdem muss ein Vertrag zwischen dem AUFTRAGSVERARBEITER und dem Sub-Auftragsverarbeiter gemäß Art. 28 Abs. 4 DSGVO geschlossen werden, in dem sichergestellt ist, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem AUFTRAGSVERARBEITER

aufgrund dieser Vereinbarung obliegen. Weisungen der VERANTWORTLICHEN an Sub-Auftragsverarbeiter werden ausschließlich über den AUFTRAGSVERARBEITER erteilt.

6.4. Kommt der Sub-Auftragsverarbeiter den Verpflichtungen aus der DSGVO nicht nach, so haftet hierfür der AUFTRAGSVERARBEITER gegenüber der VERANTWORTLICHEN.

7. Pflichten der Verantwortlichen

7.1. Die VERANTWORTLICHE verpflichtet sich, den AUFTRAGSVERARBEITER unmittelbar von Änderungen der DSGVO und relevanter Datenschutzgesetze und ergänzender Bestimmungen, die auf die gegenständige Datenverarbeitung anwendbar sind, zu unterrichten. Die VERANTWORTLICHE räumt dem AUFTRAGSVERARBEITER eine angemessene Frist ein, sich organisatorisch, administrativ und technisch auf geänderte Datenschutzbestimmungen und neue Anforderungen einzustellen.

8. Mitteilungen bei Verstößen des Auftragsverarbeiters

8.1. Der AUFTRAGSVERARBEITER erklärt rechtsverbindlich, dass er die VERANTWORTLICHE unverzüglich informiert, wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird bzw wenn Daten aus einer an ihn überlassenen Datenanwendung systematisch und schwerwiegend unrechtmäßig verwendet wurden und den Betroffenen Schaden droht. Diese Meldung hat zumindest folgende Informationen zu enthalten: (a) eine Beschreibung der Art und der Verletzung, (b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden kann, (c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten. Wenn und soweit diese Informationen nicht zur gleichen Zeit bereitgestellt werden können, hat die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen zu enthalten. Weitere Informationen sind anschließend ohne angemessene Verzögerung durch den AUFTRAGSVERARBEITER bereitzustellen, sofern sie verfügbar sind.

8.2. Der AUFTRAGSVERARBEITER trifft technisch und organisatorisch Vorsorge dafür, dass die VERANTWORTLICHE insbesondere die Bestimmungen der Art. 33 und 34 DSGVO ("Data Breach Notification") innerhalb der gesetzlichen Frist erfüllen kann. Der AUFTRAGSVERARBEITER ist in diesem Zusammenhang dazu verpflichtet, der VERANTWORTLICHEN unverzüglich sämtliche Informationen zur Verfügung zu stellen, die diese für eine Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und/oder die betroffene Person benötigt.

9. Technisch-organisatorische Maßnahmen

9.1. Der AUFTRAGSVERARBEITER gewährleistet, dass er gemäß Art. 32 DSGVO 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 Rechte und Freiheiten der Betroffenen geeignete technische und organisatorische Maßnahmen getroffen hat, um ein dem Risiko angemessenes Schutzniveau sicherzustellen. Sofern sich diesbezüglich während der Zusammenarbeit notwendige Änderungen ergeben, wird der AUFTRAGSVERARBEITER adäquate Maßnahmen nachziehen.

9.2. Der AUFTRAGSVERARBEITER gewährleistet insbesondere, dass die Verarbeitung in Übereinstimmung mit branchenüblichen Standards und den gesetzlichen Bestimmungen, insbesondere den datenschutzrechtlichen und regulatorischen Erfordernissen, erfolgt.

9.3. Der AUFTRAGSVERARBEITER verpflichtet sich, die in **Anlage D** zu dieser Vereinbarung genannten technisch-organisatorischen Maßnahmen einzuhalten, soweit diese aufgrund des

Gegenstands und der Umstände der Verarbeitung anwendbar sind. Der AUFTRAGSVERARBEITER informiert die VERANTWORTLICHE von geplanten wesentlichen Änderungen der in **Anlage D** genannten technisch-organisatorischen Maßnahmen. Als wesentlich gelten Änderungen, wenn neuartige Technologien eingesetzt werden, dadurch bisherige Mängel ausgebessert werden oder sich potentielle neue Risiken für die Datensicherheit ergeben.

9.4. Sofern während der Zusammenarbeit Änderungen notwendig werden, wird der AUFTRAGSVERARBEITER die getroffenen Maßnahmen adäquat anpassen. Die VERANTWORTLICHE trifft dabei die Pflicht, in regelmäßigen Abständen zu prüfen, ob durch geeignete technische und organisatorische Maßnahmen des AUFTRAGSVERARBEITERS ein angemessenes Datenschutzniveau gewährleistet ist.

9.5. Für den Fall, dass der AUFTRAGSVERARBEITER einen Sub-Auftragsverarbeiter heranzieht, stellt der AUFTRAGSVERARBEITER sicher, dass dieser gleichwertige technische und organisatorische Maßnahmen mit dem Sub-Auftragsverarbeiter vereinbart. Der AUFTRAGSVERARBEITER wird sich regelmäßig durch entsprechende Kontrollen davon vergewissern, dass diese Maßnahmen vom Sub-Auftragsverarbeiter zu jeder Zeit faktisch umgesetzt werden. Sollten sich hierbei Risiken zeigen, die der AUFTRAGSVERARBEITER nicht ausreichend abschwächen/steuern kann, hat er die VERANTWORTLICHE darüber in einer geeigneten Form zu informieren.

