Anlage 3: Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO

Berliner Abendblatt Medienhaus GmbH — ViralSpoon Social Media Service

Stand: Juli 2026

Berliner Abendblatt Medienhaus GmbH

Müllerstraße 12, 13353 Berlin

Der vorliegende Auftragsverarbeitungsvertrag (AVV) gilt für die Verarbeitungsmaßnahmen personenbezogener Daten durch die Berliner Abendblatt Medienhaus GmbH (auch als Auftragnehmer bezeichnet), die gegenüber Kunden (nachfolgend Auftraggeber oder Sie) in Erfüllung des Hauptvertrages erbracht werden. Berliner Abendblatt Medienhaus GmbH verarbeitet personenbezogene Daten als Auftragnehmer des Kunden. Berliner Abendblatt Medienhaus GmbH ist berechtigt, die ViralSpoon GmbH als Unterauftragnehmer für Betrieb, Hosting, KI-Funktionen, Social-Media-Management und technische Plattformleistungen einzusetzen.

Präambel

Der Auftragnehmer erbringt für den Auftraggeber Leistungen gemäß dem zwischen ihnen geschlossenen Lizenzvertrag über die Nutzung von ViralSpoon (im Folgenden Hauptvertrag). Teil der Durchführung des Hauptvertrags ist die Verarbeitung von personenbezogenen Daten im Sinne der DSGVO. Zur Erfüllung der DSGVO-Anforderungen schließen die Parteien den nachfolgenden Auftragsverarbeitungsvertrag, der mit Unterzeichnung bzw. Wirksamwerden des Hauptvertrages zustande kommt.

1. Gegenstand / Umfang der Beauftragung

(1) Im Rahmen der Zusammenarbeit der Parteien nach Maßgabe des Hauptvertrages hat der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers (nachfolgend Auftraggeberdaten). Diese Auftraggeberdaten verarbeitet der Auftragnehmer im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 4 Nr. 8 und Art. 28 DSGVO.

(2) Die Verarbeitung der Auftraggeberdaten erfolgt in der in den Anlagen beschriebenen Art sowie in dem dort spezifizierten Umfang und Zweck. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.

(3) Ob die Leistungen des Auftragnehmers für die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO geeignet sind, bedarf einer Risikobewertung durch den Auftraggeber.

(4) Dem Auftragnehmer ist eine von den in den Anlagen genannten Verarbeitungen abweichende Verarbeitung von Auftraggeberdaten untersagt — unbeschadet der in Abschnitt 2 geregelten eigenverantwortlichen Verarbeitungen.

(5) Die Verarbeitung der Auftraggeberdaten findet grundsätzlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der EU oder in einem anderen Vertragsstaat des EWR statt. Sollte es eine Verlagerung in ein Drittland geben, bedarf dies der vorherigen Zustimmung des Auftraggebers und erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind. Der Auftraggeber stimmt bereits mit Abschluss dieses AVV der Verarbeitung personenbezogener Daten durch die in den Anlagen genannten Subunternehmen zu.

(6) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen.

2. Abgrenzung der datenschutzrechtlichen Rollen

(1) Die datenschutzrechtliche Rollenverteilung folgt der tatsächlichen Bestimmung von Zweck und Mitteln der jeweiligen Verarbeitung.

(2) Der Auftragnehmer und der von ihm eingesetzte technische Plattformpartner (ViralSpoon GmbH) verarbeiten personenbezogene Daten als Auftragsverarbeiter im Sinne des Art. 28 DSGVO, soweit die Verarbeitung ausschließlich der Erbringung der gegenüber dem Auftraggeber geschuldeten Leistung dient, insbesondere dem Anlegen und Verwalten des Kundenaccounts, der Speicherung und Verarbeitung der vom Auftraggeber eingegebenen Inhalte sowie der Erstellung, Planung und Veröffentlichung der Beiträge. Für diese Verarbeitung gelten die Regelungen dieses Auftragsverarbeitungsvertrages.

(3) Soweit personenbezogene Daten zu eigenen Zwecken des Auftragnehmers oder des technischen Plattformpartners verarbeitet werden, handeln diese insoweit als eigene Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO und nicht als Auftragsverarbeiter. Dies betrifft insbesondere folgende Zwecke: (a) Gewährleistung von Betrieb, Sicherheit, Stabilität und Verfügbarkeit der Plattform; (b) Erkennung und Abwehr von Missbrauch, Betrug und Sicherheitsvorfällen; (c) Analyse, Wartung, Fehlerbehebung sowie Weiterentwicklung und Verbesserung der Plattform und ihrer Funktionen; (d) Test, Validierung, Fehleranalyse und Verbesserung der Plattformfunktionen, soweit hierfür keine Kundeneingaben, Bilder, Videos, Unternehmensinformationen oder sonstigen Inhaltsdaten zum Training externer KI-Modelle verwendet werden. Eine Nutzung solcher Inhaltsdaten zum Training externer KI-Modelle findet nicht statt. Eine interne Verbesserung der Plattform erfolgt nur anhand aggregierter, anonymisierter oder technisch erforderlicher Nutzungs-, Fehler- und Sicherheitsdaten, soweit rechtlich zulässig.

