Dies ist ein Abgleich des Vertrag zur Auftragsverarbeitung von **Taskcards** mit der Prüfliste aus dem Dokument **Auftragsverarbeitung Orientierungshilfe** des Bayerischen Landesbeauftragte für den Datenschutz (https://www.datenschutz-bayern.de/technik/orient/oh_auftragsverarbeitung.pdf)

Prompt:
“*Gleiche den AVV von Taskcards mit der Checkliste ab. Tu dieses wie folgt. Repliziere die Checkliste in Form einer Tabelle und prüfe, ob das Kriterium erfüllt ist oder nicht. Unter Bemerkungen gib an, an welcher Stelle im AVV sich ein Beleg findet . Gib dazu die Nummer im AVV an, das Kapitel, den Absatz und ein Zitat/ Anfang des Textbeleges "Textbeleg ...". Wenn der Prüfpunkt nicht zutrifft, dann vermerke dies entsprechend unter Bemerkungen.*“

Das Dokument wird ergänzt durch technische und organisatorische Maßnahmen (TOM) - https://downloads.taskcards.de/docs/TaskCards_data_protection_concept_de_en.pdf

Bei der Prüfung des Vertrags zur Auftragsverarbeitung mittels KI auf der Grundlage des Prompts oben entstand eine Tabelle, welche aber einige offene Stellen hatte. Um diese zu ergänzen wurden im nächsten Schritt auch die TOM bei der Beantwortung der Fragen berücksichtigt.

*“Überprüfe, inwieweit die technische und organisatorische Maßnahmen von TaskCards die Aussagen/ fehlenden Aussagen des AVV ergänzen oder präzisieren. Überarbeitet die Tabelle und ergänze Informationen dann in eckigen Klammern mit Verweis auf die Fundstelle in den TOM und führe alles in einer Gesamttabelle zusammen.”*

---

Hier ist die zusammengeführte Gesamttabelle. Ich habe die Originalformulierungen aus der Bayern-Checkliste beibehalten und die Belege aus AVV sowie ergänzend aus den TOM in eckigen Klammern ergänzt.

| Frage | Ja | Nein | Anmerkungen |
|---|---|---|---|
| Erfolgte eine sorgfältige Auswahl des Auftragsverarbeiters? Bietet der Auftragsverarbeiter hinreichende Garantien dafür, dass die Datenverarbeitung durch geeignete technische und organisatorische Maßnahmen im Einklang mit den datenschutzrechtlichen Anforderungen erfolgt? | X | | AVV Anlage 1 verweist auf Testat und Sicherheitskonzept. Textbeleg AVV: „Die technischen und organisatorischen Sicherungsmaßnahmen werden durch das dem Vertrag beiliegende Testat … und dem Sicherheitskonzept nachgewiesen.“ [TOM: Gesamtkonzept aus Testat und spezifizierten TOM; „Beide Teile Zusammen bilden das Gesamtkonzept…“] |
| Liegen entsprechende Referenzen und/oder Zertifikate vor? | X | | AVV Anlage 1 nennt ISO/IEC 27001-Zertifizierungen u. a. für STRATO/OVH/billwerk. [TOM: Audit/Testat bestätigt TOM nach Art. 32 DSGVO; „TOM sind für den angestrebten Schutzzweck ausreichend“.] |
| Wird der Vertrag schriftlich bzw. in einem elektronischen Format geschlossen? | X | | AVV Nr. 1 Abs. 3: „Soweit Erklärungen im Folgenden ‚schriftlich‘ zu erfolgen haben…“[1] |

[1] Der Vertrag vom Anbieter **vorunterzeichnet** ist, kann davon ausgegangen werden, dass dieser damit seine Bereitschaft signalisiert, den Vertrag mit dem Auftraggeber einzugehen. Eine Rücksendung an den Auftragnehmer sollte von daher entfallen. Es findet sich zudem weder im Vertrag selbst noch an anderer Stelle ein Hinweis darauf, dass der Anbieter eine Rücksendung des Vertrags zur Auftragsverarbeitung erwartet, um diesen rechtskräftig mit dem Auftraggeber abzuschließen.