10. Beendigung der Vereinbarung, Löschung und Rückgabe von Daten

10.1. Der AUFTRAGSVERARBEITER ist verpflichtet, nach Beendigung der Leistungserbringung alle Verarbeitungsergebnisse und Unterlagen, die personenbezogene Daten enthalten, vollständig an die VERANTWORTLICHE zu übergeben. Der AUFTRAGSVERARBEITER ist nicht berechtigt, personenbezogene Daten, Dokumente oder Teile davon weiter aufzubewahren. Ausgenommen davon sind jene Unterlagen und Dokumente zu deren Aufbewahrung der AUFTRAGSVERARBEITER rechtlich verpflichtet ist.

10.2. Alternativ und ausschließlich auf ausdrückliche Weisung der VERANTWORTLICHEN ist der AUFTRAGSVERARBEITER berechtigt, die Daten für die VERANTWORTLICHE weiter vor unbefugter Einsicht gesichert aufzubewahren oder auftragsgemäß zu vernichten, vorbehaltlich gesetzlicher Bestimmungen. Der Nachweis der ordnungsgemäßen Vernichtung ist der VERANTWORTLICHEN auf Anfrage vorzulegen.

10.3. Der AUFTRAGSVERARBEITER ist verpflichtet, die Rückgabe bzw Vernichtung auch bei Sub-Auftragsverarbeitern entsprechend herbeizuführen.

11. Einhaltung des anwendbaren Rechts

11.1. Die Parteien haben das Recht, Änderungen und/oder Ergänzungen zu jedem Teil dieser Vereinbarung über die Auftragsdatenverarbeitung zu verlangen, soweit dies erforderlich ist, um etwaigen Auslegungen, Leitlinien oder Anordnungen der zuständigen Behörden der EU oder der Mitgliedstaaten, nationalen Umsetzungsbestimmungen oder anderen rechtlichen Entwicklungen in Bezug auf die Anforderungen der DSGVO für die Beauftragung von Datenverarbeitern im Allgemeinen oder anderen Anforderungen für die Beauftragung von Datenverarbeitern zu entsprechen. Die Parteien werden sich über die erforderlichen Änderungen nach Treu und Glauben und unter Berücksichtigung ihrer Verpflichtung zur datenschutzkonformen Durchführung dieses Vertragsverhältnisses verständigen.

12. Wirksamkeit, Laufzeit und Beendigung

12.1. Diese Vereinbarung tritt mit Unterzeichnung in Kraft und wird auf unbestimmte Zeit abgeschlossen. Die Beendigung der zugrunde liegenden Lizenzvereinbarung lässt ihre Wirksamkeit unberührt. Sie gilt fort, solange der AUFTRAGSVERARBEITER personenbezogene

Daten im Auftrag der VERANTWORTLICHEN verarbeitet oder solche Daten noch gespeichert hält. Eine ordentliche Beendigung dieser Vereinbarung ist erst zulässig, wenn sämtliche dieser Daten gemäß Punkt 10 zurückgegeben oder gelöscht wurden. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

13. Dokumentenhierarchie

13.1. Im Falle von Widersprüchen oder Inkonsistenzen zwischen den Bestimmungen dieser Vereinbarung über die Auftragsdatenverarbeitung und des unter Punkt 3. genannten Lizenzvereinbarung in Bezug auf die Datenschutzverpflichtungen der Parteien haben die Bestimmungen dieser Vereinbarung über die Auftragsdatenverarbeitung Vorrang.

14. Sonstige Bestimmungen

14.1. Diese Vereinbarung über die Auftragsdatenverarbeitung unterliegt österreichischem Recht, sofern das anwendbare Datenschutzrecht nichts anderes vorsieht. Der Gerichtsstand für alle Streitigkeiten im Zusammenhang mit dieser Vereinbarung über die Auftragsdatenverarbeitung ist Wien.

14.2. Sollte eine Bestimmung dieser Vereinbarung über die Auftragsdatenverarbeitung unwirksam oder nicht durchsetzbar sein, so bleibt diese Vereinbarung über die Auftragsdatenverarbeitung im Übrigen wirksam. Die unwirksame oder undurchführbare Bestimmung ist so zu ändern, dass ihre Wirksamkeit und Durchführbarkeit gewährleistet ist, wobei die Absichten der Parteien so weit wie möglich erhalten bleiben.