(4) Bei Verarbeitungen nach Absatz 3 werden angemessene Schutzmaßnahmen ergriffen, insbesondere Pseudonymisierung oder Aggregation, soweit der jeweilige Zweck dies zulässt. Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO. Diese Verarbeitungen werden in den Datenschutzhinweisen (Anlage 4) transparent dargestellt.

(5) Die Regelungen dieses Auftragsverarbeitungsvertrages finden auf Verarbeitungen nach Absatz 3 keine Anwendung. Das Weisungsrecht des Auftraggebers bezieht sich ausschließlich auf Verarbeitungen nach Absatz 2.

3. Weisungsbefugnisse des Auftraggebers

(1) Der Auftragnehmer verarbeitet die Auftraggeberdaten im Rahmen der Beauftragung und im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung) — unbeschadet der Regelung in Abschnitt 2 dieses AVV, der den Anwendungsbereich der Auftragsverarbeitung abgrenzt. Der Auftraggeber hat das alleinige Recht, Weisungen über Art, Umfang und Methode der Verarbeitungstätigkeiten zu erteilen.

(2) Weisungen werden grundsätzlich schriftlich oder in elektronischer Form erteilt; mündlich erteilte Weisungen sind vom Auftragnehmer in elektronischer Form zu bestätigen.

(3) Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber darauf hinzuweisen und ist berechtigt, die Durchführung so lange auszusetzen, bis diese bestätigt oder geändert wird.

4. Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben. Unterlagen und Daten sind gegen Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer verpflichtet alle mit der Verarbeitung betrauten Personen zur Vertraulichkeit gemäß Art. 28 Abs. 3 lit. b DSGVO.

(3) Der Auftragnehmer verpflichtet sich, alle geeigneten technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO, insbesondere die in AVV-Anhang B aufgeführten Maßnahmen, zu ergreifen und aufrechtzuerhalten.

(4) Eine Änderung der TOM bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(5) Auf Verlangen des Auftraggebers wird der Auftragnehmer die Einhaltung der technischen und organisatorischen Maßnahmen nachweisen.

(6) Der Auftragnehmer und die bei oder für ihn Beschäftigten sind berechtigt, die Leistungen aus der Hauptverwaltung, Betriebsstätten, Niederlassungen oder aus dem Home- und Mobile-Office zu erbringen, sofern die Schutzmaßnahmen dieses AVV eingehalten werden.

5. Informations- und Unterstützungspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder sicherheitsrelevante Vorfälle wird der Auftragnehmer den Auftraggeber unverzüglich, spätestens innerhalb von 48 Stunden in Schrift- oder elektronischer Form informieren. Die Meldungen sollen die in Art. 33 Abs. 3 DSGVO genannten Angaben enthalten.

(2) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung seiner Aufklärungs-, Abhilfe- und Informationsmaßnahmen im Rahmen des Zumutbaren.

(3) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle erforderlich sind.

6. Sonstige Verpflichtungen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, sofern die Voraussetzungen des Art. 30 DSGVO zutreffen, ein Verzeichnis aller Kategorien von im Auftrag des Auftraggebers durchgeführten Verarbeitungstätigkeiten zu führen und dem Auftraggeber auf Verlangen zur Verfügung zu stellen.

(2) Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Erstellung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO zu unterstützen.

(3) Der Auftragnehmer bestätigt, dass er — soweit eine gesetzliche Verpflichtung besteht — einen Datenschutzbeauftragten bestellt hat.

(4) Sollten die Auftraggeberdaten beim Auftragnehmer durch Pfändung, Beschlagnahme oder Insolvenzverfahren gefährdet werden, informiert der Auftragnehmer den Auftraggeber unverzüglich, sofern nicht durch Anordnung untersagt.

7. Subunternehmerverhältnisse

(1) Der Auftragnehmer darf die Verarbeitung ganz oder teilweise durch weitere Auftragsverarbeiter (Unterauftragnehmer) erbringen lassen. Er informiert den Auftraggeber rechtzeitig vorab in Textform. Der Auftraggeber kann bei sachlichen Gründen innerhalb von vier Wochen nach Kenntnisnahme widersprechen.

(2) Kein Subunternehmerverhältnis liegt vor bei reinen Nebenleistungen wie Post-, Transport-, Reinigungs- oder Bewachungsleistungen.

(3) Der Auftragnehmer vereinbart mit Unterauftragnehmern die Regelungen dieses AVV inhaltsgleich; insbesondere müssen die TOM ein gleichwertiges Schutzniveau aufweisen.

