AUFTRAGSVERARBEITUNGSVERTRAG („AV“)

nach Art. 28 DSGVO

zwischen

Nutzern der Webanwendung awork

– nachfolgend „Auftraggeber“ genannt –

und

dem Auftragsverarbeiter

awork GmbH

Großer Burstah 36/38 · 20457 Hamburg

– nachfolgend „Auftragnehmer“ genannt –

PRÄAMBEL

Für diesen Auftragsverarbeitungsvertrag gelten die Begriffe und Definitionen der Verordnung (EU) 2016/679 (nachfolgend „DSGVO"), insbesondere des Art. 4 DSGVO.

1. GEGENSTAND

1.1 Gegenstand dieses Auftragsverarbeitungsvertrages ist die Festlegung des datenschutzrechtlichen Rahmens für die vertraglichen Beziehungen zwischen den Parteien.

1.2 Die Beschreibung des jeweiligen Auftrags mit den Angaben über Gegenstand des Auftrags, Umfang, Art und Zweck der Datenverarbeitung, Art der personenbezogenen Daten sowie Kategorien der betroffenen Personen befindet sich in der Anlage unter der Ziffer 1.

2. ORT DER DATENVERARBEITUNG

2.1 Die vertraglich vereinbarte Verarbeitung findet im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum („Sichere Staaten") statt, sofern sich aus der Anlage nichts Anderes ergibt.

2.2 Der Auftragnehmer darf Auftraggeberdaten durch Stellen außerhalb der Sicheren Staaten („Drittland") nur verarbeiten oder verarbeiten lassen, wenn und soweit (i) für das betreffende Drittland auf Grundlage einer gültigen Entscheidung der Europäischen Kommission ein angemessenes Datenschutzniveau festgestellt ist oder (ii) die Verarbeitung auf Grundlage und nach Maßgabe der jeweils gültigen EU-Standardvertragsklauseln („SCC") erfolgt, welche dem Auftraggeber vorzulegen und mit der im Drittland ansässigen Stelle („Datenimporteur") schriftlich zu vereinbaren sind. Sofern der Datenimporteur und der Auftragnehmer nicht identisch sind, hat der Auftragnehmer diesen SCC beizutreten. Die in dieser AV festgelegten Bestimmungen bleiben unberührt.

3. LAUFZEIT

3.1 Dieser Vertrag wird auf unbestimmte Zeit geschlossen und kann von jeder Partei mit einer Frist von drei Monaten gekündigt werden. Soweit im Zeitpunkt der Kündigung noch ein Hauptvertrag oder mehrere Hauptverträge, bei denen der Auftragnehmer im Auftrag personenbezogene Daten des Auftraggebers verarbeitet, in Kraft sind, gelten die Bestimmungen dieses Vertrages bis zu der regulären Beendigung des Hauptvertrages/der Hauptverträge fort.

3.2 Der Auftraggeber kann diesen Vertrag ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

4. WEISUNG

4.1 Der Auftragnehmer verarbeitet die personenbezogenen Daten nur im Rahmen der vom Auftraggeber erteilten Weisungen. Dies gilt nicht, soweit der Auftragnehmer durch das Recht der EU oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, zur Verarbeitung verpflichtet ist. In diesem Fall

teilt der Auftragnehmer diese rechtlichen Anforderungen vor der Verarbeitung mit, es sei denn, die Mitteilung ist durch das betreffende Recht wegen eines wichtigen öffentlichen Interesses verboten.

4.2 Falls Weisungen die unter Ziffer 1 der Anlage dieses Vertrages getroffenen Festlegungen ändern, aufheben oder ergänzen, sind sie nur zulässig, wenn eine entsprechende neue Vereinbarung in schriftlicher Form erfolgt.

4.3 Unabhängig von der Form der Erteilung dokumentieren sowohl der Auftragnehmer als auch der Auftraggeber jede Weisung des Auftraggebers in Textform. Die Weisungen sind für ihre Geltungsdauer dieses Vertrages und anschließend noch für drei Jahre aufzubewahren.

4.4 Der Auftragnehmer weist den Auftraggeber unverzüglich darauf hin, wenn eine vom Auftraggeber erteilte Weisung seiner Auffassung nach gegen gesetzliche Vorschriften verstößt. In einem solchen Fall ist der Auftragnehmer nach rechtzeitiger vorheriger Ankündigung gegenüber dem Auftraggeber berechtigt, die Ausführung der Weisung auszusetzen, bis der Auftraggeber die Weisung geändert hat oder diese bestätigt. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

4.5 Weisungen dürfen nur durch Personen erteilt werden, welche aufgrund ihrer organschaftlichen Stellung oder ihrer besonderen Funktion den Auftraggeber insoweit vertreten (z.B. Datenschutzbeauftragter, Chief Security Officer, etc.).

4.6 Der Auftragnehmer legt in der Anlage dieses Vertrages Weisungsempfänger fest. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und in schriftlicher oder elektronischer Form die Nachfolger oder Vertreter mitzuteilen.

5. UNTERSTÜTZUNGSPFLICHTEN DES AUFTRAGNEHMERS

5.1 Der Auftragnehmer ergreift angesichts der Art der Verarbeitung geeignete technische und organisatorische Maßnahmen, um den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen der betroffenen Personen nach Art. 12 bis 22 DSGVO zu unterstützen.

5.2 Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragnehmer den Verantwortlichen bei der Einhaltung seiner Pflichten nach Art. 32 bis 36 DSGVO. Im Einzelnen bei der Sicherheit der Verarbeitung, bei Meldungen von Verletzungen an die Aufsichtsbehörde, der Benachrichtigung betroffener Personen bei einer Verletzung, der Datenschutz-Folgeabschätzung und bei der Konsultation der zuständigen Aufsichtsbehörde.

5.3 Sofern sich eine betroffene Person oder eine Datenschutzaufsichtsbehörde im Zusammenhang mit den unter dieser Vereinbarung verarbeiteten personenbezogenen Daten direkt an den Auftragnehmer wendet, informiert der Auftragnehmer den Auftraggeber hierüber unverzüglich und stimmt die weiteren Schritte mit ihm ab.

6. PRÜFUNGSRECHTE DES AUFTRAGGEBERS

6.1 Der Auftragnehmer stellt dem Auftraggeber auf dessen Anfrage alle erforderlichen Informationen zum Nachweis der in diesem Vertrag und Art. 28 DSGVO geregelten Pflichten zur Verfügung.