15. Anlagen

- Anlage A: Verarbeitungsverzeichnis als Auftragsverarbeiter
- Anlage B: Löschkonzept
- Anlage C: Subdienstleister
- Anlage D: Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

_____, am _____

Wien, am 19.08.2026

_____

_____

_____

Stefan Raffeiner
Geschäftsführer - Teachino FlexCo

Anlage A: Verarbeitungsverzeichnis als Auftragsverarbeiter

Verzeichnis von Verarbeitungstätigkeiten im Produkt Teachino gemäß Art 30 Abs 2 DSGVO

Letzte Überarbeitung: 19.08.2026

Verantwortlicher: _____

Datenschutzbeauftragter des Verantwortlichen: _____

Teachino verarbeitet die nachfolgend genannten personenbezogenen Daten ausschließlich im Auftrag und nach Weisung des Verantwortlichen zur Erbringung der vertraglich vereinbarten Leistungen, einschließlich der Bereitstellung, dem Betrieb und dem Support einer Software zur Vorbereitung und Durchführung des Unterrichts.

Betroffene Person	Zweck	verarbeitete Daten
Bereitstellung der Software		
Jede Person, die die Produktseite app.teachino.io oder teachino.app öffnet	- Aufbau der Netzwerkverbindung und zur Bereitstellung der Software (technisch zwingend notwendig)	- IP-Adresse und Port
Lehrkraft	- Bereitstellung der Software - Anmeldung in die Software - E-Mail-Support im Falle von Anfragen durch die Lehrkraft - Information über Produkt-Updates - Versand von transaktionalen E-Mails.	- Vor- und Nachname - E-Mail-Adresse inkl. Status (verifiziert/nicht verifiziert) - Passwort (gehashed) - Identifier für SSO
Lehrkraft	- regelmäßige Nutzungsauswertung	- Datum- und Uhrzeit der letzten Anmeldung - Datum- und Uhrzeit der Registrierung
Schüler:in	- Bereitstellung der Software - Anmeldung in die Software	- Von Lehrkraft gewählte Bezeichnung, zumeist Vor- oder Vollname, eindeutiges Kürzel bzw. Bezeichnung aus dem Schulverwaltungssystem - Identifier für SSO bzw. Login-Code - Persönlicher Zugangscode
Unterrichtsorganisation		
Lehrkraft	- Zusammenarbeit im Kollegium innerhalb einer Schule - Ableitung des Schultyps und Land zur korrekten Steuerung der KI	- Vor- und Nachname - E-Mail-Adresse inkl. Status (verifiziert/nicht verifiziert) - Name und ID der Schule
Lehrkraft	- Planung des Unterrichts, inkl Zuordnung von Materialien zu einzelnen Stunden - Erstellung von Unterrichtsmaterialien - Zuordnung von Materialien zu unterrichteten Kursen/Klassen/Schüler:innen - korrekte Zuordnung des	- unterrichtete Kurse (Land, Schultyp, Fach, Klasse) - Stundenplan und Termine (Datum, Zeit, Kurs, Notizen) - Erstellte und hochgeladene Unterrichtsmaterialien und Ordner, inkl. Versionshistorie - KI-Chats und Prompt-Eingaben - Schülerliste (Name der Schüler:innen)

	Lehrplans	
Schüler:in	- Eindeutige Zuordnung von Materialien zu unterrichteten Kursen / Schüler:innen	- Von Lehrkraft gewählte Bezeichnung, zumeist Vor- oder Vollname, eindeutiges Kürzel bzw. Bezeichnung aus dem Schulverwaltungssystem - aus der Unterrichtsorganisation abgeleitete Daten (Land, Schultyp, Fach, Klasse, Stundenplan) - Zuordnung zu Kursen
Aufgabenbearbeitung, Dokumentation und Überprüfung		
Schüler:in	- Durchführung und , Auswertung des Unterrichts durch Lehrkräfte	- Von Lehrkraft gewählte Bezeichnung, zumeist Vor- oder Vollname, eindeutiges Kürzel bzw. Bezeichnung aus dem Schulverwaltungssystem - Identifier für SSO bzw. Login-Code - Persönlicher Zugangscode - Zugehörigkeit zu einem Kurs (und damit Schule und Lehrkraft) - Antworten auf Fragen bzw. Chatbots, inkl. Uhrzeit sowie Rückantwort der KI - Abgaben von Aufgaben in Form von Text, Audio, Video, Dateien oder Links - Stimmdaten bzw. Bilddaten samt darin ersichtlicher Handschrift bei Einsprechen / Abfotografieren von Antworten
Lehrkraft	- zur Durchführung des Unterrichts	- erstellte Aufgaben - Von Lehrkraft gewählte Bezeichnung, zumeist Vor- oder Vollname, eindeutiges Kürzel bzw. Bezeichnung aus dem Schulverwaltungssystem von Schüler:innen zur Zuordnung der Aufgabe - von Schüler:innen beantwortete Aufgaben und Chatbots samt Datum/Uhrzeit - Abgaben von Aufgaben in Form von Text, Audio, Video, Dateien oder Links - KI-generierte Rückmeldung zu beantworteten Aufgaben - deterministisch generierte Rückmeldung zu beantworteten Aufgaben - Feedback der Lehrkraft - Bewertung durch die Lehrkraft