(4) Der Auftragnehmer hat mit den in AVV-Anhang A genannten Unternehmen Subunternehmerverhältnisse begründet, denen der Auftraggeber mit Abschluss dieses AVV zustimmt. Neue Unterauftragnehmer werden in AVV-Anhang A eingetragen. Bei Widerspruch des Auftraggebers innerhalb von 3 Wochen ist der Auftragnehmer berechtigt, den Hauptvertrag innerhalb von 1 Woche zu kündigen, sollte keine alternative Lösung gefunden werden.

(5) Mit den Unterauftragnehmern hat der Auftragnehmer dem Abschnitt Subunternehmerverhältnisse entsprechende Auftragsverarbeitungsverträge geschlossen. Mit Wirksamwerden dieses AVV genehmigt der Auftraggeber die vorgenannten Unterauftragnehmer.

(6) Bestandteil der Auftragsverarbeitungsverträge mit den Unterauftragnehmern ist insbesondere, dass diese sicherstellen, angemessene und geeignete TOM nach Art. 32 DSGVO getroffen zu haben.

8. Kontrollrechte

(1) Der Auftraggeber ist berechtigt, sich regelmäßig von der Einhaltung der Regelungen dieses Vertrages zu überzeugen, z. B. durch Auskünfte, Vorlage von Zertifizierungen oder persönliche Prüfung zu den üblichen Geschäftszeiten durch einen sachkundigen Dritten, der nicht im Wettbewerb zum Auftragnehmer steht.

(2) Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und angemessene Rücksicht auf die Betriebsabläufe nehmen.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Erforderliche Verfahrensänderungen werden unverzüglich mitgeteilt.

9. Rechte Betroffener

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung seiner Pflichten nach Art. 12 bis 22 sowie Art. 32 bis 36 DSGVO und gibt dem Auftraggeber unverzüglich, spätestens innerhalb von 14 Werktagen, die gewünschte Auskunft.

(2) Macht ein Betroffener Rechte gemäß Art. 16 bis 18 DSGVO geltend, ist der Auftragnehmer verpflichtet, auf Weisung des Auftraggebers unverzüglich, spätestens binnen 7 Werktagen, zu berichtigen, zu löschen oder einzuschränken.

(3) Macht ein Betroffener Rechte unmittelbar gegenüber dem Auftragnehmer geltend, leitet dieser das Ersuchen an den Auftraggeber weiter und wartet dessen Weisungen ab.

10. Laufzeit und Kündigung

Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Er endet automatisch mit Beendigung des Hauptvertrags. Sollte der Auftragnehmer vor Ablauf des Hauptvertrages keine Auftraggeberdaten mehr verarbeiten, endet dieser Vertrag ebenfalls automatisch.

11. Löschung und Rückgabe nach Vertragsende

(1) Der Auftragnehmer gibt nach Beendigung des Hauptvertrags alle ihm überlassenen Unterlagen, Daten und Datenträger zurück oder löscht diese auf Wunsch des Auftraggebers vollständig und unwiderruflich, sofern nicht gesetzliche Aufbewahrungsfristen entgegenstehen. Dokumentationen zum Nachweis ordnungsgemäßer Verarbeitung sind 6 Monate aufzubewahren.

(2) Der Auftragnehmer bestätigt die Löschung elektronisch. Der Auftraggeber hat das Recht, die vollständige Rückgabe bzw. Löschung zu kontrollieren.

(3) Der Auftragnehmer ist verpflichtet, auch nach Vertragsende die bekannt gewordenen Daten vertraulich zu behandeln.

12. Haftung

(1) Die Haftung der Parteien richtet sich nach Art. 82 DSGVO. Eine Haftung des Auftragnehmers gegenüber dem Auftraggeber wegen Verletzung von Pflichten aus diesem Vertrag bleibt unberührt.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand verantwortlich ist, durch den der Schaden eingetreten ist.

13. Vertraulichkeit und Datengeheimnis

(1) Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen.

(2) Es besteht eine Verschwiegenheitspflicht für Mitarbeiter des Auftragnehmers und durch ihn beauftragte Dritte gemäß Art. 28 Abs. 3 lit. b DSGVO.

(3) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind und er die beschäftigten Mitarbeiter auf die Einhaltung der Datenschutzvorschriften verpflichtet.

(4) Die Verschwiegenheitspflichten bestehen auch nach Beendigung des Vertragsverhältnisses fort.

(5) Der Auftragnehmer ist verpflichtet, alle im Rahmen der Leistungserbringung erlangten Informationen und Daten geheim zu halten und nicht an Dritte weiterzugeben.

14. Schlussbestimmungen

(1) Die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der zu verarbeitenden Daten ist ausgeschlossen.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der elektronischen Form.