Insbesondere erteilt der Auftragnehmer dem Auftraggeber Auskünfte über die gespeicherten Daten und die Datenverarbeitungsprogramme.

6.2 Der Auftraggeber oder von ihm beauftragte Dritte sind – grundsätzlich nach Terminvereinbarung mindestens 30 Tage im Voraus – berechtigt, die Einhaltung der Pflichten aus diesem Vertrag und aus Art. 28 DSGVO zu überprüfen und beim Auftragnehmer Inspektionen vor Ort durchzuführen. Der Auftragnehmer ermöglicht dies und trägt dazu bei. Anlasslose Inspektionen sind auf maximal eine Inspektion pro Jahr beschränkt.

6.3 Der Auftragnehmer hat dem Auftraggeber auf Anforderung geeigneten Nachweis über die Einhaltungen der Verpflichtungen gemäß Art. 28 Abs. 1 und Abs. 4 DSGVO zu erbringen. Dieser Nachweis kann durch die Bereitstellung von Dokumenten und Zertifikaten, die genehmigte Verhaltensregeln i. S. v. Art. 40 DSGVO oder genehmigte Zertifizierungsverfahren i. S. v. Art. 42 DSGVO abbilden, erbracht werden.

7. DATENSCHUTZBEAUFTRAGTER DES AUFTRAGNEHMERS

7.1 Der Datenschutzbeauftragte des Auftragnehmers ist in der Anlage dieses Vertrages unter Ziffer 3 angeführt.

8. VERTRAULICHKEIT

8.1 Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Er wahrt bei der Verarbeitung der personenbezogenen Daten des Auftraggebers das Datengeheimnis sowie die Vertraulichkeit. Diese Pflicht besteht auch nach Beendigung dieses Vertragsverhältnisses fort.

8.2 Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht. Er verpflichtet diese Mitarbeiter durch schriftliche Vereinbarung für die Zeit der Tätigkeit und auch nach Beendigung des Beschäftigungsverhältnisses zur Wahrung der Vertraulichkeit, sofern sie nicht einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Unternehmen.

8.3 Auskünfte an Dritte oder Betroffene darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung, oder Zustimmung in einem elektronischen Format, durch den Auftraggeber erteilen. 9. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

9.1 Der Auftragnehmer führt geeignete technische und organisatorische Maßnahmen so durch, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet ist. Er gestaltet seine innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und ein angemessenes Schutzniveau erreicht wird. Insbesondere hat der Auftragnehmer unter Berücksichtigung des jeweiligen Stands der Technik die angemessene Sicherheit der Verarbeitung, insbesondere die Vertraulichkeit (inklusive Pseudonymisierung und Verschlüsselung), Verfügbarkeit, Integrität, und Belastbarkeit der für die Datenverarbeitung verwendeten Systeme und Dienstleistungen sicherzustellen.

9.2 Die technischen und organisatorischen Maßnahmen in der Anlage werden als verbindlich festgelegt.

9.3 Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen Weiterentwicklung angepasst werden. Dabei müssen die angepassten Maßnahmen mindestens dem Sicherheitsniveau der in der Anlage vereinbarten Maßnahmen entsprechen. Wesentliche Änderungen sind in schriftlicher Form oder einem elektronischen Format zu vereinbaren.

10. INFORMATIONSPFLICHTEN DES AUFTRAGNEHMERS UND VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN

10.1 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über jegliche Verstöße oder vermutete Verstöße gegen diesen Vertrag oder Vorschriften, die den Schutz personengezogener Daten betreffen.

10.2 Der Auftragnehmer unterstützt den Auftraggeber bei der Untersuchung, Schadensbegrenzung und Behebung der Verstöße.

10.3 Sollten die personenbezogenen Daten die unter dieser Vereinbarung verarbeitet werden 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 relevanten Stellen unverzüglich auch darüber informieren, dass die Herrschaft über die Daten beim Auftraggeber liegt.

10.4 Soweit Prüfungen der Datenschutzaufsichtsbehörden durchgeführt werden, verpflichtet sich der Auftragnehmer das Ergebnis dem Auftraggeber bekannt zu geben, soweit es die Verarbeitung der personenbezogenen Daten unter diesem Vertrag betrifft. Die im Prüfbericht feststellten Mängel wird der Auftragnehmer unverzüglich abstellen und den Auftraggeber darüber informieren.

11. UNTERAUFTRAGNEHMER

11.1 Der Auftraggeber berechtigt den Auftragnehmer, Subunternehmer in die Auftragsverarbeitung einzubeziehen. Einer gesonderten vorherigen Zustimmung durch den Auftraggeber bedarf es nicht. Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines Subunternehmers mindestens 6 Wochen vor der geplanten Umstellung in Textform. Der Auftraggeber kann der Änderung innerhalb von 3 Wochen ab Erhalt der Information in Textform aus wichtigem Grund widersprechen. Ein Widerspruch zieht ein beidseitiges, außerordentliches Kündigungsrecht des Hauptvertrages nach sich. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung als erteilt.

11.2 Der Auftragnehmer hat vertraglich sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber Unterauftragnehmern gelten. Der Vertrag des Auftragnehmers mit dem Subunternehmer muss schriftlich oder in elektronischem Format abgeschlossen werden.

11.3 Eine Beauftragung von Subunternehmern in Drittstaaten erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

11.4 Der Auftraggeber erteilt hiermit zudem explizit seine Zustimmung zur Beauftragung der in der Anlage aufgeführten Unterauftragnehmer.

11.5 Der Auftragnehmer stellt sicher, dass der Auftraggeber gegenüber dem Unteraufragnehmer dieselben Weisungsrechte und Kontrollrechte wie gegenüber dem Auftragnehmer nach diesem Vertrag hat. Kommt ein Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Unterauftragnehmers.

11.6 Auf Verlangen des Auftraggebers hat der Auftragnehmer den Abschluss, der mit dem Subunternehmer geschlossenen Vereinbarungen gegenüber dem Auftraggeber nachzuweisen. Der Nachweis hat in Textform zu erfolgen.