Lehrkraft	- Dokumentation des Unterrichts und von Leistungen (einschließlich Sicherung des Unterrichtsertrags)	- Von Lehrkraft gewählte Bezeichnung, zumeist Vor- oder Vollname, eindeutiges Kürzel bzw. Bezeichnung aus dem Schulverwaltungssystem von Schüler:innen - Sprachaufnahmen: Schülernamen samt Unterrichtsanmerkungen zur vereinfachten Eingabe, die automationsgestützt in strukturierte Textdokumentation umgewandelt wird - Dokumentation der Lehrkraft zu Leistungen, die außerhalb der Plattform erbracht werden (zB Note der Schularbeit; Notiz zu vergessenen Hausübungen)
Schüler:in	- Dokumentation des Unterrichts durch Lehrkräfte	- Rückmeldungen und Dokumentation von Lehrkräften zu Aufgaben, Lernfortschritt, Mitarbeit und Gesprächen - Dokumentation der Lehrkraft zu Leistungen, die außerhalb der Plattform erbracht werden (zB Note der Schularbeit; Notiz zu vergessenen Hausübungen) - (Summative) Bewertungen der Lehrkraft

Eine Übermittlung von personenbezogenen Daten an ein Drittland oder eine internationale Organisation findet grundsätzlich nicht statt. Der AUFTRAGSVERARBEITER setzt ausschließlich Sub-Auftragsverarbeiter mit Sitz innerhalb der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraums (EWR) ein.

Soweit es sich bei diesen Sub-Auftragsverarbeitern um EU-Tochterunternehmen von Konzernen mit Hauptsitz in Drittländern (z. B. den USA) handelt, hat der AUFTRAGSVERARBEITER angemessene technische und organisatorische Maßnahmen getroffen. Insbesondere verarbeiten diese Dienstleister Daten nach Möglichkeit in pseudonymisierter Form und ohne Zugriff auf den Zuordnungsschlüssel, sodass das Risiko eines unbefugten Zugriffs durch Muttergesellschaften im Drittland auf ein angemessenes Maß reduziert wird.

Ausgenommen hiervon sind Funktionen für die Bereitstellung eines Hilfe-Centers, der Kundensupport sowie der Versand von E-Mails an Lehrkräfte. Hierfür werden Sub-Auftragsverarbeiter eingesetzt, die ihrerseits Sub-Auftragsverarbeiter in Drittländern (insbesondere USA) nutzen. Eine solche Übermittlung erfolgt ausschließlich auf Basis geeigneter Garantien gemäß Art. 44 ff. DSGVO (insbesondere den EU-Standardvertragsklauseln) oder eines Angemessenheitsbeschlusses der Europäischen Kommission (wie dem EU-U.S. Data Privacy Framework).

Löschkonzept und Aufbewahrungsfristen Teachino FlexCo Software

Verantwortlich: Geschäftsführung
Datum der letzten Überarbeitung: 19.08.2025

Arten der Daten und Löschprozesse		
Datenart	**Beschreibung**	**Löschkonzept**
Server-Log-Dateien		Automatisierte Löschung nach Ablauf von 7 Tagen *Prozess: automatisierter Log-Rotation-Prozess per CronJob*
Datenbank- und File-Storage Backups	Backups dienen **ausschließlich** der Systemwiederherstellung im Falle eines technischen Ausfalls	Tägliche Backups: Automatisierte Löschung nach Ablauf von 7 Tagen. Wöchentliche Backups: Automatisierte Löschung nach Ablauf von 30 Tagen. Personenbezogene Daten, die vor dem Einspielen einer Datensicherung bereits gelöscht wurden, werden nach der Wiederherstellung des Backups automatisch erneut gelöscht. *Prozess: automatisierter Backup-Prozess per CronJob*
Nutzerdaten von Lehrkräften Daten zur Unterrichtsplanung	E-Mail-Adresse, Name, Unterrichtsplanung, Stundenplan, ...	**Auf Anfrage**: Folgende Daten von Nutzern werden auf Beauftragung gelöscht: a) Datensätze in der Datenbank, welche dieser Person zugeordnet sind oder von dieser Person erstellt wurden. Mitgliedschaften in Kursen anderer Personen (in diesem Fall wird der Kurs nicht gelöscht) b) hochgeladene Dateien der Person c) Datensätze in Support- und Kommunikationstools

		Wenn die Beauftragung zur Löschung nicht eindeutig einem Nutzer zugeordnet werden kann, wird diese erst nach eindeutiger Identifikation durchgeführt *Prozess: automatisierte Löschroutine, welche vom Kundensupport gestartet werden kann* Folgende Daten werden entsprechend der rechtlich zeitlichen Rahmen gelöscht: a) Rechnungen und Zahlungsbelege im Falle einer erworbenen SOFTWARE-Lizenz Löschungen werden mit Zeitstempel und Nutzer-ID dokumentiert, damit im Falle einer Systemherstellung über Backups die Daten erneut gelöscht werden können. **Automatisierte Löschung:** Folgende Daten von Nutzern werden automatisch gelöscht Automatisiert gelöscht werden - analog zu oben - Daten von Nutzer:innen, welche seit 36 Monaten Teachino nicht genutzt haben. - Hintergrund: Nutzer:innen pausieren aufgrund von Karenz o.Ä. ihre Nutzung längerfristig und haben ggf. auch keinen Zugriff auf Ihre dienstliche E-Mail-Adresse. Zu diesem Zweck wird das Datum der letzten Nutzung gespeichert *Prozess: automatisierte Löschroutine per CronJob*
Spracheingaben	von Lehrkräften aufgenommene Sprachdaten zur Dokumentation des Unterrichts (Schülername, inhaltliche Anmerkungen)	- Sprachdaten werden KI-gestützt in Textdateien transkribiert, wobei der Schülername pseudonymisiert wird. Die Sprachaufzeichnung wird nach der Transkription gelöscht. - Die transkribierten Textdateien werden strukturiert aufbereitet. Die temporäre Schüler-ID (Pseudonymisierung) wird nach Zuordnung innerhalb der Software gelöscht.
Sprach- und Bildeingaben von Schülern	von Schüler:innen aufgenommene Spracheingaben zur Beantwortung von Aufgaben oder hochgeladene Bilder einer handschriftlichen Aufgabenbeantwortung	- Sprach- und Bildeingaben werden nach der Transkription automatisch gelöscht.