(3) Die Regelungen dieses Vertrags gehen im Zweifel den Regelungen des Hauptvertrags vor. Unwirksame Bestimmungen werden durch wirtschaftlich gleichwertige Regelungen ersetzt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist der Sitz des Auftragnehmers (Berlin).

Festlegungen zum Vertrag

Gegenstand und Dauer des Auftrages — Übersicht der Anforderungen und Festlegungen	
(1) Hauptvertrag	Lizenzvertrag
(2) Gegenstand des Auftrages	Vollumfassende, plattformübergreifende und KI-gestützte Software zur Erledigung des Social-Media-Managements — von der Planung bis zum Post der Beiträge.
(3) Zweck der Datenverarbeitung	Zur Erfüllung der Pflichten des Auftragnehmers aus dem Hauptvertrag werden personenbezogene Daten aus dem Herrschaftsbereich des Auftraggebers vollumfänglich i.S.d. Art. 4 Nr. 2 DSGVO verarbeitet (insbesondere erhoben, gespeichert, verändert, ausgelesen, verwendet, offengelegt, abgeglichen und gelöscht). Der Zweck der Verarbeitung hängt von dem jeweils im Hauptvertrag beschriebenen Auftrag ab.
(4) Art der Daten	Stammdaten (z.B. Namen, Anschriften, Geburtsdaten) Kontaktdaten (z.B. E-Mail-Adressen, Telefonnummern) Inhaltsdaten (z.B. Fotografien, Videos, Inhalte von Dokumenten) Vertragsdaten (z.B. Vertragsgegenstand, Laufzeiten, Kunden) Zahlungsdaten (z.B. Bankverbindungen, Zahlungsdienstleister) Nutzungsdaten (z.B. Verlauf Web-Dienste, Zugriffszeiten) Verbindungsdaten (z.B. Geräte-ID, IP-Adressen, URL-Referrer) Standortdaten (z.B. GPS-Daten, IP-Geolokalisierung)
(5) Kreis der Betroffenen	Beschäftigte Auszubildende und Praktikanten Bewerber ehemalige Arbeitnehmer freie Mitarbeiter Gesellschafter, Organe der Gesellschaft Kunden / Interessenten Lieferanten und Dienstleister Geschäftspartner externe Berater Besucher Pressevertreter

AVV-Anhang A: Unterauftragnehmer (Subprozessoren)

Stand: Juli 2026. Wesentliche Änderungen werden dem Auftraggeber gemäß Abschnitt 7 dieses AVV rechtzeitig mitgeteilt.

Dienstleister	**Leistung**	**Standort / Zertifizierung**
Vercel Inc.	Hosting / Serverless Compute (Anwendungsbetrieb + Analytics)	EU-Region Frankfurt am Main — SOC 2 Type II, ISO 27001
Neon Inc.	Managed-Datenbank (PostgreSQL)	EU-Region Frankfurt am Main — SOC 2 Type II

Dienstleister	Leistung	Standort / Zertifizierung
OpenAI Ireland Ltd.	KI-Textverarbeitung	EU Data Boundary (Deutschland, Irland, Niederlande)
Anthropic Ireland Ltd.	KI-Textverarbeitung	EU Data Boundary
Google Ireland Ltd.	KI-Textverarbeitung	Finnland, Niederlande, Irland, Belgien
Cloudflare, Inc.	CDN, Web Application Firewall, Objekt-Storage (R2) — primärer Speicher für Mediendateien	EU-Region (Edge-Standorte in mehreren EU-Mitgliedstaaten, u. a. Frankfurt am Main) — ISO 27001, SOC 2 Type II
Upstash, Inc.	Cache, Rate-Limiting (Redis), Message Queue (QStash)	EU-Region Frankfurt am Main — SOC 2 Type II
Resend, Inc.	Transaktionaler E-Mail-Versand (System-Benachrichtigungen)	EU-Region Frankfurt am Main — SOC 2 Type II
Pusher Ltd.	Realtime-Kommunikation (WebSockets) für die UI-Synchronisation	EU/UK-Region — Datenschutz gemäß Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 DSGVO; bei Wegfall Ersatz durch geeignete Garantien gem. Art. 46 DSGVO
Microsoft Ireland Operations Limited	Identity- und Collaboration-Dienste (Microsoft 365 / Entra ID) — ausschließlich für interne ViralSpoon-Mitarbeitenden-Identitäten, keine Verarbeitung von Endkundendaten	EU-Region (Niederlande, Irland) — ISO 27001, SOC 2 Type II
GitHub B.V. (Mutterkonzern: GitHub, Inc., USA)	Source-Code-Hosting der ViralSpoon-Anwendung — verarbeitet ausschließlich Anwendungs-Quellcode, keine Endkundendaten	EU/USA — ISO 27001, SOC 2 Type II

AVV-Anhang B: Technische und organisatorische Maßnahmen (TOM)

Hinweis zur Umsetzung der technischen und organisatorischen Maßnahmen

Die nachfolgenden technischen und organisatorischen Maßnahmen werden je nach Verantwortungsbereich durch die Berliner Abendblatt Medienhaus GmbH als Auftragnehmer, durch die ViralSpoon GmbH als eingesetzten technischen Plattform- und Unterauftragnehmer sowie durch die jeweils eingesetzten Subprozessoren umgesetzt.