12. LÖSCHUNG UND RÜCKGABE PERSONENBEZOGENER DATEN

12.1 Der Auftragnehmer ist nach Abschluss der jeweils im Hauptvertrag vereinbarten Verarbeitungsleistungen verpflichtet, alle personenbezogenen Daten, die er im Zuge der Auftragsverarbeitung erhalten hat innerhalb von 35 Tagen zu löschen. Dies schließt insbesondere die Ergebnisse der Datenverarbeitung, überlassene Dokumente und überlassene Datenträger und Kopien der personenbezogenen Daten mit ein. Die Pflicht zur Löschung besteht nicht, sofern der Auftragnehmer nach dem Recht der EU oder der Mitgliedstaaten zur weiteren Speicherung der Daten gesetzlich verpflichtet ist. Besteht eine weitere Verpflichtung zur Speicherung, hat der Auftragnehmer die Verarbeitung der personenbezogenen Daten einzuschränken und die Daten nur für die Zwecke zu nutzen, für die eine Verpflichtung zur Speicherung besteht. Die Pflichten zur Sicherheit der Verarbeitung bestehen für den Zeitraum der Speicherung fort. Der Auftragnehmer hat die Daten innerhalb von 35 Tagen zu löschen, sobald die Pflicht zur Speicherung entfällt. Hinweis: Eine Löschung innerhalb von weniger als 35 Tagen ist aufgrund des etablierten Backupkonzeptes der verwendeten Datenbanken technisch nicht möglich.

12.2 Die Löschung hat so zu erfolgen, dass die Daten nicht wiederherstellbar sind.

12.3 Die Vorgänge sind mit Angabe von Datum zu protokollieren.

12.4 Auf Wunsch des Auftraggebers werden personenbezogene Daten, die der Auftragnehmer im Zuge der Auftragsverarbeitung vom Auftraggeber erhalten hat, nach Abschluss der jeweils im Hauptvertrag vereinbarten Verarbeitungsleistungen dem Auftraggeber innerhalb von 35 Tagen zurückgegeben.

13. HAFTUNG

13.1 Die Parteien haften gem. Art. 82 DSGVO.

13.2 Im Innenverhältnis haftet der Auftragnehmer nur für in seiner Sphäre liegendes Verschulden gegenüber dem Auftraggeber. Die Haftungsregelungen des Hauptvertrags bleiben im Innenverhältnis unberührt.

14. SCHLUSSBESTIMMUNGEN

14.1 Die Einrede des Zurückbehaltungsrechts im Sinne von § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten ausgeschlossen.

14.2 Die Anlage oder im Falle mehrerer abgeschlossener Hauptverträge die Anlagen zu diesem Vertrag sind wesentlicher Bestandteil desselben.

14.3 Für Änderungen oder Nebenabreden ist die Schriftform oder ein elektronisches Format erforderlich. Dies gilt auch für Änderungen dieses Formerfordernisses.

14.4 Sofern zwischen den Parteien wegen der in dieser AV festgelegten oder in Bezug genommenen Leistungen bereits Vereinbarungen zur Datenverarbeitung im Auftrag bestehen, werden diese Vereinbarungen mit Wirksamkeit dieser AV aufgehoben und regelt diese AV abschließend die insoweit bestehenden Rechte und Pflichten der Parteien.

14.5 Die Parteien sind sich einig, dass diese AV mittels elektronischer Signatur unterzeichnet werden soll und alternativ in Schriftform abgefasst werden kann. Sie kann mittels elektronischer Signatur wirksam dergestalt unterzeichnet werden, dass die Parteien die jeweils von ihnen unterzeichneten Exemplare in elektronischer Form als pdf austauschen. Eine Unterzeichnung kann ebenfalls durch den digitalen Online-Registrierungsprozess des Auftragnehmers erfolgen. Der Auftraggeber garantiert, dass die signierende oder den Online-Registrierungsprozess abschließende Person (Bevollmächtigter) über sämtliche zum Abschluss dieser AV erforderlichen Vollmachten und Vertretungsberechtigungen verfügt. Der Auftraggeber wird sich sämtliche Erklärungen des Bevollmächtigten zurechnen lassen. Änderungen dieser AV einschließlich ihrer Anhänge unterliegen ebenfalls den in dieser Ziffer geregelten Formerfordernissen.

14.6 Erweist sich eine Bestimmung dieser Vereinbarung als unwirksam, so berührt dies die Wirksamkeit der übrigen Bestimmungen der Vereinbarung nicht.

14.7 Diese AV unterliegt deutschem Recht. Gerichtsstand für Streitigkeiten aus dieser AV entspricht der Regelung des Hauptvertrags

ANLAGE ZUM AUFTRAGSVERARBEITUNGSVERTRAG

1. GEGENSTAND DES AUFTRAGES

1.1 GEGENSTAND DES AUFTRAGES

Der Auftragsverarbeiter ist Hersteller und Anbieter von Unternehmenssoftware zur Abwicklung aller projektbezogenen kaufmännischen Prozesse. Hierzu zählen der Vertrieb, die Beratung, Implementierung sowie Integration, Hosting und Support der Lösungen. Die Datenerhebung, -verarbeitung und -nutzung erfolgt zur Ausübung der oben angegebenen Zwecke.

1.2 UMFANG, ART (ART. 4 NR. 2 DSGVO) UND ZWECK DER DATENVERARBEITUNG

Die Verarbeitung personenbezogener Daten erfolgt zum Zweck der Bereitstellung der Software-as-a-Service-Anwendung awork, mit deren Hilfe die Arbeits-, Team- und Projektorganisation des Auftraggebers erfolgt. Das bedeutet insbesondere:

- Hosting (Daten, Applikation, System, Komponenten)
- Betrieb (Applikation, System, Komponenten)
- Wartung/Pflege (Applikation, System, Komponenten)
- Support (Applikation, System, Komponenten)
- Weiterentwicklung (Applikation, System, Komponenten)

Zu diesem Zweck werden personenbezogene Daten erfasst, gespeichert, ausgelesen, organisiert und geordnet, in Benutzeroberflächen angezeigt sowie gelöscht.