Antworten von und Bewertungen zu Schüler*innen	- Namen und Klassenlisten - Antworten auf Fragen bzw. Chatbots, inkl. Uhrzeit sowie Rückantwort der KI - Bewertungen und Dokumentation des Lernfortschritts - Zugehörigkeit zu einem Kurs (und damit Schule und Lehrkraft)	Werden mit Ende des Kalenderjahres, in dem das zugehörige Schuljahr endet, automatisch gelöscht. Beispiel: Daten zu einem Schuljahr, welches am 31.07.2026 endet, werden zum 31.12.2026 gelöscht. *Prozess: automatisierte Löschroutine per CronJob*

Anlage C: Subdienstleister

Der AUFTRAGSVERARBEITER beauftragt (Stand 19.08.2026) folgende Subdienstleister mit der Verarbeitung personenbezogener Daten zur Erfüllung des Vertrages:

Bezeichnung	Firma und Anschrift	Zweck
OVH Cloud	OVH GmbH Christophstraße 19 50670 Köln Deutschland Handelsregister: Amtsgericht Saarbrücken - HRB 15369 OVH GmbH ist eine Filiale der OVH SA-Gruppe, eine unter der Nummer 537 407 926 eingetragene Gesellschaft im Handels- und Gesellschaftsregister von Lille mit Sitz in 2, Rue Kellermann, 59100 Roubaix, Frankreich	Hosting von Datenbank, Dateien etc. sowie Teile des Betriebs der App und der Software selbst. Betroffene Daten sind daher jene, die über die Software verarbeitet werden.
Mave	mave.io B.V. Westplein 12, 3016BM Rotterdam, Netherlands	Bereitstellung von Videos zu Schulungszwecken.
Pathfindr	Pathfindr ApS Veddelev Bygade 34 4000 Roskilde Dänemark	Generation und Bearbeitung von Vorschau-Ansichten von Dokumenten, sowie Aufzeichnung und Wiedergabe von Video- und Audio-Dateien.
für die Bereitstellung des Hilfe-Centers, von Kundensupport sowie der Versand von E-Mails an Lehrkräfte		
Mailjet	Mailjet SAS 43 rue de Dunkerque 75010 Paris, Frankreich	Transaktionaler Versand von E-Mails (z.B. Passwort vergessen, Unterrichtsmaterial geteilt, ...)
Productlane	Productlane GmbH, Albert-Roßhaupter-Str. 3b, 81369 München, Deutschland	Bereitstellung einer Hilfe-Center- und Kunden-Support-Lösung. Sie zeigt Hilfeseiten an und ermöglicht die Kontaktaufnahme mit dem AUFTRAGSVERARBEITER.
Brevo	Sendinblue SAS 9-17 rue de Salneuve 75017 Paris, Frankreich	Versand von Informationen zu wichtigen Produkt-Änderungen.

für optionale KI-Transkription von Bildern von Handschrift sowie Spracheingabe		
Mistral	Mistral AI SAS 15 rue des Halles 75001 Paris, Frankreich	Bereitstellung von Cloud- und KI-Diensten zur KI-Transkription von Audioaufnahmen, Erkennung und Entfernung etwaiger PII-Daten aus Texteingaben und Texterkennung von Dokumenten. Diese Daten werden nach der Umwandlung gelöscht. Verarbeitungsort: Europäische Union.
Microsoft Ireland	Microsoft Ireland Operations Limited One Microsoft Place South County Business Park Leopardstown, Dublin 18 D18 P521, Irland	Bereitstellung von Cloud- und KI-Diensten zur OCR- bzw. KI-Transkription hochgeladener Bilder mit handschriftlichen Texten. Diese Daten werden nach der Umwandlung gelöscht. Überführung von maschinenlesbaren Texten in strukturierte Textdateien sowie Bereitstellung von generativen KI-Modellen. Microsoft erhält pseudonymisierte Daten ohne Zugang zu den Identifizierungsdaten. Während die verarbeiteten Daten für den AUFTRAGSVERARBEITER als personenbezogene Daten (pseudonymisierte Daten) anzusehen sind, sind sie mangels Möglichkeit der Re-Identifizierung für Microsoft anonyme Daten. Verarbeitungsort: Europäische Union.
Google	Google Cloud EMEA Ltd 70 Sir John Rogerson's Quay Dublin 2, Ireland	Überführung von maschinenlesbaren Texten in strukturierte Textdateien sowie Bereitstellung von generativen KI-Modellen. Google erhält pseudonymisierte Daten ohne Zugang zu den Identifizierungsdaten. Während die verarbeiteten Daten für den AUFTRAGSVERARBEITER als personenbezogene Daten (pseudonymisierte Daten)

		anzusehen sind, sind sie mangels Möglichkeit der Re-Identifizierung für Google anonyme Daten. Verarbeitungsort: Europäische Union.

