Vereinbarung über Auftragsverarbeitung

zwischen	und
Tragen Sie bitte die genaue Bezeichnung der Schule ein	LionGate AG
	Leopoldstr 244
	D-80807 München
– nachfolgend: **„Auftraggeber"** –	– nachfolgend: **„Auftragnehmer"** –

Präambel

Die LionGate AG (im folgenden LionGate oder Auftragnehmer) stellt unter dem Namen „vicole" eine Plattform für digitales Lernen zur Verfügung. Diese Vereinbarung zur Auftragsdatenvereinbarung definiert die Verpflichtungen der Vertragsparteien zum Datenschutz. Sie findet Anwendung auf alle Tätigkeiten bei denen Beschäftigte des Auftragnehmers (LionGate) oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

(1) Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

(1) Der Auftragsnehmer stellt für den Auftraggeber eine individuelle, auf Cloud-Infrastruktur betriebene Plattform für digitales Lernen zur Verfügung. Hierzu gehören der Zugang zur unabhängigen vicole Plattform der jeweiligen Schule (Access), die gemeinsame Ablage und Speicherung von Dateien (Speicherung) sowie die virtuellen Kommunikationsfunktionen mit Audio und Video zur Nutzung durch berechtigte Lehrer und Schüler.

(2) Vicole ist eine Plattform für digitales Lernen. Schulen und andere Bildungseinrichtungen können das System nutzen und dort Lernangebote bereitstellen. Hierdurch können Kurse individuell gestaltet werden. Unter anderem stehen folgende Elemente zur Verfügung:

- Persönliche Dokumentenablage mit Möglichkeit zum Teilen der Dokumente mit anderen Benutzern innerhalb der Schule
- Online-Unterricht mit Multimedia-Unterstützung (Audio, Video, Chat, Präsentation und Bildschirmfreigabe)

(3) Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

Art der Daten	Art und Zweck der Datenverarbeitung	Kategorien betroffener Personen
Daten der Schule - Bezeichnung der Schule - Ort - optional Link zur Homepage **Daten der Lehrkräfte:** - Name - Vorname - Schule - Unterrichtete Klassen/Fächer/Kurse - E-Mail-Adresse im Rahmen der Kooperationsplattform - Adresse und weitere Kontaktdaten optional, sofern vom Benutzer gewünscht (nicht notwendig) **Nutzungsbezogene Daten:** - Benutzername - Datum des letzten Logins - in der Kooperationsplattform hochgeladene Dateien - gezeigte Präsentationen und Chatbeiträge nur während des Live-Unterrichts **Daten der Schülerinnen und Schüler:** - Vorname, Nachname - Klassenstufe/-bezeichnung - E-Mail Adresse im Rahmen der Kooperationsplattform - Adresse und weitere Kontaktdaten optional, sofern vom Benutzer gewünscht (nicht notwendig) **Nutzungsbezogene Daten:** - Benutzername / Kennwort (Account) - Datum des letzten Logins - in der Kooperationsplattform hochgeladene Dateien - gezeigte Präsentationen und Chat-Beiträge nur während des Live-Unterrichts	- Unterstützung des digitalen Unterrichts - Identifizierung des Schülers / der Schülerin in der Teilnahme am Unterricht und im Austausch von Dateien - Steuerung des Zugriffs zur Lernplattform - Rückfragen der Schüler/-innen an die Lehrerkraft - Kommentare/Antworten durch die Lehrkraft an die Schüler/-innen	- Von der Schulleitung beauftragte(r) Administrator(en), für den/die eine Dienstanweisung erlassen wurde - Lehrkräfte - Schülerinnen und Schüler

(4) Daten der Lehrkräfte dürfen grundsätzlich nur gespeichert werden, soweit die jeweiligen Lehrkräfte wirksam eingewilligt haben. Einer Einwilligung bedarf es nicht, soweit die Kooperationsplattform auf Grund von Regelungen des Kultusministeriums oder durch Beschluss der Schule (Gesamtkonferenz) verpflichtender Bestandteil des Unterrichts ist. In

diesem Fall sind die Betroffenen vor dem Einsatz der Plattform über Art und Umfang der Datenverarbeitung umfassend durch die Schule zu informieren. Verantwortlich für die Einholung der Einwilligung ist der Auftraggeber.

(5) Daten der Schülerinnen und Schüler dürfen grundsätzlich nur gespeichert werden, soweit die Betroffenen bzw. bei Minderjährigen bis zur Vollendung des 16. Lebensjahres die Erziehungsberechtigten sowie bei Minderjährigen ab Vollendung des 16. Lebensjahres diese selbst und die Erziehungsberechtigten wirksam eingewilligt haben. Verantwortlich für die Einholung der Einwilligung ist der Auftraggeber.