Soweit Maßnahmen den technischen Betrieb der ViralSpoon-Plattform, Hosting, Datenbanken, KI-Funktionen, Social-Media-Schnittstellen, Logging, Verschlüsselung, Backup, Zugriffskontrollen oder sonstige Plattform- und Infrastrukturleistungen betreffen, werden diese ganz oder teilweise durch die ViralSpoon GmbH und/oder deren Subprozessoren umgesetzt.

Die Berliner Abendblatt Medienhaus GmbH stellt im Rahmen ihrer Verantwortlichkeit als Auftragnehmer sicher, dass die eingesetzten Unterauftragnehmer auf ein angemessenes Schutzniveau verpflichtet werden und die in diesem Anhang beschriebenen Maßnahmen insgesamt ein dem Risiko angemessenes Schutzniveau gemäß Art. 32 DSGVO gewährleisten.

Verantwortliche für die Datenverarbeitung sind gemäß Art. 32 DSGVO verpflichtet, technische und organisatorische Maßnahmen zu treffen, durch die die Sicherheit der Verarbeitung personenbezogener Daten gewährleistet wird. Diese Übersicht erläutert, welche konkreten Maßnahmen durch den Auftragnehmer im Hinblick auf die Verarbeitung personenbezogener Daten getroffen sind.

Weisungen zu technischen und organisatorischen Maßnahmen	
1. Organisation der Informationssicherheit *Es sind Richtlinien, Prozesse und Verantwortlichkeiten festzulegen, mit denen die Informationssicherheit implementiert und kontrolliert werden kann.* *Primärer Umsetzungsbereich: Berliner Abendblatt Medienhaus GmbH und ViralSpoon GmbH, jeweils für den eigenen Organisations- und Verantwortungsbereich.* **Maßnahmen:** **x** Festlegung der Rollen und Verantwortlichkeiten für Betrieb von Anwendungen und System, Datenschutz und Informationssicherheit.	**Weitere umgesetzte Maßnahmen / Erläuterungen:** Durch vollständig cloudbasiertes Arbeiten ist kein Prozess für die Verwaltung und Entsorgung von Datenträgern erforderlich.