Anlage D: Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Der Auftragsverarbeiter ist verpflichtet, die in der folgenden Tabelle aufgeführten technischen und organisatorischen Sicherheitsmaßnahmen umzusetzen, anzuwenden und ständig auf dem neuesten Stand zu halten, und zwar zusätzlich zu den Maßnahmen, die in der Gesetzgebung zum Schutz personenbezogener Daten in der jeweils geltenden Fassung vorgesehen sind und die auf die vom Auftragsverarbeiter erbrachten Dienstleistungen anwendbar sind, sowie zu den zusätzlichen Maßnahmen, die erforderlich sind, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten, bevor er mit der Verarbeitung personenbezogener Daten im Auftrag der Verantwortlichen beginnt. Die nachstehende Tabelle stellt eine nicht erschöpfende Aufzählung dar; der Auftragsverarbeiter verpflichtet sich daher, alle weiteren Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Sicherheitsniveaus unter Berücksichtigung des Stands der Technik und der Kosten der Umsetzung sowie der Art, des Umfangs, des Kontexts und des Zwecks der Verarbeitung sowie des unterschiedlich wahrscheinlichen und schwerwiegenden Risikos für die Rechte und Freiheiten natürlicher Personen umzusetzen, anzuwenden und, in Absprache mit der VERANTWORTLICHEN, ständig zu aktualisieren.

Der AUFTRAGSVERARBEITER verpflichtet sich zur Einhaltung der jeweils anwendbaren europäischen sowie nationalen gesetzlichen Bestimmungen zur Informationssicherheit und zum Telekommunikationsdatenschutz (insbesondere der Vorgaben der einschlägigen nationalen Sicherheits- und Telekommunikationsgesetze). Darüber hinaus sind geeignete Maßnahmen im Zusammenhang mit dem Trennungsprinzip, d.h. der getrennten Verarbeitung von Daten, die für unterschiedliche Zwecke und Kunden erhoben werden, sicherzustellen.

SICHERHEITSBEREICHE		SICHERHEITSMASSNAHMEN
1. NETZ- UND SYSTEMSICHERHEIT	1.1	Firewall- und Router-Konfigurationen müssen eingerichtet werden, um den ein- und ausgehenden Datenverkehr von "nicht vertrauenswürdigen" Netzen (einschließlich drahtloser Netze) und Systemen zu beschränken. Es ist jeder Datenverkehr mit Ausnahme von Protokollen zu verhindern, die für die persönliche Datenumgebung (PDE) erforderlich sind.
	1.2	Für IKT-Ressourcen (z. B. Datenbanken, Anwendungen, Betriebssysteme), die personenbezogene Daten verarbeiten, müssen Sicherheitshärtungskonfigurationen (über Vorlagen) angewandt werden, um nur die für die betreffenden Tätigkeiten unbedingt erforderlichen Dienste zu ermöglichen.
	1.3	Personenbezogene Daten müssen gegen das Risiko des Eindringens (z. B. IPS, IDS) und gegen Schadsoftware geschützt werden, indem geeignete elektronische Instrumente aktiviert werden, die rechtzeitig aktualisiert werden, sobald eine Signatur verfügbar ist.
	1.4	Regelmäßige Software-Updates (z. B. Patching von Client- und Server-Betriebssystemen und Basisanwendungen) müssen nach bewährten Verfahren durchgeführt werden, auf jeden Fall aber nicht später als sechs Monate, und kritische und hochsichere Patches müssen umgehend installiert werden.