1.2.1 ERGÄNZENDE OPTIONALE KI-VERARBEITUNGEN · NEU IN V05

Soweit KI-gestützte Funktionen im gebuchten awork-Tarif oder im awork-AI-Add-on verfügbar sind, finden die nachfolgenden Verarbeitungen nur statt, wenn die betreffende Funktion bzw. das betreffende Modell für den Workspace freigegeben und durch den Auftraggeber oder seine Nutzer tatsächlich verwendet oder konfiguriert wird:

- Übermittlung und vorübergehende Verarbeitung von Prompts, ausgewählten Workspace-Inhalten und dem für die Anfrage erforderlichen Kontext zur Generierung von Text-, Bild- oder sonstigen Modellergebnissen
- Speicherung von Chatverläufen und vom Nutzer gespeicherten AI-Inhalten ausschließlich in der von awork kontrollierten Azure-Infrastruktur, damit diese im Produkt angezeigt werden können
- Ausführung von Agents, Tools, Connections, Triggern und Zeitplänen innerhalb der vom Auftraggeber eingeräumten Berechtigungen
- keine Nutzung von Auftraggeberdaten zum Training allgemeiner Modelle und keine Speicherung von Prompts oder Outputs durch die eingesetzten Modellinferenzanbieter
- kein Einsatz von AWS Bedrock als Ausfall- oder Lastspitzen-Fallback für die reguläre Azure-basierte KI-Verarbeitung

Berechtigte Workspace-Administratoren können verfügbare Modelle nach Maßgabe der Produktfunktionen deaktivieren. Deaktivierte Modelle werden nicht für neue Verarbeitungen eingesetzt.

1.3 KREIS DER BETROFFENEN UND ART DER DATEN

Zu folgenden Personengruppen werden personenbezogene Daten erhoben, verarbeitet und genutzt, sofern dies zur Erfüllung des genannten Zweckes erforderlich ist:

- Interne und externe Mitarbeiter (z.B. Freelancer) und Aushilfen des Auftraggebers
  - Berufliche Kontakt- und (Arbeits-)Organisationsdaten zur Verwaltung von Usern: Name, Vorname, Geschlecht, E-Mail, Telefonnummer, Foto
  - Daten zu beruflichen Verhältnissen: Berufsbezeichnung, Log-File-Informationen, IP-Adresse, Arbeitszeit, Abwesenheitszeiten, Tätigkeiten
- Interessenten, Kunden und sonstige Geschäftspartner des Auftraggebers
  - Berufliche Kontakt- und (Arbeits-)Organisationsdaten: Name, Vorname, E-Mail, Telefonnummer
- Bei Nutzung optionaler KI-Funktionen zusätzlich
  - Inhalte aus Prompts, ausgewähltem Workspace-Kontext, Dokumenten und Dateien sowie Modelloutputs
  - Agent-Konfigurationen, Tool-Aufrufe und Agent-/Tool-Aktivitätsinformationen
  - Sonstige personenbezogene Daten, die der Auftraggeber zur Verarbeitung freigibt; besondere Kategorien nach Art. 9 DSGVO nur, soweit der Auftraggeber solche Daten eigenverantwortlich eingibt oder freigibt

2. WEISUNGSBERECHTIGTE PERSONEN

2.1 WEISUNGSBERECHTIGTE PERSONEN DES AUFTRAGGEBERS

Weisungen dürfen nur durch Personen erteilt werden, welche aufgrund ihrer organschaftlichen Stellung oder ihrer besonderen Funktion den Auftraggeber insoweit vertreten (z.B. Datenschutzbeauftragter, Chief Security Officer, etc.).

2.2 WEISUNGSEMPFÄNGER BEIM AUFTRAGNEHMER

Lucas Bauche, Geschäftsführer · Nils Czernig und Tobias Hagenau, Geschäftsführer · Kommunikationskanal: privacy@awork.com

3. DATENSCHUTZBEAUFTRAGTER

PROLIANCE GmbH · www.datenschutzexperte.de · Leopoldstraße 21 · 80802 München · datenschutzbeauftragter@datenschutzexperte.de

ANLAGE: VERZEICHNIS UNTERAUFTRAGSVERARBEITER

Die awork Anwendnung kann ohne KI-Datenverarbeitungen genutzt werden; KI-Funktionen des Standardprodukts sind durch den Administrator deaktivierbar, das awork-AI-Add-On bedarf einer gesonderten Buchung. Als optional oder bedingt bezeichnete Anbieter werden nur eingesetzt, wenn die bezeichnete Funktion bzw. das bezeichnete Modell für den Workspace verfügbar und aktiviert ist.

A. ALLGEMEINE PLATTFORMDIENSTE

Microsoft Ireland Operations Limited – Azure Compute/Storage

Leistungsgegenstand	Primäres Hosting. Bereitstellung der technischen Infrastruktur für den Betrieb von awork in deutschen Rechenzentren; umfasst Server, Speicherplatz und Netzwerkdienste.
Verarbeitete Daten	Alle unter Anlage 1.2 genannten Daten; alle in awork eingegebenen Daten, z.B. Projekte, Aufgaben, Zeiterfassungen und Dokumente; Benutzer- und Zugriffsberechtigungen; hochgeladene Dateien und Inhalte.
Ort	Deutschland: Frankfurt am Main (Germany West Central) und Berlin (Germany North). Sämtliche Kundendaten werden ausschließlich in Deutschland gespeichert und verarbeitet.
Schutzmaßnahmen	DPA mit Microsoft; ISO 27001, SOC 2 und BSI C5; Verschlüsselung aller Daten bei Übertragung und Speicherung; strenge Zugriffskontrollen nach dem Minimalprinzip; keine Übermittlung von Kundendaten außerhalb Deutschlands.

Microsoft Ireland Operations Limited – Azure Front Door/CDN

Leistungsgegenstand	Schnelle und sichere Auslieferung der awork-Anwendung über ein globales Content Delivery Network sowie Schutz vor Cyberangriffen.
Verarbeitete Daten	Technische Verbindungsdaten, insbesondere IP-Adresse und Browserinformationen; zwischengespeicherte statische App-Ressourcen wie Bilder, Skripte und Stylesheets; keine Verarbeitung von Geschäftsdaten.
Ort	Primär EU/Deutschland: Kundendaten werden in der gewählten EU-Region gespeichert und verarbeitet. Nur bei einem Zugriff aus einem Nicht-EU-Land kann eine technisch bedingte, kurzzeitige Verarbeitung technischer Verbindungsdaten über den geografisch nächstgelegenen Server erfolgen; gespeicherte Inhalte sind davon nicht betroffen.
Schutzmaßnahmen	DPA mit Microsoft; EU-Datenresidenz für Kundendaten; verschlüsselte Übertragung; technische Verbindungsdaten werden maximal 30 Tage gespeichert; keine dauerhafte Speicherung von Geschäftsinhalten im CDN; bei technisch bedingter Drittlandverarbeitung gelten Angemessenheitsbeschluss oder SCC.