| | | |
|---|---|---|
| Bleibt die Verantwortung für die ausgelagerten Bereiche bzw. Tätigkeiten beim Verantwortlichen? | X | AVV Nr. 8 Abs. 1: „Für die Beurteilung der Zulässigkeit … sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.“ |
| Enthält der Vertrag genaue Bestimmungen zu Gegenstand der Verarbeitung? | X | AVV Nr. 2.1 „Gegenstand“: Leistungserbringung nach Nutzungsvertrag[2] für TaskCards.de und AVV Nr. 3.1 |
| Enthält der Vertrag genaue Bestimmungen zu Dauer der Verarbeitung? | X | AVV Nr. 2.2: Verarbeitung ab Erstregistrierung/Anmeldung bis Kündigung. |
| Enthält der Vertrag genaue Bestimmungen zu Art der Verarbeitung? | X | AVV Nr. 3.1: „Speicherung, Administration der Plattform, Pflege des Backend, Nutzerverwaltung, Prüfung, Löschen oder Vernichtung von Nutzerdaten.“ |
| Enthält der Vertrag genaue Bestimmungen zu Zweck der Verarbeitung? | X | AVV Nr. 3.1: „Zur Verfügung stellen der Plattform TaskCards im Rahmen eines Nutzungsvertrages…“ |

[2] Der Nutzungsvertrag dürfte inhaltlich den Nutzungsbedingungen unter https://taskcards.eu/de/nutzungsbedingungen/ entsprechen. Dort wird der Gegenstand der Verarbeitung genauer angegeben.

| | | |
|---|---|---|
| Enthält der Vertrag genaue Bestimmungen zu Art der personenbezogenen Daten? | X | AVV Nr. 3.2 nennt u. a. Personenstammdaten, Kommunikationsdaten, Vertragsstammdaten, Kundenhistorie, IP-Adresse/Browser, Abrechnungs- und Zahlungsdaten.[3] |
| Enthält der Vertrag genaue Bestimmungen zu Kategorien der betroffenen Personen? | X | AVV Nr. 3.3: Kunden, Interessenten, Beschäftigte, Lernende, Minderjährige, Ansprechpartner. |
| Enthält der Vertrag genaue Bestimmungen zu Rechten und Pflichten des Verantwortlichen? | X | AVV Nr. 8 „Rechte und Pflichten des Auftraggebers“. |
| Hat der Auftragsverarbeiter die Weisungsgebundenheit versichert? | X | AVV Nr. 4 Abs. 1: Verarbeitung ausschließlich wie vertraglich vereinbart oder angewiesen. |
| Hat der Auftragsverarbeiter zugesagt, die Weisungen des Verantwortlichen zu dokumentieren? | X | AVV Nr. 10 Abs. 5: „Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.“ |

[3] Diese Auflistung greift eigentlich etwas kurz, denn es geht ja auch um die mit Personen verknüpften Inhaltsdaten, welche in der Plattform verarbeitet werden. Damit gemeint sind die Inhalte, welche Nutzende in die Plattform eintragen oder hochladen. Da sie mit identifizierbaren Nutzen verbunden sind, sind sie in der Regel personenbezogen oder -beziehbar. Es gibt genauere Informationen dazu in den Einwilligungserklärungen für Lehrkräfte (https://downloads.taskcards.de/docs/Agreement_teacher_de.pdf) und Schülerinnen und Schüler (https://downloads.taskcards.de/docs/Agreement_pupil_de.pdf). Das Verfahrensverzeichnis (https://downloads.taskcards.de/docs/Template_LPA_de.pdf) bleibt hier genauso allgemein wie der AVV.