SICHERHEITSBEREICHE		SICHERHEITSMASSNAHMEN
2. DATENSICHERHEIT	2.1	Die Aufbewahrungsfrist für personenbezogene Daten muss auf das Maß beschränkt werden, das für jede einzelne erbrachte Dienstleistung erforderlich ist, allerdings unter Beachtung der geltenden rechtlichen und/oder regulatorischen Verpflichtungen.
	2.2	Für die Löschung von Daten, die für die erbrachte Einzelleistung nicht mehr benötigt werden, und für die Stilllegung von IKT-Anlagen müssen unumkehrbare und sichere Bereinigungsverfahren eingeführt werden, um alle personenbezogenen Daten zu entfernen und/oder vor der Entsorgung oder Wiederverwendung sicher und unwiderruflich zu überschreiben. Sollte dies nicht möglich sein, müssen die Datenträger nach bewährten Verfahren und Standards vernichtet oder unbrauchbar gemacht werden, und es ist eine Bescheinigung über die Vernichtung erforderlich.
	2.3	Papierdokumente, die personenbezogene Daten enthalten, müssen physisch vernichtet werden, bevor sie mit speziellen Geräten wie Schreddern entsorgt werden.
	2.4	Die Verarbeitung von Produktionsdaten (Echtdaten) ist auf Produktionsumgebungen beschränkt. In Ausnahmefällen und mit den erforderlichen Genehmigungen dürfen QA-Umgebungen nur dann (echte) personenbezogene Daten verarbeiten, wenn sie als Produktionsumgebung geschützt sind. Andere Vorproduktionsumgebungen (z. B. Entwicklung, Test, UAT, ...) müssen entweder anonymisierte oder zusammengefasste Daten verwenden.
	2.5	Personenbezogene Daten müssen unlesbar gemacht werden (z. B. durch Verschlüsselung), wenn sie auf tragbaren digitalen Medien, Sicherungsmedien und Protokolldateien gespeichert werden.
	2.6	Die Anzahl der Speicherorte für personenbezogene Daten (z. B. Datenbanken, Dateien, Kopien, Archive) muss auf ein Minimum reduziert werden, um unnötige Doppelarbeit zu vermeiden.
	2.7	Die Übertragung personenbezogener Daten über offene, öffentliche oder nicht vertrauenswürdige Netze muss durch starke Kryptographie und die Verwendung sicherer Protokolle geschützt werden. Ist eine Kanalverschlüsselung nicht möglich, müssen Dateien und Anhänge, die personenbezogene Daten enthalten, durch Verschlüsselung geschützt werden, wenn sie über offene, öffentliche oder nicht vertrauenswürdige Netze übertragen werden.
	2.8	Personenbezogene Daten dürfen nicht auf Wechseldatenträger kopiert werden, es sei denn, es handelt sich um Datenträger, die vom Auftragsverarbeiter für bestimmte Aufgaben ausdrücklich zugelassen sind (siehe Maßnahme 2.5).

SICHERHEITSBEREICHE		SICHERHEITSMASSNAHMEN
	2.9	Datenträger (abnehmbare und nicht abnehmbare), die personenbezogene Daten enthalten, müssen durch angemessene physische und logische Sicherheitsmaßnahmen vor unbefugtem Zugriff geschützt werden.
	2.10	Die Mitarbeiter, die Zugriff auf Papierdokumente haben, müssen angemessen über die richtigen Verhaltensregeln zum Schutz der in Papierdokumenten enthaltenen personenbezogenen Daten unterrichtet und geschult werden.
	2.11	Papierdokumente werden nach Gebrauch bzw. Ablauf von Aufbewahrungsfristen sicher vernichtet.
	2.12	Die Verarbeitung der Daten des Auftraggebers erfolgt strikt getrennt von Daten anderer Auftraggeber sowie von eigenen Daten des Auftragsverarbeiters (z. B. durch logische Trennung mittels Datenbank-Mandanten-IDs, Rollen- und Rechtekonzepte oder physische Trennung).
3. DATENVERFÜGBARKEIT	3.1	Es müssen geeignete Verfahren eingeführt werden, um die rechtzeitige Verfügbarkeit der personenbezogenen Daten (als Recht der betroffenen Person) zu gewährleisten. Back-up-Verfahren müssen mindestens wöchentlich Kopien der personenbezogenen Daten gewährleisten. Wiederherstellungspunkt- und Wiederherstellungszeitziel müssen den jeweiligen Geschäftsanforderungen entsprechen.
4. IDENTITÄTS- UND ZUGANGSMANAGEMENT	4.1	Die Zugangsberechtigung zu Produktionsumgebungen, die personenbezogene Daten enthalten, muss nach den Grundsätzen "Kenntnisnahme erforderlich" und "geringstmögliches Recht" erteilt werden.
	4.2	Es müssen Richtlinien und Verfahren eingeführt werden, um die ordnungsgemäße Identifizierung von Benutzern und Administratoren zu gewährleisten, die auf Systemkomponenten zur Verwaltung personenbezogener Daten zugreifen. Jedem Benutzer muss ein Benutzername zugewiesen werden, bevor er Zugang zu den Authentifizierungssystemen und personenbezogenen Daten erhält. Jeder Nutzername darf nur eine Person identifizieren.
	4.3	Passwörter für Fernzugänge zu Systemen, die personenbezogene Daten verwalten, müssen durch einen Authentifizierungsmechanismus geschützt werden, und in Passwortmanager-Tools verwaltet werden, um die Sicherheit der Zugangsdaten zu gewährleisten (in Verbindung mit Maßnahme 4.6). Wo technisch möglich muss eine 2-Faktor-Authentifizierung verwendet werden.
	4.4	Passwörter für Systeme und Geräte, die personenbezogene Daten verwalten, müssen komplex sein (mindestens acht Zeichen und z. B. eine Kombination aus Groß- und

