AUFTRAGSVERARBEITUNGSVEREINBARUNG

nach Art 28 Abs 3 DSGVO

PRINCEBERG – KI-Arbeitsplatz für Kanzleien

Fassung 5.0 vom 4.11.2026

Besonderer Hinweis (§ 864a ABGB). PRINCEBERG weist auf die **fett gedruckten** Punkte 6.3 (Speicherung und Meldungen durch den Anbieter der KI-Dienste, E-Mail-Dienstleister in den USA), 8.2 (Ausnahmen von der Löschung) und 9.2 (Grenzen der Einsicht) hin.

1 GEGENSTAND UND DAUER

1.1 Diese Vereinbarung („**AVV**“) regelt die Verarbeitung personenbezogener Daten, die PRINCEBERG als Auftragsverarbeiter für den Kunden als Verantwortlichen beim Betrieb der Plattform vornimmt. Sie ist Teil des Vertrags nach dem Bestellschein und gilt, solange PRINCEBERG solche Daten verarbeitet. Begriffe haben die Bedeutung, die der Plattformvertrag und die DSGVO ihnen geben. Gegenstand, Art, Zweck, Datenarten und Betroffene beschreibt Anhang A.

1.2 Für Daten des Kunden und seiner Nutzer, die PRINCEBERG zur Vertragsabwicklung, Zugangsverwaltung, Abrechnung, Sicherheit und zur Auswertung der Nutzung ohne Inhalte verarbeitet, ist PRINCEBERG Verantwortlicher; es gilt die Datenschutzerklärung von PRINCEBERG.

1.3 Der Kunde ist als Verantwortlicher für die Rechtmäßigkeit der Verarbeitung, die Rechtsgrundlage, die Information der Betroffenen und die Rechtmäßigkeit seiner Weisungen verantwortlich. Seine Rechte ergeben sich aus den Punkten 2, 5, 7 und 9.

2 WEISUNGEN (Art 28 Abs 3 lit a)

2.1 PRINCEBERG verarbeitet die Daten nur auf dokumentierte Weisung des Kunden, auch bei Übermittlungen in Drittländer, außer PRINCEBERG ist nach Unionsrecht oder dem Recht eines Mitgliedstaats zur Verarbeitung verpflichtet; dann teilt PRINCEBERG dies vorab mit, sofern das Recht es nicht verbietet.

2.2 Der Vertrag und die Nutzung der Plattform sind die Weisungen des Kunden; weitere erteilt er in Textform an haris@princeberg.com. Hält PRINCEBERG eine Weisung für rechtswidrig, informiert PRINCEBERG den Kunden unverzüglich (Art 28 Abs 3 Satz 3).

3 VERTRAULICHKEIT UND BERUFSGEHEIMNIS (lit b)

3.1 PRINCEBERG gewährleistet, dass alle Personen, die Kundendaten verarbeiten dürfen, vor Aufnahme der Tätigkeit schriftlich zur Vertraulichkeit und zum Datengeheimnis (§ 6 DSG) verpflichtet, über die Folgen einer Verletzung belehrt und auf die anwaltliche Verschwiegenheit nach § 9 RAO und § 40 RL-BA 2015 hingewiesen wurden. Die Verpflichtung gilt über das Ende der Tätigkeit hinaus. Das Muster legt PRINCEBERG auf Verlangen vor.

3.2 Bei Hausdurchsuchungen, Sicherstellungen und Herausgabeverlangen gilt Punkt 6.3 des Plattformvertrags.

4 SICHERHEIT (lit c)

4.1 PRINCEBERG trifft die technischen und organisatorischen Maßnahmen nach Art 32 DSGVO laut Anhang C, darf sie an den Stand der Technik anpassen, ohne das Schutzniveau zu senken, und überprüft ihre Wirksamkeit mindestens jährlich. Einzelheiten, die einen Nachbau erleichtern könnten, nennt das technische Detailblatt, das PRINCEBERG auf Anfrage unter Geheimhaltung übergibt.