| | | | |
|---|---|---|---|
| Dürfen die im Rahmen der Auftragsverarbeitung verarbeiteten Daten ausschließlich zur Erfüllung der vertraglich vereinbarten Leistung verwendet werden (Gebot der Zweckbindung)? | X | | AVV Nr. 4 Abs. 1: „Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.” |
| Wurden dem Auftragsverarbeiter Bekanntgabe, Verkauf, Vermietung oder anderweitige Verwendung der Daten durch Dritte bzw. die kommerzielle Verwendung verboten? | X | | Im AVV nicht wörtlich als Verkauf/Vermietung formuliert, aber Zweckbindung/Eigennutzungsverbot. Textbeleg AVV Nr. 4 Abs. 1: keine anderen, insbesondere keine eigenen Zwecke. |
| Ist gewährleistet, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen? | X | | AVV Nr. 4 Abs. 4: schriftliche Verpflichtung zur Vertraulichkeit. [TOM: Verpflichtung von Mitarbeitern und Dienstleistern auf Vertraulichkeit.] |
| Wurden diese Personen auf das Datengeheimnis verpflichtet bzw. hingewiesen? | X | | AVV Nr. 4 Abs. 4: schriftliche Vertraulichkeitsverpflichtung. [TOM: Schulungsmaßnahmen und Vertraulichkeitsverpflichtung.] |
| Hat sich der Verantwortliche davon durch eine Einsicht in die Verpflichtungs-/Hinweiserklärungen überzeugt? | | X | Kein ausdrückliches Einsichtsrecht in einzelne Verpflichtungserklärungen gefunden. [TOM ergänzen Schulung/Verpflichtung, aber keine Einsicht in Erklärungen.] |

| | | |
|---|---|---|
| Wurden die Mitarbeiter des Auftragsverarbeiters bezüglich der Einhaltung des Datenschutzes und der Datensicherheit informiert und geschult? | X | AVV Nr. 4 Abs. 5: Personen werden mit Datenschutzbestimmungen vertraut gemacht. [TOM: Schulungen für Informationssicherheit und Datenschutz, neue Beschäftigte, Auffrischungen.] |
| Werden im Rahmen der Auftragsverarbeitung ausschließlich fachlich geeignete Mitarbeiter eingesetzt? | X | AVV regelt Schulung/Anleitung. [TOM: nur geschulte/kompetente Personen dürfen Administrationstätigkeiten durchführen; Rollen und Verantwortlichkeiten sind festgelegt.] |
| Wurde beim Auftragsverarbeiter ein betrieblicher/behördlicher Datenschutzbeauftragter bestellt? | X | AVV Nr. 4 Abs. 9 und Anlage 3: Datenschutzbeauftragter Karsten Greibel. |
| Sind dessen Kontaktdaten bekannt? | X | AVV Anlage 3 nennt Telefon und E-Mail: datenschutz@dsign-systems.net. |
| Wurden sowohl von Seiten des Verantwortlichen als auch des Auftragsverarbeiters verantwortliche Ansprechpartner zur Klärung eventuell auftretender fachlicher, technischer und organisatorischer Fragen benannt? | X | AVV Anlage 3 nennt weisungsberechtigte Personen/Ansprechpartner; auf Auftraggeberseite auszufüllen. |