Birdie.so / Philo Labs

Leistungsgegenstand	Tool zur Fehlererfassung und -meldung. Wird nur aktiv, wenn ein Nutzer selbst einen Bug mithilfe eines Screensrecordings meldet; erfasst technische Kontextinformationen zur schnelleren Problemlösung.
Verarbeitete Daten	Fehlerbeschreibung und Kommentare; automatisch erfasste technische Daten wie Browser, Betriebssystem und Console-Logs; optional vom Nutzer hinzugefügte Screenshots oder Bildschirmaufnahmen; Basis-Nutzerdaten wie Name und E-Mail für Rückmeldungen.
Ort	EU: Paris, Frankreich.
Schutzmaßnahmen	DPA mit garantierter ausschließlicher EU-Verarbeitung; keine Drittlandübertragung; verschlüsselte Datenübertragung; Datenminimierung auf bugrelevante Informationen; automatische Löschung nach Ticketbearbeitung nach 90 Tagen. Geschäftsdaten werden nicht automatisch übertragen.

Twilio Ireland Limited – Segment

Leistungsgegenstand	Ausschließlich technische Daten- und Kontextweiterleitung an Intercom zur Bereitstellung und Verbesserung des Kundensupports
Verarbeitete Daten	technische Nutzungs- und Gerätedaten, Account-/Nutzerkontext für Supportzwecke sowie gegebenenfalls vom Nutzer übermittelte supportbezogene Inhalte
Ort	primär EU: Verarbeitung in den USA im Rahmen der Twilio-Infrastruktur möglich
Schutzmaßnahmen	DPA; EU-US Data Privacy Framework; SCC als zusätzliche Absicherung; Datenminimierung

Intercom, Inc.

Leistungsgegenstand	Kundensupport und Supportkommunikation in awork
Verarbeitete Daten	<u>Bei Support-Kontakt:</u> a) Name, E-Mail, Chat-Verlauf b) vom Nutzer geteilte Inhalte (z.B. Screenshots) <u>Bei System-Nachrichten:</u> a) E-Mail-Adresse für wichtige Updates
Ort	USA
Schutzmaßnahmen	DPA; EU-US Data Privacy Framework; SCC als zusätzliche Absicherung; ISO 27001/SOC 2; verschlüsselte Übertragung; Datenminimierung

B. OPTIONALE KI-INFRASTRUKTUR UND MODELLINFERENZ

Microsoft Ireland Operations Limited – Azure AI Foundry · optional/bedingt

Leistungsgegenstand	KI-Funktionen im Standardprodukt und im awork-AI-Add-on
Verarbeitete Daten	Prompts, erforderlicher Workspace-Kontext und generierte Text- oder Bildausgaben
Ort der Verarbeitung	EU: Primär Germany West Central, Fallback-Ressource Sweden Central
Speicherung und Training	Keine Speicherung von Inferenzdaten beim Modellinferenzdienst und kein Training allgemeiner Modelle. Chatverläufe werden ausschließlich in der awork-Azure-Infrastruktur gespeichert.
Schutzmaßnahmen und Steuerung	- Auftragsverarbeitungsvertrag mit Microsoft - Verschlüsselte Übertragung der Daten - Integrierte Sicherheits- und Inhaltsfilter - Nutzung der KI-Funktionen je Workspace durch Administratoren deaktivierbar - Kein unmittelbarer Zugriff von OpenAI auf Prompts oder Modellausgaben

Google Cloud – Vertex AI API · optional/bedingt

Leistungsgegenstand	Bereitstellung ausgewählter Google-/Gemini-Text- und Bildmodelle
Verarbeitete Daten	Prompts, erforderlicher Workspace-Kontext und generierte Ausgaben
Ort der Verarbeitung	EU: Google Cloud Region Europe-West1, Belgien
Speicherung und Training	Keine Speicherung von Inferenzdaten beim Modellinferenzdienst und kein Training allgemeiner Modelle. Chatverläufe verbleiben in der awork-Azure-Infrastruktur.
Schutzmaßnahmen und Steuerung	- Auftragsverarbeitungsvertrag mit Google - Verschlüsselte Übertragung der Daten - Verarbeitung in der festgelegten Google-Cloud-Region in Belgien - Integrierte und konfigurierbare Sicherheitsfilter prüfen Ein- und Ausgaben auf gefährdende Inhalte und können diese blockieren - Nutzung der über Google bereitgestellten Modelle je Workspace durch Administratoren deaktivierbar

Amazon Web Services EMEA SARL – Amazon Bedrock Runtime · optional/bedingt

Leistungsgegenstand	Bereitstellung von ausgewählten Anthropic Modellen

Verarbeitete Daten	Prompts, erforderlicher Workspace-Kontext und generierte Ausgaben
Ort der Verarbeitung	Europäische Union: Deutschland (eu-central-1), Irland (eu-west-1), Frankreich (eu-west-3), Schweden (eu-north-1), Italien (eu-south-1) und Spanien (eu-south-2). Die Inferenzanfragen können innerhalb dieser AWS-Regionen verarbeitet werden; eine globale Verarbeitung findet nicht statt.
Speicherung und Training	Keine Speicherung von Inferenzdaten beim Modellinferenzdienst und kein Training allgemeiner Modelle. Chatverläufe verbleiben in der awork-Azure-Infrastruktur.
Schutzmaßnahmen und Steuerung	- Auftragsverarbeitungsvertrag mit Amazon Web Services - Verschlüsselte Übertragung der Daten - Ausschließliche Verwendung geografisch begrenzter EU-Inferenzprofile - Kein Zugriff der Modellanbieter auf Prompts oder Modellausgaben - Nutzung der über AWS bereitgestellten Modelle je Workspace durch Administratoren deaktivierbar - Sicherheits- und Inhaltsfilter über Amazon Bedrock Guardrails

TensorX Limited · optional/bedingt

Leistungsgegenstand	Bereitstellung ausgewählter Open-Source-KI-Modelle, derzeit Qwen, GLM, Kimi und DeepSeek
Verarbeitete Daten	Prompts, erforderlicher Workspace-Kontext und generierte Ausgaben
Ort der Verarbeitung	Ausschließlich innerhalb des EWR auf TensorX-eigener Hardware in Dublin, Irland, und Helsinki, Finnland
Speicherung und Training	Keine Speicherung oder Protokollierung von Prompts und Modellausgaben; keine Nutzung für Trainingszwecke; Verarbeitung der Inferenzdaten ausschließlich im flüchtigen Arbeitsspeicher auf TensorX-eigener Hardware; keine Weitergabe an Modellanbieter
Schutzmaßnahmen und Steuerung	- Auftragsverarbeitungsvetrag mit TensorX - Verarbeitung ausschließlich im flüchtigen Arbeitsspeicher auf eigener Hardware - Keine Weitergabe der Inferenzdaten an die Modellanbieter

4. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

Unverändert aus V04 übernommen.

4. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

4.1 ZUTRITTSKONTROLLE ZU RÄUMLICHKEITEN UND EINRICHTUNGEN, IN DENEN DATEN VERARBEITET WERDEN

a) Zutritt zu den Räumlichkeiten des Auftragnehmers, die zur Durchführung des Auftrags verwendet werden, ist auf die zur Durchführung des Auftrags erforderlichen Personen beschränkt.

b) Die Eingänge zu den Räumlichkeiten des Auftragnehmers, in denen Personenbezogene Daten verarbeitet werden, sind mit Sicherheits- oder Magnetkartenschlössern gegen Zutritt Unbefugter gesichert.

c) Die Ausgabe von Schlüsseln und Zugangskarten ist protokolliert.

d) Türen, Tore und Fenster der Räumlichkeiten des Auftragnehmers, in denen Personenbezogene Daten verarbeitet werden, sind außerhalb der Betriebszeiten fest verschlossen; Türen, Tore und Fenster in Keller und Erdgeschoss sowie alle weiteren leicht zu erreichenden Zugänge zu diesen Räumen sind derart ausgeführt, dass diese Unbefugten nur erheblich erschwert zugänglich sind, etwa durch einbruchhemmende Türen, Tore, Fenster und Schlösser und/oder den Einsatz einer Einbruchmeldeanlage, sowie die in VdS 2333 beschriebenen Sicherungsmaßnahmen der Sicherungsklasse SG1.

e) Zur Durchführung des Auftrags vom Auftragnehmer verwendete Server sind in einem separat abgesicherten Serverraum oder Rechenzentrum untergebracht, welche durch eine Zutrittskontrollanlage entsprechend Klasse B nach VdS 2367 gegen den Zutritt Unbefugter gesondert gesichert sind. Diese Räume sind einbruchhemmend geschützt und mindestens gemäß den Vorgaben der Sicherungsklasse SG1 nach VdS 2333 ausgeführt. Der Zutritt zu diesen Räumlichkeiten ist auf das zur Wartung und Instandsetzung sowie auf die im Übrigen konkret erforderlichen Rollen und Personen beschränkt.

4.2 ZUGANGSKONTROLLE

a) Die zur Durchführung des Auftrags vom Auftragsverarbeiter eingesetzten informationsverarbeitenden Systeme (Client- und Serversysteme) sind durch Authentifikations- und Autorisationssysteme geschützt.

b) Identifikations- und Authentifikationsinformationen (insbesondere in Form von Benutzernamen und Passwörtern), welche mit der Zugangsberechtigung zu den zur Durchführung des Auftrags eingesetzten informationsverarbeitenden Systemen verbunden sind, werden nur an die mit der Durchführung des Auftrags beauftragten Personen und lediglich in dem für die jeweilige Aufgabe erforderlichen Umfang vergeben.

c) Jede Vergabe von Zugangsberechtigungen wird für die Laufzeit des Auftrags dokumentiert.

d) Alle Zugänge und Kennungen („Accounts“) werden ausschließlich personenspezifisch vergeben. Die Benutzung von Accounts durch mehrere Personen (Gruppen-Accounts) unterbleibt grundsätzlich.

e) Identifikations- und Authentifikationsinformationen werden ausschließlich persönlich verwendet, ein in solchen Informationen enthaltenes Passwort wird als Initialpasswort vergeben und wird

unverzüglich nach dem Erhalt durch die berechtigte Person entsprechend den in diesem Anhang festgelegten Bestimmungen auf ein nur der berechtigten Person bekanntes Passwort umgesetzt; jegliche Weitergabe unterbleibt. Sofern Unbefugte Kenntnis von Zugangsdaten erhalten, zeigt der Auftragsverarbeiter dies dem Verantwortlichen unverzüglich an.

f) Die Wahl der Passwörter erfolgt in ausreichender Komplexität und Güte. Ausreichende Komplexität und Güte bedeutet mindestens eine Länge von zehn (10) Zeichen bei Nutzung von drei der folgenden 4 Kategorien (Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen), keine Verwendung generischer Begriffe oder von Eigennamen sowie die Unzulässigkeit mindestens der letzten drei (3) verwendeten Passwörter.

g) Der Auftragsverarbeiter hält Authentifikationsdaten (insbesondere Passwörter und kryptographische Schlüssel) gegenüber Unbefugten streng geheim, bewahrt diese nicht im Klartext auf und verwendet diese ausschließlich unter Einsatz einer dieses Anhangs entsprechenden Verschlüsselung oder als unumkehrbare kryptographische Prüfsumme (insbesondere bei der Speicherung und der Übertragung im Netzwerk).

h) Für die Verschlüsselung wird der AES Algorithmus mit 256 Bit und für Password Hashes der HMAC Algorithmus mit 512 Bit verwendet.

i) Jede Herausgabe von Hardware an Mitarbeiter des Auftragnehmers wird für die Dauer des Auftrags dokumentiert.

4.3 ZUGRIFFSKONTROLLE

a) Sofern personenbezogene Daten zur Durchführung des Auftrags auf informationsverarbeitenden Systemen des Auftragsverarbeiters gespeichert sind, ist für sämtliche Zugriffe auf personenbezogene Daten ein abgestuftes und geeignet granulares Rechtesystem eingerichtet und technisch implementiert. Dadurch ist sichergestellt, dass die Zugriffsrechte so gestaltet sind, dass sie nur den für die Leistungserbringung eingesetzten Mitarbeiter jeweils für die Erfüllung der konkreten Aufgaben im notwendigen Umfang Zugriff auf die personenbezogenen Daten erlauben. Dabei ist die Vergabe von Administratorenrechte auf das zwingend erforderliche Maß an Mitarbeitern des Auftragsverarbeiters begrenzt.

b) Alle verarbeiteten Daten werden verschlüsselt übertragen. Alle personenbezogenen Daten werden verschlüsselt in unseren Datenbanksystemen abgelegt. Jeder Zugriff erfolgt ebenfalls über verschlüsselte Datenkanäle.

c) Sofern personenbezogene Daten auf informationsverarbeitenden Systemen des Auftragsverarbeiters gespeichert sind, werden sämtliche Zugriffe auf personenbezogene Daten (einschließlich des lesenden, verändernden und löschenden Zugriffs) nach Benutzer, Datum, Uhrzeit und den jeweils betroffenen Personenbezogene Daten mindestens für die Dauer von 90 Tagen protokolliert.

d) Alle im Rahmen der Auftragsverarbeitung verwendeten Endgeräte (Laptops, Telefone usw.) sind mit automatischer Bildschirmsperre bei Inaktivität versehen.

e) In den Räumen des Auftragnehmers herrscht eine Clean-Desk-Policy, Schreibtische und sonstige Oberflächen sind frei von jeglichen Unterlagen zu hinterlassen.