5 UNTERAUFTRAGSVERARBEITER (lit d, Abs 2 und 4)

5.1 Der Kunde genehmigt die Unterauftragsverarbeiter in Anhang B und erteilt die allgemeine Genehmigung, weitere hinzuzuziehen oder zu ersetzen.

5.2 PRINCEBERG veröffentlicht jede beabsichtigte Hinzuziehung oder Ersetzung mindestens 30 Tage vor dem Wirksamwerden auf https://princeberg.com/rechtliches/unterauftragsverarbeiter und teilt sie dem Administrator in Textform mit. Der Kunde kann binnen 14 Tagen ab der Mitteilung aus wichtigem Grund widersprechen. Einigen sich die Parteien nicht, kann der Kunde den Vertrag zum Wirksamwerden der Änderung kündigen; bis dahin bleibt es beim bisherigen Stand.

5.3 PRINCEBERG legt jedem Unterauftragsverarbeiter durch Vertrag Datenschutzpflichten auf, die dieser AVV entsprechen (Art 28 Abs 4), und haftet dem Kunden nach Punkt 9 des Plattformvertrags für dessen Pflichten. Die Unterauftragsverarbeiter arbeiten nach eigenen Standardbedingungen; soweit diese von dieser AVV abweichen, nennt Anhang B die Abweichung. Mit diesen offengelegten Abweichungen genehmigt der Kunde die Unterauftragsverarbeiter.

6 ORT DER VERARBEITUNG, DRITTLÄNDER

6.1 PRINCEBERG speichert Kundendaten in Rechenzentren in der Europäischen Union. Die KI-Dienste verarbeiten Anfragen nach Angaben ihres Anbieters in Mitgliedstaaten der Europäischen Union (EU-Datenzone); Bereitstellungen, die Anfragen weltweit verarbeiten, verwendet PRINCEBERG nicht.

6.2 In Drittländer übermittelt PRINCEBERG personenbezogene Daten nur an die Empfänger in Anhang B und nur nach Kapitel V DSGVO (Standarddatenschutzklauseln nach dem Durchführungsbeschluss (EU) 2021/914 oder Angemessenheitsbeschluss). Zugriffe, die der Kunde selbst veranlasst (etwa durch einen von ihm angebundenen Dienst), sind keine Übermittlung durch PRINCEBERG.

6.3 **Der Anbieter der KI-Dienste prüft Ein- und Ausgaben der KI-Sprachmodelle auf missbräuchliche Nutzung. Die Prüfung erfolgt zuerst automatisiert, auch durch KI-Modelle; dabei werden Ein- und Ausgaben nicht gespeichert. Reicht die automatisierte Prüfung in einem Fall nicht aus oder fällt sie aus, kann der Anbieter markierte Ein- und Ausgaben in einem Speicher, der der Ressource von PRINCEBERG zugeordnet ist (keine Trennung je Kanzlei), in der Geografie dieser Ressource innerhalb der Europäischen Union speichern und von berechtigten Mitarbeitern im Europäischen Wirtschaftsraum sichten lassen. Eine feste Speicherfrist nennt der Anbieter nicht. Eine Ausnahme von dieser Speicherung besteht nicht. Nach dem Datenschutzanhang des Anbieters kann dieser offensichtliches Material über sexuelle Ausbeutung und sexuellen Missbrauch von Kindern, von dem er bei der Erbringung seiner Dienste Kenntnis erlangt, an das National Center for Missing and Exploited Children (USA) oder eine andere Behörde melden. Diese Speicherung und Meldungen beruhen auf den Bedingungen des Anbieters, nicht auf einer**

Weisung des Kunden; PRINCEBERG legt sie hier offen. Benachrichtigungen, die der Kunde einrichtet (etwa Fristenüberblick, Treffer eines Monitors), können Inhalte aus Akten enthalten; der E-Mail-Dienstleister nach Anhang B verarbeitet sie auch in den USA.

7 UNTERSTÜTZUNG, VERLETZUNGEN (lit e und f)

7.1 PRINCEBERG unterstützt den Kunden mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen betroffener Personen (Kapitel III DSGVO) und unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei seinen Pflichten nach Art 32 bis 36 DSGVO. Anträge, die PRINCEBERG erreichen, leitet PRINCEBERG unverzüglich weiter und beantwortet sie nicht selbst.