| | | |
|---|---|---|
| Ist die Sicherheit der Datenverarbeitung angemessen gewährleistet (vgl. Art. 32 DSGVO), insbesondere mit Blick auf Pseudonymisierung und Verschlüsselung? | X | AVV Anlage 1 verweist auf TOM/Testat. [TOM: HTTPS TLS 1.2/1.3, verschlüsselte Verbindungen, Verschlüsselung mobiler Endgeräte.] |
| Ist die Sicherheit der Datenverarbeitung angemessen gewährleistet, insbesondere mit Blick auf Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste? | X | [TOM: Maßnahmen zu Vertraulichkeit, Zutrittskontrolle, Zugangskontrolle, Rollen/Rechte, Netzwerk, Business Continuity; Testat bestätigt ausreichende TOM.] |
| Ist die Sicherheit der Datenverarbeitung angemessen gewährleistet, insbesondere mit Blick auf Datenverfügbarkeit und Wiederherstellbarkeit? | X | [TOM: Business Continuity mit 3-2-1-Backup-Regel, täglichen Backup-Prüfungen und Wiederherstellungstests.] |
| Ist die Sicherheit der Datenverarbeitung angemessen gewährleistet, insbesondere mit Blick auf regelmäßige Überprüfung, Bewertung und Evaluierung der Sicherheitsmaßnahmen? | X | [TOM: „Regelmäßige Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen nach dem PDCA-Zyklus“.] |
| Wurden detaillierte Sicherheitsanforderungen erarbeitet? | X | AVV nur pauschal. [TOM: detaillierte Maßnahmenkataloge; Orientierung an CISIS12/EN ISO 27001; jährlicher bzw. anlassbezogener Verbesserungsprozess.] |

| | | | |
|---|---|---|---|
| Wurde daraufhin vom Auftragsverarbeiter ein entsprechendes Sicherheitskonzept entworfen und umgesetzt? | X | | AVV Anlage 1 verweist auf Sicherheitskonzept. [TOM: „Die Dokumente allgm_TOM_DSign und spez_TOM_WebApp_TaskCards stellen das vollständige Sicherheitskonzept der Anwendung dar.“] |
| Entspricht das Sicherheitskonzept den Anforderungen der Art. 32 ff. DSGVO? | X | | [TOM: Testat zur Sicherheit der Verarbeitung gemäß Art. 32 DSGVO; „TOM sind … ausreichend“.] |
| Wurde der Verantwortliche bei der Erstellung des Sicherheitskonzeptes einbezogen? | | X | Nicht ersichtlich. TOM beschreiben Konzept und Testat, aber keine Mitwirkung des Verantwortlichen bei der Erstellung.[4] |
| Wurden sowohl die Vorgehensweise bei Sicherheitsverletzungen als auch das Eskalationsverfahren gemeinsam festgelegt? | X | | AVV Nr. 9 regelt Meldepflichten. [TOM: „Vorhandensein von Eskalationsprozessen bei Sicherheitsverletzungen … im Notfallmanagement“.] |
| Werden revisionsfähige Aufzeichnungen über alle die Informationssicherheit betreffenden Vorkommnisse geführt? | X | | [TOM Nr. 1: „Konsequente Dokumentation bei Sicherheitsvorkommnissen (Security Reporting)“.][5] |

[4] Eine Mitwirkung an der Erstellung eines Sicherheitskonzeptes beim Auftragsverarbeiter durch den Auftraggeber ist in der Regel unüblich.
[5] Inwieweit die Aufzeichnungen revisionsfähig sind, geht aus den Unterlagen nicht hervor.

| | | | |
|---|---|---|---|
| Erfolgt eine regelmäßige Auswertung dieser Sicherheitsverletzungen? | X | | [TOM Nr. 1: Protokollierung mit regelmäßiger anlassloser Auswertung von Log-Dateien zur Erkennung ungewöhnlicher Einträge.] |
| Wird dieses Sicherheitskonzept regelmäßig hinsichtlich seiner Gültigkeit überprüft und gegebenenfalls neuen Sicherheitsanforderungen angepasst? | X | | AVV Nr. 5 Abs. 2 erlaubt Anpassung bei technischem/organisatorischem Fortschritt. [TOM: PDCA-Zyklus und regelmäßige Aktualisierung von Konzepten/Dokumentationen.] |
| Liegt dieses Sicherheitskonzept dem Verantwortlichen in schriftlicher Form vor? | X | | AVV Anlage 1 verweist auf beiliegendes Testat und Sicherheitskonzept. |
| Wurde dieses Sicherheitskonzept vom Verantwortlichen überprüft? | | X | Nicht belegt. Kontrollrechte bestehen, aber keine dokumentierte Prüfung des Sicherheitskonzepts durch den Verantwortlichen.[6] |
| Sind die Übermittlung bzw. Weitergabe von Daten und der Transport von Datenträgern vertraglich geregelt? | X | | AVV Nr. 5 Abs. 7 regelt mobile Datenträger. [TOM: mobile Datenspeicher, Verschlüsselung, Backup/Synchronisierung, Verlustregelungen.] |