4.4 EINGABEKONTROLLE

a) Die Eingabe, Änderung und Löschung von Daten in den verwendeten Server-Systemen wird automatisiert protokolliert.

b) Die Eingabe, Änderung und Löschung von Daten in den verwendeten Server-Systemen ist durch das Verwenden individueller Benutzernamen nachvollziehbar.

c) Die Vergabe von Rechten zu Eingabe, Änderung und Löschung von Daten in den verwendeten Server-Systemen erfolgt auf Basis eines Berechtigungskonzepts.

d) Dateien und Dokumente werden in Dokumentenmanagement-Systemen gespeichert, die Eingaben und Änderungen automatisch mit Datum und Benutzerkennung protokollieren.

e) Vor der Installation neuer Programme und Updates auf den verwendeten Serversystemen wird deren Integrität durch Funktionstests sichergestellt.

4.5 AUFTRAGSKONTROLLE

a) Über die allgemeinen Grundsätze sowie über die sich aus dieser AV ergebenden spezifischen Anforderungen des Datenschutzes, einschließlich der Datensicherheit, werden die beim Auftragsverarbeiter zur Durchführung des Auftrags beschäftigten Personen vor dem Einsatz beim Auftragsverarbeiter zur Durchführung des Auftrags und sodann regelmäßig umfassend geschult.

b) Am Ende und auf Grundlage des in a) dieses Abschnitts festgelegten Schulungsprozesses werden die beim Auftragsverarbeiter zur Durchführung des Auftrags beschäftigten Personen auf die Vertraulichkeit und den Schutz personenbezogener Daten verpflichtet. Diese Verpflichtung erstreckt sich auf das Fernmeldegeheimnis und die damit verbundenen Grundsätze und Anforderungen an die Vertraulichkeit der Telekommunikation, wenn dies nach Maßgabe des konkreten Auftrags erforderlich ist, insbesondere wenn der Auftrag den Zugriff auf Verkehrsdaten umfasst.

c) Die Vergabe von Aufträgen an Unterauftragnehmer erfolgt ausschließlich schriftlich, nach Abschluss eines Auftragsverarbeitungsvertrages und eingehender Prüfung der beim Unterauftragnehmer etablierten Technischen und organisatorischen Maßnahmen.

d) Es wird ein zentrales Verzeichnis aller abgeschlossenen Auftragsverarbeitungsverträge der beauftragten Subunternehmer geführt.

e) Nach Beendigung der Zusammenarbeit mit Unterauftragnehmern werden diese angewiesen, sämtliche verarbeiteten personenbezogenen Daten ordnungsgemäß zu löschen.

4.6 GETRENNTE VERARBEITUNG VON DATEN/TRENNUNGSKONTROLLE

a) Sofern personenbezogene Daten auf informationsverarbeitenden Systemen des Auftragsverarbeiters gespeichert sind, wird eine vollständige Trennung der Personenbezogene Daten von personenbezogenen Daten anderer Auftraggeber realisiert und dadurch die jederzeitige und vollständige Identifizier- und Löschbarkeit von personenbezogene Daten sichergestellt, z.B., durch Speicherung der personenbezogenen Daten in einem eigenen Mandanten, in einer eigenen Partition oder unter eindeutigen Identifier getrennt abrufbar.

b) Eine entsprechende Trennung wird auch für personenbezogene Daten selbst realisiert, wenn sie zu verschiedenen Zwecken gespeichert werden.

4.7 WEITERGABEKONTROLLE

a) Personenbezogene Daten können nicht unbefugt kopiert (insbesondere auf externe Datenträger gespeichert), weitergegeben und/oder gelöscht werden.

b) Datenträger sowie sämtliche Dokumente, sofern sie Personenbezogene Daten enthalten (einschließlich sämtlicher gegebenenfalls vorhandener Sicherungskopien von personenbezogenen Daten und Kopien von Originaldokumenten) werden in ordnungsgemäß verschlossenen, und ausschließlich für die Durchführung des Auftrags genutzten Datensicherungsschränken verwahrt, wenn und solange sie nicht nach Maßgabe dieses Anhangs in der Bearbeitung sind.

c) Originaldokumente, die personenbezogene Daten enthalten, werden durch die den Prozess verantwortlich leitenden Personen an die zur Leistungserbringung eingesetzten Personen herauszugeben und von diesen nach Arbeitsschluss wieder entgegengenommen.

d) Den bei der Durchführung des Auftrags beschäftigten Personen ist die Anfertigung von handschriftlichen Aufzeichnungen nur in dem zur Leistungserbringung erforderlichen Umfang und auf besonders gekennzeichneten Arbeitsmitteln (z.B. paginiertes oder farbiges Papier) gestattet.

e) Nach Maßgabe dieses Anhangs herausgegebene Originaldokumente oder nach Maßgabe dieses Anhangs erstellte handschriftliche Aufzeichnungen werden, auch bei auch nur kurzzeitigem Verlassen des Arbeitsplatzes, vor unberechtigtem Zugriff geschützt (“Clean Desk Policy“).

f) Die den bei der Durchführung des Auftrags beim Auftragsverarbeiter beschäftigten Personen nutzen Client-Systeme die ausreichend gesichert sind. Alle Client Systeme sind mit Firewall und Virenschutz versehen und werden regelmäßig auf gängige Sicherheitsstandards überprüft.

g) Auf Durchführung des Auftrags vom Auftragsverarbeiter verwendeten Server-Systemen mit nicht-flüchtigem Speicher, z.B. Netzwerkdrucker oder Scanner, werden personenbezogene Daten nicht über den unmittelbar zur Vertragsdurchführung erforderlichen Umfang hinaus gespeichert. Sofern Dritte mit der Wartung solcher Systeme betreut sind, gilt Ziffer 5.3 dieses Anhangs entsprechend.