Weisungen zu technischen und organisatorischen Maßnahmen	
x Verpflichtung der Mitarbeiter auf Geheimhaltung und Wahrung des Datengeheimnisses. **x** Regelmäßige Durchführung von Schulungen und Awareness-Maßnahmen.	
2. Privacy by Design *Systeme sollen so konzipiert sein, dass der Umfang der verarbeiteten personenbezogenen Daten minimiert wird.* **Maßnahmen:** **x** Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind. **x** Die Verarbeitungen und Systeme sind so konzipiert, dass sie ein DSGVO-konformes Löschen der personenbezogenen Daten ermöglichen und sicherstellen.	**Weitere umgesetzte Maßnahmen / Erläuterungen:**
3. Privacy by Default **Maßnahmen:** **x** Einfache Ausübung des Widerrufsrechts durch technische Maßnahmen. **x** Trackingfunktionen, die den Betroffenen überwachen, sind standardmäßig deaktiviert. **x** Sämtliche Vorbelegungen von Auswahlmöglichkeiten erfüllen die Anforderungen der DSGVO (keine Vorbelegungen von Opt-ins).	**Weitere umgesetzte Maßnahmen / Erläuterungen:**
4. Zugriffskontrolle und Zugangskontrolle **Maßnahmen:** **x** Berechtigungskonzepte dokumentiert. **x** Vermeidung von Gruppenusern. **x** Zugriff auf Daten ist eingeschränkt und nur für Berechtigte möglich. **x** Sperrung des Benutzerkontos bei Fehlversuchen / Inaktivität. **x** Anzahl der Administratoren auf das Notwendigste reduziert. **x** Protokollierung von Zugriffen auf Anwendungen, insbesondere bei Eingabe, Änderung und Löschung von Daten. **x** Regelmäßige Überprüfung der Berechtigungen. **x** Passwortrichtlinie, Implementierung komplexer Passwörter.	**Weitere umgesetzte Maßnahmen / Erläuterungen:** Zugriffsrechte werden rollenbasiert vergeben (Rollen: Owner, Admin, Manager, Creator); Berechtigungen werden mindestens einmal jährlich durch die Geschäftsführung überprüft und dokumentiert. Zentrale Identitätsverwaltung aller Mitarbeitenden über Microsoft Entra ID (Microsoft 365); verknüpfte SaaS-Zugänge werden über Entra ID gesteuert und bei Statusänderung innerhalb von 24 Stunden deaktiviert. Pflicht-2FA für alle administrativen und privilegierten Zugänge. Zugriff auf Produktionssysteme über HTTPS mit SSH-Key-Authentifizierung; Serverzugriff über IP-Whitelist. Session-Cookies mit 2-Tage-Gültigkeit und automatischer Invalidierung. Kundenaccounts werden über companyId-Scoping mandantenseitig isoliert. Anwendungsseitig: reCAPTCHA v3 zur Erkennung von Missbrauch; Cloudflare Firewall-Regeln, Rate-Limiting und Bot-Management. Branch-Protection-Rules in GitHub verhindern direkte Merges ohne Review.
5. Kryptographie und/oder Pseudonymisierung *Einsatz von Verschlüsselungsverfahren zum Schutz der Vertraulichkeit, Authentizität und Integrität personenbezogener Daten.* **Maßnahmen:** **x** Verschlüsselung von Datenträgern (z.B. mobile Festplatten, USB-Sticks). **x** Verschlüsselung von Endgeräten (PC, Laptop, Smartphones). **x** Verschlüsselte Ablage von personenbezogenen Daten. **x** Verschlüsselung von Zugängen zum Netzwerk und -verbindungen. **x** Einsatz von Verfahren zur Anonymisierung von Daten.	**Weitere umgesetzte Maßnahmen / Erläuterungen:** Ausschließlich offene, standardisierte Verschlüsselungsverfahren nach ISO/IEC- und NIST-Empfehlungen: TLS 1.2/1.3 für sämtliche Client-Server- und Infrastruktur-Verbindungen (Neon, Cloudflare R2, Upstash, Pusher, Resend, Stripe, OpenAI/Anthropic/Google); AES-256 für Speicherung at rest; bcrypt für Passwort-Hashing; JOSE-Standards (RFC 7515-7518) für JWT-Tokens. Sichere Cookie-Attribute (HttpOnly, Secure, SameSite) und HSTS aktiv. Webhook-Signaturen über HMAC-SHA256. Zahlungsdaten ausschließlich über Stripe (PCI DSS Level 1). Secrets und API-Keys verschlüsselt in Vercel Environment Variables. Mitarbeiter-Endgeräte vollständig verschlüsselt (macOS FileVault / Windows BitLocker). Keine proprietären Verschlüsselungsverfahren.
6. Schutz von Gebäuden **Maßnahmen:** ☐ Zonenkonzept und Festlegung von Sicherheitsbereichen. ☐ Gebäudesicherung durch Zäune. ☐ Sicherheitsschlösser und Schlüsselverwaltung. ☐ Alarmanlage / Videoüberwachung. ☐ Einsatz von Wachpersonal.	**Weitere umgesetzte Maßnahmen / Erläuterungen:** Kein Besucher- oder Kundenverkehr. ViralSpoon GmbH arbeitet remote, daher keine räumlichen Zutrittskontrollen erforderlich. Admin-UI mit HTTPS, Passwort und zertifikatsbasierter Authentifizierung, IP-Whitelist. Serverzugriff via SSH-Key. Cloudflare: WAF, Bot-Management, Rate-Limiting. Weitere Maßnahmen durch unsere zertifizierten Cloud-Provider.