[6] In der Regel sind Verantwortliche selten in der Lage, ein Sicherheitskonzept zu überprüfen. Sie könnten allenfalls Experten hinzuziehen, die das Sicherheitskonzept dann genauer untersuchen. Im Kontext Schule ist so etwas nicht zu erwarten, da die Kompetenzen weder in der Schule noch - in den meisten Fällen - beim Schulträger selbst vorliegen. Sie liegen allenfalls bei den großen kommunalen Dienstleistern und deren Experten vor.

| | | |
|---|---|---|
| Ist die Auslagerung von personenbezogenen Daten bzw. die Verschiebung von Dienstleistungen in das Ausland geregelt bzw. verboten? | X | AVV Nr. 4 Abs. 10: Verarbeitung grundsätzlich innerhalb der EU; AVV Nr. 7 Abs. 7: Subunternehmer außerhalb EU nicht gestattet. Anlage 2 nennt Deutschland/Frankreich/EWR. |
| Ist eine Pflicht des Auftragsverarbeiters vereinbart, dem Verantwortlichen die Einhaltung der datenschutzrechtlichen Anforderungen nachzuweisen und Überprüfungen zu ermöglichen? | X | AVV Nr. 8 Abs. 4–5: Kontrollrechte, Auskünfte, Nachweise, Stichproben. |
| Hängt die Vergabe von Unteraufträgen von der Genehmigung des Verantwortlichen ab bzw. kann er der Vergabe widersprechen? | X | AVV Nr. 7 Abs. 2: Subunternehmer nur mit schriftlicher Zustimmung des Auftraggebers.[7] |
| Unterliegt ein Unter-Auftragsverarbeiter den gleichen datenschutzrechtlichen Anforderungen wie der Auftragsverarbeiter? | X | AVV Nr. 7 Abs. 3: vergleichbare Datenschutzpflichten; Einsicht in Verträge auf Verlangen. |

[7] Das ist eine der Möglichkeiten, wie das geregelt werden kann. Die andere ist die, dass der Auftragnehmer den Auftraggeber informiert und der eine Frist von mehreren Wochen zum Widerspruch erhält. In der Praxis kommt es sehr selten vor, dass alle Auftragnehmer eine schriftliche Einwilligung erteilen müssen. Wenn ein Auftraggeber die Einwilligung nicht erteilt, bleibt letztlich nur die Beendigung des Vertragsverhältnisses, was aber in keinem (mir) aus der schulischen Praxis bekannten Fall bisher vorgekommen ist.