SICHERHEITSBEREICHE		SICHERHEITSMASSNAHMEN
		Kleinbuchstaben, Zahlen und Sonderzeichen) und dürfen für den Nutzer nicht leicht zu ermitteln sein .
	4.5	Systemressourcen und Zugriffsrechte müssen jedem Benutzerkonto eindeutig zugewiesen werden.
	4.6	Der Fernzugriff (von externen Netzen) auf die Umgebung, in der personenbezogene Daten verarbeitet werden, muss durch eine mehrstufige Authentifizierung geschützt werden.
	4.7	Jeder Zugang zu Datenbanken, die personenbezogene Daten enthalten, muss geschützt/kontrolliert werden, um die Grundsätze des "Need to know", des "least privilege" und der Rückverfolgbarkeit zu gewährleisten.
	4.8	Die Zugriffsrechte der Nutzer auf personenbezogene Daten müssen in regelmäßigen Abständen, in jedem Fall aber mindestens einmal jährlich, im Rahmen des regulären Identitäts- und Zugriffsmanagementprozesses überprüft bzw. neu zertifiziert werden.
5. PROTOKOLLIERUNG UND ÜBERWACHUNG	5.1	Der Zugriff auf Produktionsumgebungen, die personenbezogene Daten enthalten, und der Zugriff auf personenbezogene Daten im Allgemeinen müssen überwacht und protokolliert werden, um die Verbindung zwischen dem Zugriff und dem einzelnen Benutzer, der auf personenbezogene Daten zugreift, genau zu erfassen. Außerdem muss eine Überwachung durchgeführt werden, um Bedrohungen der Sicherheit personenbezogener Daten zu verhindern und zu erkennen.
	5.2	Jeder Änderung personenbezogener Daten (Änderung, Löschung, Einfügung) muss durch Aufzeichnung der Mindestinformationen, die erforderlich sind, um die Zugriffsmodalitäten zu rekonstruieren und eine Überwachung im System zu ermöglichen, nachvollzogen werden: - Benutzeridentifikation - Art des Events - Datum und Uhrzeit - Anzeige von Erfolg oder Misserfolg - Quelle des Ereignisses - Identität der betroffenen Daten (Kennung der betroffenen Person), Systemkomponente oder Ressource.
6. ORGANISATION UND MENSCHLICHE SICHERHEIT	6.1	Es müssen geeignete Verfahren eingeführt werden, um die Verfügbarkeit der personenbezogenen Daten zu gewährleisten.
	6.2	Es muss das gesamte Personal mit den Grundsätzen und Verfahren im Zusammenhang mit der Sicherheit personenbezogener Daten vertraut gemacht werden. Beispielsweise können regelmäßige Tests oder Simulationen durchgeführt werden, um festzustellen, ob Mitarbeiter auf einen Link in einer verdächtigen E-Mail klicken oder persönliche/empfindliche Informationen weitergeben, ohne

SICHERHEITSBEREICHE		SICHERHEITSMASSNAHMEN
		die Zuverlässigkeit der Quelle durch geeignete Sicherheitsverfahren zu überprüfen. In der Folge müssen die Mitarbeiter, die dem Test zum Opfer fallen, gezielt geschult werden.
	6.3	Mit allen Unterauftragnehmern von Dienstleistungen müssen klare vertragliche Vereinbarungen unterzeichnet werden, um ihre Verantwortung für die Sicherheit der personenbezogenen Daten, die sie im Auftrag des für die Verarbeitung Verantwortlichen verarbeiten / speichern / übermitteln, festzulegen. Unterauftragnehmener müssen entweder über eine ISO-27001-Zertifizierung verfügen oder einen von uns bereitgestellten äquivalenten Sicherheitsfragebogen positiv beantworten.
	6.4	Die Verantwortlichkeiten und Pflichten der Mitarbeiter in Bezug auf die Vertraulichkeit personenbezogener Daten müssen eindeutig festgelegt werden und auch nach Beendigung oder Wechsel des Beschäftigungsverhältnisses gelten.
7. DATENSCHUTZ DURCH TECHNIK	7.1	Prozesse und Werkzeuge für den Lebenszyklus der sicheren Softwareentwicklung (SDLC) müssen mit geeigneten Sicherheitsprüfungen / -kontrollen und -anforderungen integriert werden, um sicherzustellen, dass neue IKT-Software / -Anwendungen unter Berücksichtigung der Anforderungen an die eingebettete Sicherheit entworfen und entwickelt werden.
	7.2	Die Prozesse des IKT-Änderungsmanagements müssen mit geeigneten Sicherheitsprüfungen / -kontrollen und -anforderungen integriert werden, um den kontinuierlichen Schutz der vorhandenen IKT-Software / -Anwendungen bei relevanten Änderungen zu gewährleisten. Durch die Prüfungen/Kontrollen aufgedeckte Abweichungen müssen klassifiziert und auf der Grundlage ihrer Kritikalität angemessen gehandhabt werden (wobei Abhilfe- und Schadensbegrenzungsmaßnahmen je nach Kritikalität zeitnah durchgeführt werden).
8. BENACHRICHTIGUNG ÜBER EINE VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN	8.1	Prozesse und Instrumente für das Incident Management müssen ordnungsgemäß implementiert und werden, um die Erkennung und Klassifizierung von Verletzungen des Schutzes personenbezogener Daten zu ermöglichen, damit sie dem für die Verarbeitung Verantwortlichen innerhalb der im Abschnitt "Meldepflicht und Verletzung des Schutzes personenbezogener Daten" festgelegten Fristen ordnungsgemäß mitgeteilt werden können.
	8.2	Es muss ein spezielles Register für Verletzungen des Schutzes personenbezogener Daten erstellt und geführt werden.