h) In den Räumlichkeiten des Auftraggebers bereitgestellte WLAN-Zugänge für den Netzwerkzugriff sind verschlüsselt.

i) Besteht nach Maßgabe des Auftrags für den Auftragsverarbeiter eine Pflicht zur Löschung von personenbezogenen Daten, wird der Auftragsverarbeiter

i. die datenschutzgerechte nicht wieder herstellbare Löschung sämtlicher, personenbezogene Daten enthaltender, löschbaren elektronischen Datenträger (insbesondere Festplatten, USB-Sticks, Disketten, Bänder) durchführen;

ii. die nachhaltige und irreversible Entfernung von personenbezogenen Daten aus Datenbank- oder File-Systemen sowie aus allen anderen löschbaren Speichermedien realisieren;

iii. sämtliche, personenbezogene Daten enthaltende Papierdokumente und sonstige nicht-gemäß (i) oder (ii) dieser Ziffer löschbaren Datenträger (einschließlich sämtlicher personenbezogene Daten enthaltener Fehldrucke, Speicherkarten, USB-Sticks, etc.) mit einem handelsüblichen Dokumentenvernichter gemäß der Sicherheitsstufe 3 gemäß DIN-Norm 32757 oder einem mindestens gleichwertigen Verfahren vernichten, wobei defekte magnetische Datenträger, die nicht wie oben angegeben mechanisch vernichtet werden können (z.B. defekte Festplatten), sind mittels eines zugelassenen Löschgerätes nach DIN 33858 zu löschen;

iv. die Löschung für die Dauer des Auftrages protokollieren.

4.8 VERFÜGBARKEIT UND BELASTBARKEIT (ART. 32 ABS. 1 LIT. B DSGVO)

a) Vom Auftragsverarbeiter zur Durchführung des Auftrags verwendete Server-Systeme werden durch Firewalls geschützt, welche diese Server-Systeme gegen nicht betriebsnotwendige Zugriffe sichern.

b) Sämtliche gegebenenfalls vom Auftragnehmer zur Durchführung des Auftrags verwendete Software wird aktualisiert gehalten und sicherheitsrelevante Aktualisierungen (insbesondere Updates, Patches, Fixes) werden unverzüglich eingespielt, nachdem diese vom Hersteller der Software allgemein verfügbar gemacht und vom Auftragsverarbeiter im Rahmen eines dem Stand der Technik entsprechenden Verfahren getestet werden. Bei als „kritisch" oder sinngemäß qualifizierten Aktualisierungen beträgt die Frist nach Satz 1 höchstens zwei (2) Tage.

c) Originaldokumente, die personenbezogene Daten enthalten, sowie beim Auftragsverarbeiter rechtmäßig auf informationsverarbeitenden Systemen gespeicherte Personenbezogene Daten werden durch technische und organisatorische Maßnahmen vor Verlust durch zufällige, fahrlässige oder vorsätzliche Löschung oder Veränderung geschützt.

d) Sicherungskopien von beim Auftragnehmer rechtmäßig auf informationsverarbeitenden Systemen gespeicherten personenbezogene Daten werden nach denselben Maßgaben wie Originaldaten behandelt, insbesondere gegen unbefugten Zugriff gesichert.

e) Sämtliche verwendeten Server-Systeme verfügen über Feuer- und Rauchmeldeanlagen, Feuerlöschsysteme, klimatisierte Serverräume, Schutzmaßnahmen gegen Überspannung, Videoüberwachung sowie Alarmmeldungssysteme bei unberechtigten Zutritten zum Serverraum.

f) Sämtliche Speichersysteme verfügen über redundante Speichermedien (z.B. RAID-Systeme, Spiegelungen oder vergleichbar).

g) Der Auftragnehmer verfügt über ein Backup- und Recovery-Konzept, das die Wiederherstellung von Backups der letzten 30 Tage ermöglicht.

h) Die Datenspeicherung erfolgt getrennt von der Speicherung von Betriebs- und Anwendungssystemen.

i) Die Speicherung von Daten und Backups erfolgt in mindestens zwei getrennten Brandschutzzonen.

j) Die Datenwiederherstellung wird regelmäßig getestet und das Testergebnis protokolliert.

4.9 DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN, PRIVACY BY DEFAULT

a) Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

b) Durch geeignete technische Maßnahmen (Selbstständiges Anstoßen und Bestätigen des Löschvorgangs) wird die einfache Ausübung des Widerrufsrechts der Betroffenen gewährleistet.

4.10 ORGANISATIONSKONTROLLE

a) Es wird ein externer Datenschutzbeauftragter durch den Auftragnehmer bestellt.

b) Der bestellte Datenschutzbeauftragte wird durch einen internen Mitarbeiter („Lead-Function Datenschutz") in seiner Arbeit unterstützt.

c) Sämtliche Mitarbeiter des Auftragnehmers werden mindestens einmal pro Jahr in Datenschutzfragen und vorliegenden Datenschutzkonzepten geschult. Schulungsmaterialien liegen schriftlich und als Schulungsvideos vor.

d) Für Mitarbeiter des Auftragnehmers gelten interne Richtlinien und Arbeitsanweisungen zu a. Umgang mit personenbezogenen Daten im Home-Office / Mobile-Office, b. Nutzung des betrieblichen Internetzugangs und des betrieblichen E-Mail-Accounts, c. Nutzung privater Geräte für betriebliche Tätigkeiten (Bring your own device).

e) Alle Mitarbeiter des Auftragnehmers werden schriftlich auf die datenschutzrechtliche Vertraulichkeit verpflichtet.

4.11 REGELMÄßIGE ÜBERPRÜFUNG UND WIRKSAMKEITSKONTROLLE

a) Die in diesem Anhang aufgeführten Maßnahmen werden mindestens einmal jährlich durch die Geschäftsführung und die ITLeitung in Zusammenarbeit mit dem Datenschutzbeauftragten überprüft.

b) Für den Fall, dass bei der Überprüfung festgestellt wird, dass sich technologische Standards oder organisatorische Prozesse geändert haben und solche Änderungen eine Anpassung der hier aufgelisteten Maßnahmen erforderlich machen, werden die dadurch erforderlich werdenden Anpassung unverzüglich umgesetzt. Dabei wird der Grundsatz der Angemessenheit beachtet.

c) Änderungen werden zudem auf ad hoc Basis durchgeführt, sofern dies aus Gründen der Sicherheit erforderlich ist.

d) Die Überprüfung sowie daraus resultierende Änderungen werden dokumentiert und abgelegt.