Weisungen zu technischen und organisatorischen Maßnahmen	
7. Schutz von Betriebsmitteln / Informationswerten **Maßnahmen:** **x** Sichere Platzierung der Systeme, so dass Schutz vor Diebstahl gewährleistet ist. **x** Unterbringung der Server- und Netzkomponenten in gesicherten Räumen (Cloud-Provider). ☐ Schutz der Betriebsmittel vor Feuer, Wasser oder Überspannung. ☐ Regelmäßige Wartung der Betriebsmittel.	**Weitere umgesetzte Maßnahmen / Erläuterungen:** Ablage von Akten und Dokumenten erfolgt rein digital. Sicherungs-Backup läuft cloudbasiert auf MS Azure. Weitere Maßnahmen durch zertifizierte Cloud-Provider.
8. Betriebsverfahren und Zuständigkeiten **Maßnahmen:** **x** Klare Zuordnung von Verantwortlichkeiten für die System- und Anwendungsbetreuung. **x** Trennung der Verarbeitung von Daten der einzelnen Mandanten. **x** Trennung von Entwicklungs-, Test- und Produktivsystemen. **x** Überwachung des Systembetriebs und der Anlagen.	**Weitere umgesetzte Maßnahmen / Erläuterungen:**
9. Datensicherungen **Maßnahmen:** **x** Datensicherungskonzept mit regelmäßigen Backups. **x** Auslagerung der Backups in andere Brandzonen. ☐ Regelmäßige Tests der Datensicherung und Wiederherstellung.	**Weitere umgesetzte Maßnahmen / Erläuterungen:** Mehrschichtiges Backup-Konzept: Datenbank (Neon, EU Frankfurt) mit automatischen täglichen Backups und Point-in-Time-Recovery (PITR). Objekt-Storage (Cloudflare R2) mit Geo-Redundanz über mehrere EU-Edge-Standorte. Sämtliche Backups AES-256-verschlüsselt at rest. Aufbewahrungsfristen mandantenspezifisch gemäß HGB/AO konfiguriert; gesperrte Daten werden nach Fristablauf automatisch gelöscht. Initialer Restore-Test durchgeführt; jährliche formalisierte Tests im Rahmen der ISO/IEC 27001-Vorbereitung (2026/2027) geplant. Mandantenisolation stellt sicher, dass Wiederherstellung eines Kunden keine Auswirkung auf andere hat.
10. Schutz vor Malware und Patchmanagement *Verhinderung von Schwachstellen durch aktuellen Virenschutz und Patchmanagement.* **Maßnahmen:** **x** Regelmäßige Überwachung des Status von Sicherheitsupdates und Systemschwachstellen. **x** Regelmäßiges Einspielen von Sicherheitspatches und Updates.	**Weitere umgesetzte Maßnahmen / Erläuterungen:** Mehrstufiges Schutzkonzept: Anwendungsebene: ESLint mit Next.js-Sicherheitsregeln, TypeScript Strict Mode und npm audit als automatisierte Schwachstellen-Scans bei jedem Deployment; kritische CVEs werden vor Deployment behoben. CI/CD-Pipeline mit Production-Gate. Locked Dependencies; keine ungeprüften Abhängigkeiten erreichen die Produktion. Infrastrukturebene: Patch-Management durch zertifizierte PaaS-Provider (Vercel, Neon, Cloudflare, Upstash). Cloudflare WAF blockiert bekannte Angriffsmuster (OWASP-Regelsätze). Endgeräteebene: Microsoft Defender auf allen Mitarbeiter-Endgeräten aktiv; Geräteverwaltung über Microsoft 365 / Entra ID.
11. Protokollierung und Überwachung *Maßnahmen, die nachträgliche Prüfung ermöglichen, ob und von wem personenbezogene Daten verarbeitet wurden.* **Maßnahmen:** **x** Protokollierung von Aktivitäten der Systemadministratoren. **x** Überwachung der Systemnutzung. **x** Protokollierung von Zugängen. **x** Protokollierung von Zugriffen. **x** Auswertung von Log-Dateien. ☐ Protokollierung über SIEM-System.	**Weitere umgesetzte Maßnahmen / Erläuterungen:** Mehrschichtiges Logging- und Monitoring-System: Infrastrukturebene: Azure Monitor mit Activity Logs, Microsoft Defender for Cloud und Sign-In Logs aktiv; Speicherdauer standardmäßig 30 Tage, verlängerbar über Log Analytics. Privilegierte Zugänge werden provider-seitig mit Zeitstempel und Akteur protokolliert; Pflicht-2FA. Anwendungsebene: strukturiertes Audit-Trail-System mit UserId, Timestamp und Delta; automatische Redaktion sensibler Felder vor Speicherung. Rate-Limiting-Logging auf sensiblen Endpunkten. Cloudflare Analytics und WAF-Logs. Zugriff auf Audit-Logs nach Need-to-Know-Prinzip. Formales SIEM im Rahmen der ISO/IEC 27001-Einführung (2026/2027) geplant.
12. Netzwerksicherheitsmanagement **Maßnahmen:** **x** Einsatz von Firewallsystemen.	**Weitere umgesetzte Maßnahmen / Erläuterungen:** Nutzung einer Cloud Firewall; Cloudflare WAF mit OWASP-Regelsätzen; Rate-Limiting und Bot-Management.
13. Informationsübertragung **Maßnahmen:**	**Weitere umgesetzte Maßnahmen / Erläuterungen:**