| | | |
|---|---|---|
| Ist eine Pflicht des Auftragsverarbeiters zur Unterstützung des Verantwortlichen hinsichtlich der Betroffenenrechte vereinbart? | X | AVV Nr. 4 Abs. 7–8: Unterstützung bei geltend gemachten Rechten, Anfragen werden weitergeleitet. |
| Ist der Auftragsverarbeiter vertraglich verpflichtet, den Verantwortlichen bei Einhaltung seiner Pflichten aus Art. 32 bis 36 DSGVO zu unterstützen? | X | AVV Nr. 9 Abs. 4: Unterstützung bei Pflichten nach Art. 33 und 34 DSGVO; Nr. 4 Abs. 6 unterstützt bei VVT und DSFA. |
| Ist eine Pflicht zur Löschung bzw. Rückgabe der Daten nach Beendigung des Auftrags vereinbart? | X | AVV Nr. 11 Abs. 1–3: Daten nach Wahl des Auftraggebers vernichten oder übergeben; Nachweis der Vernichtung. |
| Sind Zurückbehaltungsrechte hinsichtlich der Daten und Datenträger ausgeschlossen? | X | AVV Nr. 14 Abs. 4: Zurückbehaltungsrecht hinsichtlich Daten und Datenträger ausgeschlossen. |
| Sind die Daten vor dem Zugriff Dritter sicher (z. B. Pfändung, Beschlagnahme)? | X | AVV Nr. 14 Abs. 2: bei Gefährdung durch Maßnahmen Dritter, Insolvenz etc. unverzügliche Verständigung des Auftraggebers. |
| Kann die Aufgabenerfüllung seitens des Verantwortlichen auch im Falle eines Vertragsendes, Vertragsbruches, Geschäftsaufgabe, Insolvenz usw. sichergestellt werden? | Teilweise | AVV regelt Rückgabe/Löschung und Informationspflicht bei Gefährdung. [TOM: Business Continuity/Backups ergänzen Verfügbarkeit; keine vollständige Exit-/Insolvenzstrategie ersichtlich.] |

| | | | |
|---|---|---|---|
| Sind Beginn, Mindestdauer und Ende des Vertrages eindeutig geregelt? | Teilweise | | AVV Nr. 2.2 regelt Beginn und Ende; Mindestdauer nicht ausdrücklich.[8] |
| Kann der Vertrag unter Einhaltung einer entsprechenden Kündigungsfrist beendet werden? | X | | AVV Nr. 2.2: bis Kündigung dieses Vertrags oder Hauptvertrags; Sonderkündigung in Nr. 13. |
| Kann eine Vertragsauflösung bei krassen Vertragsverletzungen erfolgen? | X | | AVV Nr. 13 Abs. 1–2: außerordentliche Kündigung bei schwerwiegendem Datenschutzverstoß, Nichtbefolgung rechtmäßiger Weisung oder verweigerten Kontrollrechten. |
| Wurden der Auftragsverarbeiter und das von ihm beschäftigte Personal dazu verpflichtet, alle im Rahmen der Auftragsverarbeitung erworbenen Kenntnisse und Informationen auch nach Vertragsauflösung vertraulich zu behandeln? | X | | AVV Nr. 14 Abs. 1: Vertraulichkeit auch über Vertragsende hinaus. „... Auch über die Beendigung des Vertrages vertraulich zu behandeln.” |
| Ist geregelt, welches Gericht in Streitfällen anzurufen ist und welches Recht dabei zur Anwendung kommt? | | X | Keine entsprechende Regelung gefunden. TOM ergänzen dies nicht.[9] |

[8] Der AVV regelt Beginn und Ende nur allgemein („ab Erstregistrierung“ bis Kündigung). Die Nutzungsbedingungen konkretisieren dies erheblich: § 9 regelt Laufzeitmodelle von „1 Monat oder 1 Jahr“, automatische Verlängerung, Kündigungsfristen sowie Mindestvertragslaufzeiten („frühestens zum Ende der vereinbarten Mindestvertragslaufzeit“). Die FAQ ergänzen dies weiter: Kündigung beim Jahresmodell 1 Monat vor Ablauf, beim Monatsmodell bis einen Tag vor Ablauf möglich.