7.2 Wird PRINCEBERG eine Verletzung des Schutzes personenbezogener Daten des Kunden bekannt, informiert PRINCEBERG den Kunden unverzüglich, spätestens binnen 48 Stunden ab Kenntnis, in Textform an den Administrator und ergreift die erforderlichen Maßnahmen. Die Meldung enthält die Angaben nach Art 33 Abs 3 DSGVO, soweit bekannt, und wird ergänzt, sobald weitere Angaben vorliegen. Meldung an die Aufsichtsbehörde und Benachrichtigung der Betroffenen sind Sache des Kunden.

8 LÖSCHUNG UND RÜCKGABE (lit g)

8.1 Während der Laufzeit löscht der Kunde Kundendaten selbst. Gelöschte Dateien liegen 30 Tage im Papierkorb der Plattform. Frühere Fassungen von Dateien bleiben gespeichert, bis sie bereinigt werden; auf Verlangen bereinigt PRINCEBERG sie binnen 30 Tagen.

8.2 **Binnen 30 Tagen nach Ende der Abruffrist nach Punkt 5.5 des Plattformvertrags löscht PRINCEBERG alle Kundendaten samt früheren Dateifassungen und Protokollen nach Wahl des Kunden oder gibt sie zuvor zurück und bestätigt die Löschung in Textform. Kopien in Sicherungen und Betriebsprotokollen sind spätestens 90 Tage danach entfernt. Ausgenommen sind: (a) Vertrags- und Abrechnungsunterlagen (Bestellschein, Angebote, Bestellungen, Rechnungen, Zahlungen, Schriftverkehr über Abschluss, Änderung und Beendigung) mit den darin enthaltenen Angaben zum Kunden und zu den für ihn handelnden Personen, ohne Inhalte aus Akten; PRINCEBERG bewahrt sie als Verantwortlicher sieben Jahre ab Ende des Kalenderjahres auf, auf das sie sich beziehen, und darüber hinaus, solange sie für ein anhängiges Verfahren von Bedeutung sind (§ 132 BAO, § 212 UGB); (b) Daten, die PRINCEBERG nach Unionsrecht oder dem Recht eines Mitgliedstaats aufbewahren muss. Aufbewahrungspflichten des Kunden begründen keine Speicherung bei PRINCEBERG. Nicht sichern kann PRINCEBERG die Löschung von Inhalten, die der Anbieter der KI-Dienste zur Missbrauchsprüfung gespeichert hat (Punkt 6.3), und von Benachrichtigungen beim E-Mail-Dienstleister, solange dessen Vertrag mit PRINCEBERG läuft (Anhang B); diese Speicherungen beruhen auf den Bedingungen der Unterauftragsverarbeiter, nicht auf einer Rechtspflicht. PRINCEBERG legt sie hier offen.**

9 NACHWEISE UND KONTROLLEN (lit h)

9.1 PRINCEBERG stellt dem Kunden auf Anfrage alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten nach Art 28 DSGVO erforderlich sind, und ermöglicht Überprüfungen einschließlich Inspektionen durch den Kunden oder einen von ihm beauftragten, auch gegenüber PRINCEBERG zur Verschwiegenheit verpflichteten Prüfer. Überprüfungen sind 14 Tage vorher anzukündigen, finden in den üblichen Geschäftszeiten statt, stören den Betrieb nicht unangemessen und erfolgen ohne konkreten Anlass höchstens einmal im Kalenderjahr. Für

die Unterauftragsverarbeiter führt PRINCEBERG den Nachweis durch deren veröffentlichte oder zur Weitergabe freigegebene Prüfberichte und Zertifikate.

9.2 **Einsicht in Quellcode, Systemanweisungen, Prüfregeln und Modellkonfiguration gewährt PRINCEBERG nur, soweit sie zum Nachweis zwingend erforderlich ist, vor Ort und ohne Kopien.** Rechte der Aufsichtsbehörden bleiben unberührt.