(6) Die Vereinbarung zur Auftragsdatenvereinbarung gilt unbefristet und kann von beiden Parteien mit einer Frist von einem Monat jeweils zum Monatsende gekündigt werden.

(2) Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO).

(2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

(3) Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DSGVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen so zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

(3) Für die Einhaltung der vereinbarten Schutzmaßnahmen und deren geprüfter Wirksamkeit wird auf die genehmigten Verhaltensregeln nach Art. 40 DSGVO verwiesen, denen sich der Auftragnehmer unterworfen hat.

(4) Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(5) Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

(6) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(7) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(8) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

(9) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(10) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück.

(11) In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren.

(12) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

(13) Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

(14) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Die Löschung ist schriftlich zu bestätigen.

(15) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

(4) Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung / -erhebung / -nutzung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich.

(2) Die Plattform wird vorkonfiguriert durch den Auftragnehmer bereitgestellt. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und schriftlich festzulegen oder in einem dokumentierten elektronischen Format festzulegen.

(3) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(4) Im Falle einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt § 3 Abs. (15) entsprechend.

(5) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.
Datenschutzbeauftragter des Auftraggebers:
_____

(5) Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person oder den Antrag an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

(6) Nachweismöglichkeiten

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

(2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

(3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

(7) Subunternehmer (weitere Auftragsverarbeiter)

(1) Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist zulässig.

(2) Ein Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

(3) Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Subunternehmer durchgeführt:

Name und Anschrift des Subunternehmers	Beschreibung der Teilleistung
Amazon Web Services EMEA SARL 38 avenue John F. Kennedy L-1855 Luxembourg	Bereitstellung der Cloud Infrastruktur (Server) in deutschem Rechenzentrum. Siehe hierzu auch: https://aws.amazon.com/de/compliance/gdpr-center/

(4) Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer holt der Auftragnehmer die Zustimmung des Auftraggebers ein, wobei diese nicht ohne wichtigen datenschutzrechtlichen Grund verweigert werden darf.

(5) Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

(6) Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

(7) Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO). Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seinen unterstellten Personen erfüllt hat.

(8) Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher « im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Es gilt deutsches Recht.

(9) Technisch-Organisatorische Maßnahmen

(1) Für die auftragsgemäße Bearbeitung personenbezogener Daten nutzt der Auftragnehmer folgende Einrichtungen:

Amazon Web Services EMEA SARL
38 avenue John F. Kennedy
L-1855 Luxembourg

Die Daten des Auftragnehmers werden in einer ausfallsicheren Datenbank und einem ausfallsicheren Objektspeicher gespeichert.

(2) Die folgenden technischen und organisatorischen Maßnahmen werden als verbindlich festgelegt:

a. Der Auftragnehmer gewährleistet, dass

- Unbefugten der Zugang zu den Verarbeitungsanlagen verwehrt wird,
- Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können,
- die Datenverarbeitungssysteme nicht mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten benutzt werden können,
- die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können,
- die innerbehördliche Organisation den besonderen Anforderungen des Datenschutzes gerecht wird.

b. Der Auftragnehmer beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

c. Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden.

(10) Haftung und Schadensersatz

(1) Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

_____, den _____ München, den _____

_____ _____
Auftraggeber Auftragnehmer

Anhang 1:
Technische und organisatorische Maßnahmen des Auftragnehmers nach Art. 32 DSGVO (TOM)

Die digitale Unterrichtsplattform „vicole" wird auf Basis einer Cloud-Infrastruktur in vollständig getrennten Umgebungen für die jeweilige Schule bereitgestellt.

Alle Server und Infrastrukturkomponenten befinden sich an einem von drei physischen Standorten im Großraum Frankfurt/Main in Deutschland (Region „eu-central-1" von Amazon Web Services) in Rechenzentren, die gemäß ISO27001:2013 zertifiziert sind.

Für die in den Rechenzentren anzuwendenden TOMs wird auf die einschlägigen Informationen von Amazon Web Service verwiesen, die zusammen mit dem Zertifikat selbst unter
https://aws.amazon.com/de/compliance/iso-27001-faqs/
abrufbar sind.

Alle Daten der Anwender von vicole werden in den oben genannten Rechenzentren gespeichert. Eine Verarbeitung der Daten auf EDV-Anlagen der LionGate AG findet darüber hinaus nur statt, soweit technisches Personal während der Bereitstellung und Betreuung mit Client-Computern auf diese Umgebungen zugreift. Eine Speicherung von Daten auf eigenen Servern der LionGate AG erfolgt nicht.

Die nachfolgenden Abschnitte von LionGate zusätzlich getroffenen, technischen und organisatorischen Maßnahmen.

1. Vertraulichkeit

1.1 Zutrittskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
Manuelles Schließsystem mit Sicherheitsschlössern an den Büroräumen	Dokumentation Schlüsselausgabe durch GF/Assistenz
Elektronisches Schließsystem oder manuelles Schließsystem am Gebäude	Empfang am Gebäudeeingang während Geschäftszeiten

1.2 Zugangskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
Persönliches Login mit Benutzername und Passwort	Zentrale Verwaltung aller Benutzerzugänge
2-Faktor-Authentifizierung für kritische Systeme	Joiners-/Leavers-Prozess mit zentraler Sperre der Benutzerzugänge bei Ausscheiden von Mitarbeitern
Anti-Virus-Software	„Clean Desk" Policy
VPN-Verbindung für Zugriff auf interne Server	Richtlinie „Mobiles Arbeiten"
Mobile Endgeräte mit Zugangscodes	
Verschlüsselung von Datenträgern der Laptops	
Automatische Desktopsperre mit Passwort	
Zentrale Passwortrichtlinie mit Komplexitätsregeln und regelmäßigem Passwortwechsel	

1.3 Zugriffskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
Protokollierung von Benutzerzugriffen in den Audit-Logs der Server-Betriebssysteme (Erfolg / Fehler)	Limitierte Liste namentlich bekannter Administratoren
Aktenvernichter in den Büroräumen	Berechtigungskonzepte je Anwendung
Persönliche Benutzerkonten	Zentrale Vergabe von Benutzerrechten über Rollenzuordnungen und Freigabe durch GF
Speicherung Zugangsdaten für privilegierten Zugriff in verschlüsseltem Passwortdepot	

1.4 Trennungskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
Strikte Trennung von Entwicklungs-, Test- und Produktivsystemen	Berechtigungskonzepte je Anwendung
Strikte Trennung von kundenspezifischen Systemen	

1.5 Pseudonymisierung / Anonymisierung

Technische Maßnahmen	Organisatorische Maßnahmen
	Verbot der Weitergabe personenbezogener Daten. Weitergabe nur nach schriftlicher Anweisung des Data Owners (Kunden)

2. Integrität

2.1 Weitergabekontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
Zugriff auf Daten ausschließlich über verschlüsselte Verbindungen nach aktuellem Stand der Technik (TLS, ssh, …)	Verbot der Übertragung der verarbeiteten Daten aus den geschützten Umgebungen.
Protokollierung des Zugriffes auf die Infrastruktur in den Audit-Logs der Server-Betriebssysteme	
Zugriff nur über VPN-Verbindungen und Bastion Hosts	
Verschlüsselung der Daten „At Rest"	

2.2 Eingangskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
	Änderung / Eingabe / Löschung von Kundendaten nur nach schriftlichem Auftrag durch den Data Owner, auch in elektronischer Form

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
Regelmäßige, automatische Sicherungen aller Daten außerhalb der jeweiligen Blast Area	Regelmäßige Überprüfungen der Backups / Recovery-Tests

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1 Datenschutz-Maßnahmen

Technische Maßnahmen	Organisatorische Maßnahmen
Zentrale Dokumentation aller Verfahren und Richtlinien zum Datenschutz und zur IT-Sicherheit in einem internen Wiki mit Zugriffsmöglichkeit für alle Mitarbeiter	Externer Datenschutzbeauftragter: Bitkom Servicegesellschaft mbH Albrechtstraße 10 10117 Berlin
Jährliche Überprüfung der Maßnahmen und Richtlinien	Mitarbeiter sind geschult und auf den Datenschutz verpflichtet
	Mindestens jährliche Sensibilisierung der Mitarbeiter durch den DSB

4.2 Incident-Response-Management

Technische Maßnahmen	Organisatorische Maßnahmen
Einsatz und regelmäßiges Update von Firewalls	Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
Einsatz und regelmäßige Aktualisierung von Viren-Scannern	Einbindung des DSB
Regelmäßiges Update / Patching von Betriebssystemen, mindestens monatlich	Dokumentation von Sicherheitsvorfällen in einem Ticketing-System (Jira)

4.3 Datenschutzfreundliche Voreinstellungen

Technische Maßnahmen	Organisatorische Maßnahmen
Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	

4.4 Auftragskontrolle (Outsourcing an Dritte)

Technische Maßnahmen	Organisatorische Maßnahmen
	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit
	Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standardvertragsklauseln