[9] Weder AVV noch Nutzungsbedingungen enthalten eine ausdrückliche Gerichtsstands- oder Rechtswahlklausel. Da die dSign Systems GmbH mit Sitz in Schmalkalden ein deutscher Anbieter ist, kann man ohne Zweifel davon ausgehen, dass der Gerichtsstandort natürlich Deutschland ist und deutsches Recht gilt.

| | | |
|---|---|---|
| Ist die Örtlichkeit der Datenhaltung beim Auftragsverarbeiter eindeutig bestimmt und schriftlich festgehalten? | X | AVV Anlage 1/2 nennt Orte der Verarbeitung: Deutschland, Frankreich/EWR. [TOM: TaskCards wird auf Servern ausgewählter Hostinganbieter betrieben; STRATO und OVH genannt.] |
| Ist die Zugangskontrolle am Ort der Auftragsverarbeitung gewährleistet? | X | AVV verweist auf TOM. [TOM: Sicherheitsbereiche, Zutrittsschutz, Protokollierung des Zutritts, Zutrittsberechtigungen, Begleitung von Fremdpersonal, Überwachung der Räume.] |
| Ist die Zugriffsrechtevergabe auf eventuell ausgelagerte Datenbestände revisionsfähig geregelt und dokumentiert? | X | [TOM: Rollen-/Rechtekonzept, Rollenprofile, Zuweisung/Entzug, regelmäßige Überprüfung, Verwaltung nur durch Administratoren.] |
| Existieren Vorgaben bezüglich der Benutzereinrichtung, der Änderung von Benutzerberechtigungen und der Vorgehensweise bei einem Ausscheiden von Benutzern? | Teilweise | [TOM: Rollenverwaltung mit Zuweisung/Entzug und regelmäßiger Überprüfung; ausdrücklicher Ausscheidensprozess nicht gesondert belegt.] |
| Wurden und werden geeignete Maßnahmen zur Gewährleistung der Zugangs- und Zugriffskontrolle ergriffen? | X | [TOM: eindeutige Kennungen, Vermeidung von Gruppenkennungen, starke Passwörter, automatische Sperrung bei Fehlversuchen, keine Klartextspeicherung, bcrypt mit Salt.] |

| | | |
|---|---|---|
| Ist gewährleistet, dass jeder Beschäftigte des Auftragsverarbeiters nur auf die Daten des Verantwortlichen zugreifen darf, die er zur Erfüllung seiner Aufgaben benötigt? | X | [TOM: „Nutzer sollen nur auf die personenbezogenen Daten zugreifen können, die für ihre Tätigkeit erforderlich sind.“ Rollen-/Rechtekonzept.] |
| Sind besonders schützenswerte Daten durch organisatorische und technische Maßnahmen vor einer Einsichtnahme durch das Personal des Auftragsverarbeiters geschützt? | Teilweise | [TOM: Verschlüsselung mobiler Endgeräte, rollenbasierte Zugriffe, Zugriffskontrolle. Eine generelle verschlüsselte Datenspeicherung aller Inhaltsdaten vor Einsichtnahme durch Personal ist nicht eindeutig belegt.][10] |
| Wurden bzw. werden Maßnahmen zur Notfallvorsorge festgelegt und ergriffen? | X | [TOM: Business Continuity, 3-2-1-Backup-Regel, tägliche Backups, Wiederherstellungstests, Schutz gegen Ransomware.] |
| Liegt ein detailliertes Notfallkonzept vor? | Teilweise | [TOM: Eskalationsprozesse bei Sicherheitsverletzungen und Business-Continuity-Maßnahmen vorhanden; ein eigenständiges detailliertes Notfallhandbuch ist nicht eindeutig belegt, wird aber erwähnt „Vorhandensein von Eskalationsprozessen bei Sicherheitsverletzungen (Wer ist wann wie zu informieren?), u. a. im Notfallmanagement.] |

[10] Der Punkt ist bezüglich Task Cuts eigentlich auch nicht wirklich relevant, da in der Plattform keine besonders schützenswerten Daten verarbeitet bzw. gespeichert werden sollten.