Weisungen zu technischen und organisatorischen Maßnahmen	
x Weitergabe von Daten an Dritte nur nach Prüfung der Rechtsgrundlage. **x** Sichere Datenübertragung zwischen Client und Server. **x** Angemessener Schutz von E-Mails, die sensible Informationen beinhalten. **x** Sicherer Transport und Versand von Datenträgern, Daten und Dokumenten.	
14. Netztrennung **Maßnahmen:** ☐ Logische Mandantentrennung. ☐ Datentrennung durch Segmentierung von Netzwerken. ☐ Trennung der Netze bei Remote-Zugriffen.	**Weitere umgesetzte Maßnahmen / Erläuterungen:** Durch rein cloudbasierte Infrastruktur keine Notwendigkeit für getrennte Netzwerke. Azure-Funktionen wie VNETs, NSG, Defender sind aktiv. Weitere Maßnahmen durch zertifizierte Cloud-Provider.
15. Anschaffung, Entwicklung und Instandhaltung von Systemen **Maßnahmen:** **x** Festlegung von sicherheitsspezifischen Regelungen und Anforderungen für den Einsatz neuer Informationssysteme.	**Weitere umgesetzte Maßnahmen / Erläuterungen:** Sicherheit ist als fester Bestandteil der gesamten Entwicklungspipeline integriert (Security by Design): mehrstufiger CI/CD-Prozess mit Pre-Commit-Hooks (Husky), TypeScript-Typprüfung, automatisierten Sicherheits-Checks (ESLint, ast-grep, npm audit) pro Pull Request und Production-Gate vor jedem Deployment. Strikt getrennte Umgebungen (Development, Preview, Production) mit separaten Datenbanken, separatem Objekt-Storage und getrennten API-Keys. Migrations-Review: Datenbankschema-Änderungen durchlaufen automatisierten Schema-Diff und manuellen Review. Locked Dependencies in allen Builds; regelmäßige Dependency-Reviews im Pull-Request-Prozess.
16. Lieferantenbeziehungen **Maßnahmen:** **x** Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere Datensicherheit). **x** Schriftliche Weisungen an den Auftragnehmer (AVV) i.S.d. DSGVO. **x** Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart. **x** Vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen. **x** Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis. **x** Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags.	**Weitere umgesetzte Maßnahmen / Erläuterungen:**
17. Management von Informationssicherheitsvorfällen *Konsistente und wirksame Maßnahmen für das Management von Sicherheitsvorfällen.* **Maßnahmen:** ☐ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen. **x** Sofortige Information des Auftraggebers bei Datenschutzvorfällen. ☐ Einbindung des DSB bei Datenschutzvorfällen. ☐ Formaler Prozess zur Nachbearbeitung von Sicherheitsvorfällen.	**Weitere umgesetzte Maßnahmen / Erläuterungen:** Definierte Eskalationspfade (Slack, E-Mail) zur Vorfallbehandlung. Audit-Trail-System protokolliert sicherheitsrelevante Operationen. Provider-seitige Alerts (Cloudflare, Azure). DSB ist in Meldepflichten (Art. 33 DSGVO) eingebunden. Versicherungsschutz für Übertragung elektronischer Daten. Formaler dokumentierter Incident-Response-Plan im Rahmen der ISO/IEC 27001-Einführung (2026/2027) geplant.
18. Business Continuity Management **Maßnahmen:** ☐ Einsatz redundanter Systeme. ☐ Dokumentierte Notfallpläne. ☐ Regelmäßige Tests der Notfallmaßnahmen. **x** Frühzeitige Information des Auftraggebers bei Notfällen.	**Weitere umgesetzte Maßnahmen / Erläuterungen:** Hohe Verfügbarkeit durch Vercel + Neon mit SOC 2-zertifizierten Prozessen. Automatische tägliche Backups der Datenbank. Versionierter Objekt-Storage. Formaler dokumentierter BCM-Plan im Rahmen der ISO/IEC 27001-Vorbereitung (2026/2027) geplant.

Weisungen zu technischen und organisatorischen Maßnahmen	
19. Einhaltung gesetzlicher und vertraglicher Anforderungen **Maßnahmen:** **x** Sicherstellung der Einhaltung der gesetzlichen Verpflichtungen im Rahmen der Zusammenarbeit. **x** Rückgabe sämtlicher Daten, Betriebsmittel und Informationswerte an den Auftraggeber bei Vertragsende. **x** Einrichtung eines Lizenzmanagements. **x** Geheimhaltungsverpflichtungen mit Mitarbeitern sowie Sublieferanten und Dienstleistern.	**Weitere umgesetzte Maßnahmen / Erläuterungen:** Lizenzmanagement über SaaS-, Agentur- und Content-Plattform-Verträge. Rückgabe sämtlicher Daten darin geregelt. NDAs werden mit Mitarbeitern, Sublieferanten und Dienstleistern geschlossen.
20. Datenschutzanforderungen und Datenschutzmanagement **Maßnahmen:** **x** Einrichtung einer Datenschutzorganisation. **x** Bestellung eines Datenschutzbeauftragten. ☐ Verzeichnis der Verarbeitungstätigkeiten. ☐ Datenschutzfolgeabschätzung für Verfahren mit sensiblen Daten. **x** Durchführung von Datenschutzschulungen. **x** Aufbau eines Datenschutz-Managementsystems. ☐ Dokumentiertes Datenschutz-Konzept. ☐ Umgesetzte Richtlinien zum Datenschutz.	**Weitere umgesetzte Maßnahmen / Erläuterungen:** Die Umsetzung erfolgt auf Basis dokumentierter technischer und organisatorischer Maßnahmen sowie verbindlicher Datenschutzschulungen.