10 HAFTUNG UND DAUER

10.1 Für die Haftung gilt Punkt 9 des Plattformvertrags; Ansprüche betroffener Personen nach Art 82 DSGVO bleiben unberührt. Die AVV kann nicht gesondert vom Vertrag gekündigt werden. Datenschutzanfragen des Kunden gehen an haris@princeberg.com.

ANHANG A – BESCHREIBUNG DER VERARBEITUNG

Gegenstand und Dauer: Betrieb der Plattform für den Kunden für die Dauer des Vertrags und der anschließenden Abruf- und Löschfristen.

Art der Verarbeitung: Speichern, Ordnen und Durchsuchen von Kundendaten; Auswertung durch KI-Sprachmodelle (Beantwortung von Fragen, Recherche, Entwürfe, Übersetzung); Texterkennung gescannter Dokumente; Spracherkennung beim Diktat; Übermittlung von Suchbegriffen an das Rechtsinformationssystem des Bundes (öffentliche Stelle, kein Auftragsverarbeiter); bei eingeschalteter Auslandsrecherche Übermittlung abstrakter Suchangaben ohne Personenbezug an einen Recherchedienst für ausländisches Recht außerhalb der EU (Punkt 5.4 des Plattformvertrags; kein Auftragsverarbeiter); Eintragungen in vom Kunden verbundene Kalender; Versand von Benachrichtigungen; Empfang und Ablage von Unterlagen, die der Kunde PRINCEBERG zur Erbringung der Leistung übermittelt; Löschung.

Zweck: Bereitstellung der Plattform für die anwaltliche Tätigkeit des Kunden.

Datenarten: Identifikations- und Kontaktdaten; Daten zu Mandaten, Verfahren und Verträgen; Finanzdaten; Inhalte von Dokumenten, Schriftsätzen und E-Mails; Protokolldaten. Soweit die Tätigkeit des Kunden es mit sich bringt, auch besondere Kategorien (Art 9 DSGVO) und Daten über Straftaten (Art 10 DSGVO).

Betroffene: Mandanten, Gegenparteien und deren Vertreter, Zeugen, Sachverständige und sonstige Verfahrensbeteiligte, Vertragspartner, Lieferanten und Beschäftigte des Kunden, sonstige in Kundendaten genannte Personen.

ANHANG B – UNTERAUFTRAGSVERARBEITER

Stand am Tag der Unterschrift: die Liste auf https://princeberg.com/rechtliches/unterauftragsverarbeiter in der Fassung vom 4.11.2026, die lautet:

Unterauftragsverarbeiter	Leistung	Ort der Verarbeitung	Garantie
Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland	Microsoft Azure: Betrieb der Plattform und der Datenbanken, Speicherung der Dokumente, Texterkennung (Eingabe und Ergebnis bis 24 Stunden zwischengespeichert), Spracherkennung, KI-Sprachmodelle, Schlüsselverwaltung, Betriebsüberwachung ohne Inhalte; Missbrauchsprüfung nach Punkt 6.3	Rechenzentren in der EU (Irland, Niederlande, Schweden); KI-Verarbeitung in Mitgliedstaaten der EU (EU-Datenzone); Zugriffe zu Support-, Wartungs- und Sicherheitszwecken nach dem Datenschutzanhang von Microsoft auch aus Drittländern	Datenschutzanhang von Microsoft in der jeweils geltenden Fassung (bei Unterschrift: Fassung vom 1.11.2026); Standarddatenschutzklauseln 2021/914 zwischen Microsoft Ireland und Microsoft Corporation; EU-US Data Privacy Framework nach Angaben von Microsoft
Microsoft Ireland Operations Limited (wie oben)	Microsoft 365: E-Mail und Ablage von PRINCEBERG, etwa wenn der Kunde PRINCEBERG Unterlagen per E-Mail schickt	Rechenzentren in der EU	wie oben
Plus Five Five, Inc. („Resend“), 2261 Market Street #5039, San Francisco, CA 94114, USA	Versand von System-E-Mails, Rechnungen und der vom Kunden eingerichteten Benachrichtigungen	Versand über Rechenzentren in Irland; Verarbeitung von Empfänger, Betreff, Inhalt und Zustellprotokollen überwiegend in den USA, auch durch Unterauftragsverarbeiter von Resend	Standarddatenschutzklauseln 2021/914, Modul 3; EU-US Data Privacy Framework nach Angaben von Resend

Keine Unterauftragsverarbeiter sind Dienste, die der Kunde selbst anbindet, sein Single Sign-on, das Rechtsinformationssystem des Bundes (Empfänger von Suchbegriffen) und der Recherchedienst für ausländisches Recht (erhält keine personenbezogenen Daten).

Offengelegte Abweichungen der Standardbedingungen (Punkt 5.3): (1) Microsoft speichert bei der Missbrauchsprüfung markierte Ein- und Ausgaben ohne feste Frist und kann Material über Kindesmissbrauch an Behörden melden (Punkt 6.3); nicht gleichwertig, offengelegt. (2) Microsoft meldet Verletzungen unverzüglich ohne Stundenfrist; die Frist nach Punkt 7.2 läuft ab Kenntnis von PRINCEBERG. (3) Eigene Unterauftragsverarbeiter von Microsoft und Resend: allgemeine Zustimmung, Ankündigung durch den Anbieter, Einspruch nur durch Kündigung des Dienstes; PRINCEBERG leitet Ankündigungen weiter. (4) Überprüfungen bei Microsoft und Resend nur durch Prüfberichte und unabhängige Prüfer. (5) Personal von Microsoft und Resend ist zur Vertraulichkeit verpflichtet, nicht einzeln auf § 9 RAO. (6) Resend löscht Daten erst binnen 90 Tagen nach Ende des Kontos von PRINCEBERG. (7) Behördenersuchen: Microsoft verweist an PRINCEBERG, verständigt, soweit nicht verboten, und gibt nur das Mindestmaß heraus.

ANHANG C – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Zutritt: Betrieb in zertifizierten Rechenzentren (ISO/IEC 27001) in der Europäischen Union; PRINCEBERG betreibt keine eigenen Server mit Kundendaten.

Zugang: Persönliche Zugänge; Zwei-Faktor-Authentifizierung und Single Sign-on; zeitlich begrenzte Sitzungen; Begrenzung von Anmeldeversuchen; Beschränkung auf freigegebene IP-Adressen durch den Administrator.

Zugriff: Rollen und Berechtigungen je Kunde und Akt; Trennung der Daten jedes Kunden; Zugriff von Mitarbeitern von PRINCEBERG nur im Einzelfall zur Störungsbehebung, auf Ersuchen des Kunden oder zur Erfüllung einer Pflicht; Geheimnisse außerhalb des Programmcodes.

Weitergabe: Verschlüsselte Übertragung; Weitergabe nur an die Unterauftragsverarbeiter nach Anhang B; an die Empfänger von Suchangaben gehen keine personenbezogenen Daten; Protokoll der Auslandsrecherche; kein Training von KI-Modellen mit Kundendaten.

Eingabe: Prüfprotokoll sicherheitsrelevanter Vorgänge; Änderungen an Akten, Fristen, Beteiligten und Aufgaben durch die Plattform erst nach Freigabe, außer bei der vom Kunden eingestellten automatischen Übernahme.

Verfügbarkeit: Regelmäßige Sicherung der Datenbanken mit zeitpunktgenauer Wiederherstellung; Versionierung und Papierkorb für Dateien; Betriebsüberwachung.

Verschlüsselung, Pseudonymisierung: Verschlüsselung im Ruhezustand und bei der Übertragung; wählbare automatische Pseudonymisierung personenbezogener Angaben vor der Verarbeitung durch das Sprachmodell; sie kann Angaben übersehen, der Kunde prüft das Ergebnis.

Organisation: Schriftliche Verpflichtung der Mitarbeiter (Punkt 3); Ablauf zur Meldung von Verletzungen (Punkt 7.2); Löschkonzept (Punkt 8); jährliche Überprüfung (Punkt 4). Weitere Einzelheiten im technischen Detailblatt auf Anfrage unter Geheimhaltung.