| | | | |
|---|---|---|---|
| Wird dieses Notfallkonzept regelmäßig auf Aktualität und Angemessenheit überprüft und getestet? | Teilweise | | [TOM: PDCA-Zyklus und regelmäßige Tests der Wiederherstellung; bezogen auf Backups ja, als vollständiges Notfallkonzept nur teilweise belegt.] |
| Ist die Aufbewahrungsdauer von Daten und Datenträgern beim Auftragsverarbeiter geregelt? | X | | [TOM: Archivierung: Regelungen, welche Daten auf welcher Rechtsgrundlage wie lange aufzubewahren sind.] |
| Wurden dabei die gesetzlichen Anforderungen berücksichtigt? | X | | [TOM Nr. 11: Archivierung knüpft an Rechtsgrundlagen und Aufbewahrungsfristen an.] |
| Sind die Rückgabe der Daten(träger) und Unterlagen vertraglich geregelt? | X | | AVV Nr. 11 Abs. 1: Vernichtung oder Übergabe nach Wahl des Auftraggebers; Abs. 2 auch bei Subunternehmern. |
| Wurden und werden die betroffenen Personen bezüglich der Auslagerung ihrer Daten bzw. der Datenverarbeitung informiert? | | X | Keine Regelung im AVV/TOM, die eine Information der Betroffenen durch TaskCards belegt. Verantwortung liegt nach AVV beim Auftraggeber.[11] |
| Sind die Rechte der betroffenen Personen v. a. bezüglich Auskunft, Berichtigung und Löschung im Rahmen der Auftragsverarbeitung gewährleistet? | X | | AVV Nr. 4 Abs. 7–8: Unterstützung bei Betroffenenrechten; Auskünfte nur nach Zustimmung, Anfragen werden weitergeleitet. |

[11] Hier um mögliche andere Unterauftragsverarbeiter oder eine Auslagerung der Datenverarbeitung in einen Drittstaat. Letzteres ist aber nach den verschiedenen Aussagen des Anbieters nicht deren Konzept.

| | | | |
|---|---|---|---|
| Erfolgt eine regelmäßige Kontrolle der Auftragsverarbeitung durch den Verantwortlichen? | Teilweise | | AVV Nr. 8 Abs. 4–5 enthält Kontrollrechte; keine Pflicht des Verantwortlichen zur regelmäßigen Kontrolle. [TOM: Audits/Testate und regelmäßige Überprüfung der TOM.][12] |
| Werden die Ergebnisse der Auftragsverarbeitung zumindest stichprobenartig auf Richtigkeit überprüft? | X | | AVV Nr. 8 Abs. 5: Bei Nachweis der korrekten Umsetzung sollen Kontrollen auf Stichproben beschränkt werden. |
| Ist der Auftragsverarbeiter dazu verpflichtet, den Verantwortlichen schriftlich über Verfahrensveränderungen und Probleme zu informieren? | X | | AVV Nr. 5 Abs. 2–3: Änderungen bez. Datensicherheitsmaßnahmen und unzureichende Sicherheitsmaßnahmen sind mitzuteilen; Wesentliche Änderungen müssen vereinbart werden mit dem Auftraggeber. Nr. 9: Meldung von Datenschutzverletzungen/Störungen. |
| Informiert der Verantwortliche den Auftragsverarbeiter über Veränderungen von vertragsrelevanten Vorhaben und Daten, zum Beispiel bei Veränderungen gesetzlicher Grundlagen? | | X | Keine ausdrückliche Regelung gefunden.[13] |

[12] In der Praxis sind solche Kontrollen beim Auftragnehmer durch den Auftraggeber selbst unüblich und übersteigen darüber hinaus auch die Kompetenzen des Auftraggebers. Bei größeren Auftraggebern wie Behörden und größeren Unternehmen verlässt man sich in der Regel auf Zertifikate und Audits durch Dritte.

[13] Der Punkt ist eher unerheblich, denn gem. AVV Nr. 8 Abs. 1 ist zunächst der Verantwortliche zuständig, wenn es eine Veränderung gesetzlicher Grundlagen, beispielsweise im Schulrecht, gibt.: „Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich."