Beschreibung der Verarbeitung personenbezogener Daten

Kleos

Beschreibung der Verarbeitung personenbezogener Daten und leistungsbezogene technische und organisatorische Maßnahmen

Dieser Anhang ist Bestandteil des Auftragsverarbeitungsvertrags („AVV“) zwischen dem Dienstleister und dem Kunden.

1. Verarbeitung personenbezogener Daten

Der Dienstleister darf als Auftragsverarbeiter im Rahmen der Erbringung von Software-Services bzw. Professional Services personenbezogene Daten des Kunden in seinem Auftrag und nach seiner Anweisung verarbeiten:

- Installation und Konfiguration
- Hosting und Beaufsichtigung (cloudbasierte Version)
- Datenmigration
- Support und Wartung

Zwischen dem Dienstleister und dem Kunden gelten insoweit die Bestimmungen des Vertrages und der Auftragsverarbeitungsvertrag („AVV“), ergänzt durch nachfolgende Konditionen.

1.1 Kategorien von personenbezogenen Daten, die verarbeitet werden

Als Datenverantwortlicher kann der Kunde in KLEOS Kundendaten, einschließlich personenbezogener Daten, eingeben, speichern und bearbeiten. Der Anbieter als Verarbeiter hat im Voraus keine Kenntnis über die Art der vom Kunden erstellten, eingegebenen und in KLEOS hochgeladenen personenbezogenen Daten.

In seiner Standardkonfiguration bietet KLEOS grundlegende Felder, die vom Kunden ausgefüllt werden können, um persönliche Daten wie Name, Adresse, Telefonnummer, E-Mail-Adresse, Geburtsdatum usw. zu bearbeiten.

Zusätzliche optionale Informationen können ebenfalls eingegeben werden, wenn dies im Rahmen eines bestimmten Geschäftsprozesses erforderlich ist (Geschäftsadresse, Geschäftstelefon usw.), je nach dem vom Kunden festgelegten Verarbeitungszweck. Das Vorhandensein solcher Felder ist das Ergebnis einer bewussten Entscheidung des Kunden während der Projektphase (vom Kunden beim Dienstleister angeforderte Einstellungen) oder während der Verwaltung der Softwaredienste (vom Kunden oder einem Dritten im Namen des Kunden vorgenommene Konfiguration/Einstellung) und unterliegt somit der alleinigen Verantwortung des Kunden.

In der Standardkonfiguration von KLEOS gibt es keine Freitext-Kommentarfelder im Verzeichnis der natürlichen Personen. Das Vorhandensein eines solchen Feldes ist das Ergebnis einer bewussten Entscheidung des Kunden in der Projektphase (Einstellung/Konfiguration, die der Kunde beim Anbieter beantragt) oder während der Verwaltung der Software-Services (Konfiguration/Einstellung, die vom Kunden oder einem Dritten im Namen des Kunden vorgenommen wird) und unterliegt somit der alleinigen Verantwortung des Kunden.

A. Nutzerdaten
- Vorname, Nachname
- Geschlecht
- Passwort
- Funktion
- Fakultativ: Kontaktangaben (E-Mail, Telefon, Adresse)

B. Daten von Mandanten/Verfahrensbeteiligten
- Vor- und Nachname (ggf. Titel), Anrede
- Datum der Geburt
- Karriere/Berufsfeld
- Familienstand

- Kontaktdaten und -verlauf (insbesondere Adresse, E-Mail-Adresse, Telefonnummer)
- Daten zur Unternehmensgeschichte
- Finanzdaten, Daten zu Finanztransaktionen
- Bankverbindung und Zahlungsmodalitäten
- Daten für die Rechnungsstellung
- Steuerliche Daten
- Mandatsbezogene Akten und/oder Dokumente

Personenbezogene Daten werden von den Nutzern über die Funktionen der Softwaredienste zu den hier beschriebenen Zwecken eingegeben. Personenbezogene Daten werden nicht direkt von den betroffenen Personen selbst erhoben. Die vom für die Verarbeitung Verantwortlichen erstellten, eingegebenen und in KLEOS hochgeladenen personenbezogenen Daten liegen im alleinigen Ermessen und Risiko des für die Verarbeitung Verantwortlichen.

2.1 Kategorien von betroffenen Personen

Als Datenverantwortlicher kann der Kunde in KLEOS persönliche Daten eingeben, speichern und bearbeiten, auch von den folgenden Personen:

- Mitarbeiter des Kunden, Kunden und sonstige Vertragspartner des Kunden
- Andere Personen, über die der Kunde Daten in Kleos erfasst und speichert (z.B. Verfahrensbeteiligte, Parteien, Anwälte der gegnerischen Partei, externe Kollegen, die an einem Fall beteiligt sind, Sachverständige, Zeugen)

3.1 Zweck der Verarbeitung

Der Auftraggeber als Verantwortlicher ist für die Bestimmung des Zwecks der mit KLEOS durchgeführten Verarbeitung verantwortlich. KLEOS kann für die folgenden Zwecke verwendet werden:

- Fallbearbeitung
- Erfüllung des Mandats
- Kommunikation mit Kunden
- Rechnungsstellung
- Übermittlung an Gerichte, Versicherungsgesellschaften, Dritte, Bevollmächtigte
- Nutzungsstatistik (
  kann vom Benutzer deaktiviert werden - Benutzerentscheidung)

Nutzungsstatistiken helfen uns, das Produkt für Sie zu verbessern. Eine Weitergabe von Daten findet nicht statt.
Die Nutzungsstatistik kann deaktiviert werden, wodurch die auf Basis der Nutzungsdaten ermittelten Hilfe- und Informationsboxen nicht mehr zur Verfügung stehen.
Die Rechtsgrundlage für diese Verarbeitung ist in Art. 6 (1) (1) (f) GDPR.

Für das ordnungsgemäße Funktionieren von Kleos ist keine Verbindung mit anderen Systemen erforderlich, und insbesondere werden keine Informationen aus dem Verzeichnis natürlicher Personen in andere Systeme exportiert. Verbindungen, die auf Wunsch des Kunden zwischen KLEOS und anderen vom Kunden verwalteten Systemen hergestellt werden, unterliegen der Aufsicht und alleinigen Haftung des Kunden.

4.1 Art der Verarbeitung

Die Verarbeitung hängt von den Dienstleistungen ab, die der Auftragsverarbeiter im Rahmen der Vereinbarung erbringt, und kann die Aufzeichnung, Organisation, Änderung, Extraktion, Abfrage, Offenlegung durch Übermittlung, Speicherung, Einschränkung, Löschung oder Vernichtung umfassen.

5.1 Aufbewahrungsfrist

Als für die Datenverarbeitung Verantwortlicher bestimmt der Auftraggeber die Aufbewahrungsfrist für die von/in KLEOS verwalteten personenbezogenen Daten (Vertragsakten, Streitfälle, Kontaktinformationen, zugehörige Dokumente usw.).

Im Cloud-Modus speichert der Anbieter die Kundendaten und erstellt Sicherungskopien der Kundendaten während der Laufzeit dieses Vertrags in Übereinstimmung mit den Bestimmungen des Vertrags, einschließlich derjenigen dieses Anhangs. Im Vor-Ort-Modus ist der Kunde für den Schutz und die Sicherung der Softwaredienste, ihrer Installation und der Kundendaten verantwortlich.

Der Dienstleister als Auftragsverarbeiter bewahrt die Kundendaten, gegebenenfalls auch personenbezogene Daten, in den folgenden Fällen und während der folgenden Aufbewahrungsfristen auf (vorbehaltlich gesetzlicher Verpflichtungen oder Verjährungsfristen):

- Personenbezogene Daten über den Support (Informationen, die der Kunde für Wartungstickets bereitstellt): Kundendaten, einschließlich ggf. personenbezogener Daten, werden sechs (6) Monate nach Ablauf der Vereinbarung aus den Support-Datenbanken des Anbieters gelöscht; als für die Datenverarbeitung Verantwortlicher stellt der Kunde sicher, dass bei der Meldung und Bearbeitung eines Fehlers an die Support-Dienste des Anbieters keine personenbezogenen Daten (in Form von Screenshots usw.) an den Auftragsverarbeiter übermittelt werden;

- Kopieren von Kundendaten (DUMP) zur Unterstützung: Um ein technisches Problem zu lösen, kann es erforderlich sein, dass der Anbieter einen Teil der Kundendaten, gegebenenfalls auch personenbezogene Daten, in eine Testumgebung kopiert, nachdem er die Zustimmung des Kunden eingeholt hat. Diese Kundendaten werden nur zur Lösung des jeweiligen Problems verwendet und spätestens zwei (2) Monate nach Behebung des Problems aus der Testumgebung gelöscht;

- Nach der Datenmigration: Der Anbieter wird die migrierten Daten für einen Zeitraum von zwei (2) Monaten aufbewahren, um die Korrekturen in diesem Zeitraum abzuschließen, falls erforderlich. Der Kunde ist dafür verantwortlich, die Daten zu kopieren/zu sichern und sie dem Anbieter nach diesem Zeitraum bei Bedarf zur Verfügung zu stellen;

- Nach Beendigung/Ablauf des Vertrages: Im Rahmen der im Vertrag vorgesehenen Reversibilitätsdienste werden die Kundendaten, sofern vorhanden, in dem vereinbarten Format an den Kunden übermittelt. Der Anbieter bewahrt dann die entsprechenden Datenbanken für zwei (2) Monate (oder einen anderen im Vertrag festgelegten Zeitraum) auf seinen Servern auf, bevor er sie vorbehaltlich der gesetzlichen Aufbewahrungspflichten vollständig vernichtet.

2. Technische und organisatorische Sicherheitsmaßnahmen

Der Anbieter ergreift die geeigneten technischen und organisatorischen Sicherheitsmaßnahmen ("TOMs"), die auf der Grundlage des Stands der Technik zum Zeitpunkt des Vertragsabschlusses bewertet werden, und der Anbieter bewertet diese TOMs im Laufe der Zeit, wobei er die Kosten der Umsetzung, die Art, den Umfang, den Kontext und die Zwecke der Verarbeitung sowie die Wahrscheinlichkeit hoher Risiken für die Rechte und Freiheiten der betroffenen Personen berücksichtigt.

Kleos ermöglicht durch die nachfolgenden technischen und organisatorischen Maßnahmen die Umsetzung der Grundsätze des Datenschutzes und die Einhaltung der Rechte der Betroffenen:

2.1 Zugangskontrolle: Rechenzentrum / Hosting IT-Infrastruktur

Standort des Rechenzentrums	Innerhalb der EU/EEA Primäres Rechenzentrum: Deutschland, Frankfurt Sekundäres Rechenzentrum: Deutschland, Berlin https://azure.microsoft.com/de-de/explore/global-infrastructure/geographies/#choose-your-region
Zertifizierung von Rechenzentren	ISO/IEC 27001:2013
Geo-Redundanz	Kundendaten werden durch georedundante Speicherung gegen den Verlust eines Rechenzentrums geschützt.
Web-Anwendungs-Firewall	Innerhalb der EU/EWR Regionale Dienste mit begrenzter Verkehrslenkung innerhalb der EU

2.2 Schutz und Wiederherstellung von Daten

Richtlinie zur Aufbewahrung von Sicherungskopien	**Frequenz:**	**Beibehaltung:**
	Täglich	30 Tage
	Wöchentlich (vollständige Backups)	7 Wochen
	Monatlich (Vollsicherung)	4 Monate
Externe Backups (auf Kundenwunsch)	Ein Kunde hat die Möglichkeit, gegen gesonderte Bestellung und Bezahlung ein Backup seiner Daten anzufordern. Die Bereitstellung des Backups kann online oder mittels verschlüsselter Datenträger erfolgen.	

2.3 Datenverschlüsselung und Schutz des Datenaustauschs

Kommunikation zwischen Client und Server	HTTPS-Protokoll, gesichert mit TLS (Transport Layer Security) unter Verwendung von Version 1.2 und AES 256
Verwaltungsinformationen/Metadaten	Alle gespeicherten Daten werden mit AES256 verschlüsselt. Die für die Verschlüsselung verwendeten Schlüssel werden in einem sicheren Schlüsselverwaltungssystem mit strenger, geregelter Zugangskontrolle durch Wolters Kluwer gespeichert und geschützt.
Daten im Ruhezustand	Alle gespeicherten Daten werden mit AES256 verschlüsselt. Die für die Verschlüsselung verwendeten Schlüssel werden in einem sicheren Schlüsselverwaltungssystem mit strenger, geregelter Zugangskontrolle durch Wolters Kluwer gespeichert und geschützt

Daten im Transit	Die Client-Kommunikation ist mit TLS 1.2 und AES-256-Verschlüsselung gesichert.
Schlüsselverwaltung	Alle Verschlüsselungsschlüssel werden durch den Einsatz eines Hardware-Sicherheitsmoduls (HSM) geschützt.

2.4 Mittel zur Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und ständigen Belastbarkeit von Verarbeitungssystemen und -diensten

Minimierung der Datenmenge	Erstellung von Benutzern: Für das Anlegen von Benutzern sind nur der Name, der Vorname, die Rolle (Profil), die E-Mail-Adresse und das Passwort des Benutzers erforderlich.
Begrenzung der Speicherdauer	**Benutzerdaten:** Anonymisierung der Daten bei Deaktivierung des Zugangs durch den Kunden.
Informationen über Daten	Auskunft über den Umfang der gespeicherten Daten können jederzeit von den dazu berechtigten Nutzern erteilt werden.
Löschung von Daten	Manuelle Löschungsroutinen oder Anonymisierung
Berichtigung von Daten	Die Adressen natürlicher Personen können jederzeit von den dazu berechtigten Nutzern geändert werden.

2.5 Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Sicherheitsscans	Die technische Lösung von Kleos wird regelmäßig auf sicherheitsrelevante Schwachstellen geprüft.
Penetrationstests	Das Kleos-Produkt wird in regelmäßigen Abständen von internen und externen Penetrationstestern geprüft.
Geschäftskontinuitätsplan	Der Business Continuity Plan (BCP) für die Kleos-Plattform umfasst eine detaillierte Strategie und eine Reihe von Systemen, um eine erhebliche Unterbrechung des Betriebs zu verhindern oder bei Bedarf eine schnelle Wiederherstellung durchzuführen. WOLTERS KLUWER hat einen Business Continuity Plan für die Kleos Plattform entwickelt und überprüft diesen in regelmäßigen Abständen.
Ebene der Infrastruktur	Die technische Lösung von Kleos wird aktiv auf bösartige Software gescannt.
Kleos Speicherfunktionen (z.B. Dokumenten-Upload)	Wenn eine Datei in das KLEOS-Produkt übertragen wird (z. B. beim Speichern eines Dokuments), wird diese auf bösartige Inhalte überprüft

Empfehlung	Achten Sie auch auf die Sicherheit Ihrer Endgeräte. Wir empfehlen Ihnen, alle Endgeräte mit Passwörtern oder biometrischer Sicherheit gegen unbefugten Zugriff zu schützen. Ebenso sollten auf allen Endgeräten Datenträgerverschlüsselungs- und Malwareschutzsoftware installiert und auf dem neuesten Stand sein. Stellen Sie sicher, dass das Betriebssystem regelmäßig aktualisiert wird.

3. Lernen und Vorschlagen & Crashreports

3.1 Lernen und Vorschlagen

Sie erhalten interaktive Vorschläge in Form von Hilfetexten und Videos in Abhängigkeit von Ihrer Nutzung der Software. Zur kontinuierlichen Verbesserung der Nutzererfahrung erheben wir zusätzlich die nachfolgenden Daten.
Diese Datenerhebung kann selbstverständlich auf Wunsch deaktiviert werden. Bitte beachten Sie, dass durch die Deaktivierung dieser Funktion die interaktiven Vorschläge nicht mehr angeboten werden. Bitte verwenden Sie in diesem Fall ausschließlich die Dokumentationen.

Auf Ebene der Anwaltskanzlei

- Anzahl der Besucher (Nutzer), die sich tatsächlich mit Kleos verbunden haben
- Datum des ersten und letzten Logins auf Kleos
- Anzahl der aktiven Tage auf Kleos (alle Besucher zusammen)
- Anzahl der Klicks innerhalb von Kleos (alle Besucher zusammen)
- Aufenthaltsdauer in Kleos (alle Besucher zusammen)
- Sprache des Benutzers (wie in Kleos eingestellt)
- Genutzte Funktionen

A. Systemdaten:

- Name des Betriebssystems des Geräts, das bei der letzten Anmeldung bei Kleos verwendet wurde (z.B.: Windows, Mac OS, iOS)
- Name und Version des Browsers, der bei der letzten Anmeldung bei Kleos verwendet wurde
  ODER (für Kleos mobile): Typ des mobilen Geräts (z.B.: iPhone 13 pro)
- Gerätetyp (Desktop/Laptop, Handy, Tablet)

Weitere Daten als die oben aufgeführten Daten werden nicht an uns übermittelt. Insbesondere werden keinerlei personenbezogene Daten der einzelnen Anwender (z.B. Name, Ort, Registrierungs-Schlüssel, Client-IP-Adresse) übermittelt. Eine – auch nachträgliche – Zuordnung der an uns übermittelten Daten zu einzelnen Nutzern ist nicht möglich.

Die Übermittlung der vorgenannten Daten erfolgt automatisch. Die Übermittlung findet in der Regel einmal pro Sitzung beim Beenden der Anwendung statt.

Zweck der Datenverarbeitung

Die Erhebung dieser Daten dient vornehmlich der Aus- und Weiterbildung des Anwenders im Hinblick auf die Anwendung der Software. Zusätzlich helfen die erhobenen Daten die Nutzerfreundlichkeit, Effektivität und Sicherheit der Software kontinuierlich zu verbessern.

In diesen Zwecken liegt auch unser berechtigtes Interesse an der Datenverarbeitung nach Art. 6 Abs. 1 Satz 1 lit. f DSGVO.

3.2 Crashreports

Für die Meldung von Crashreports verwenden wir den intern entwickelten Mechanismus "Elsatrace". Die Rechtsgrundlage für diese Verarbeitung ist in Art. 6 (1) (1) (b) GDPR.

Welche Daten sammelt Elsatrace von den Nutzern?

Zu den gesammelten Daten gehören unter anderem: Benutzer- und Datenbankkennung, Fehlerbeschreibung und Fehlercode, genauer Zeitpunkt des Fehlers.

Wie verwendet Wolters Kluwer die gesammelten Informationen?
Die gesammelten Daten und Informationen werden verwendet, um unseren Entwicklern einen Einblick in die Funktionalität und Handhabung ihrer Anwendungen zu geben, einschließlich aller aufgetretenen Probleme.

Gibt es eine Möglichkeit für die Nutzer, die Sammlung von Daten und Informationen zu verhindern?
Nein.

Wir verwenden ein von Wolters Kluwer selbst entwickeltes ETL-Tool (Extract, Transform, Load), um die Nutzung zu analysieren und die folgenden Daten zu sammeln:

Verwendungsdaten

- Name der Datenbank
- Eröffnung der Anwendung
- Abschluss der Anwendung
- Wie oft eine Funktion verwendet oder eine bestimmte Funktionsoption ausgewählt wurde.

Andere als die oben genannten Daten werden nicht an uns übermittelt. Insbesondere werden keine personenbezogenen Daten der einzelnen Nutzer (z.B. Name, Standort, Registrierungsschlüssel, Client-IP-Adresse) übermittelt. Keine der an uns übermittelten Daten können - auch im Nachhinein - einzelnen Nutzern zugeordnet werden.
Die vorgenannten Daten werden automatisch an uns übermittelt. Die Übermittlung erfolgt in der Regel einmal pro Sitzung, beim Beenden der Anwendung.
Alle so übertragenen Daten werden verschlüsselt und über https versendet. Vor der Übertragung werden die Daten unverschlüsselt auf der Festplatte des jeweiligen Nutzer-PCs gespeichert. Dies bietet jedem Nutzer die Möglichkeit, selbst eine genaue Analyse vorzunehmen und sich zu vergewissern, dass keine persönlichen Daten übermittelt werden.

Zweck und Rechtsgrundlage der Datenverarbeitung
Wir setzen Analysewerkzeuge ein, um u.a. die Benutzerfreundlichkeit, Effektivität und Sicherheit unserer Produkte zu verbessern. Dazu benötigen wir Informationen über die Hard- und Software in Ihrer Kanzlei sowie über das Nutzungsverhalten der Anwender.
Diese Zwecke umfassen auch unser berechtigtes Interesse an der Datenverarbeitung gemäß Art. 6 (1) (1) (f) GDPR.

Dauer der Lagerung
Die Daten von Absturzberichten werden nicht dauerhaft gespeichert. Die Daten der Nutzungsstatistiken werden 12 Monate lang aufbewahrt.

Gelegenheit zum Einspruch
Der Nutzer hat keine Möglichkeit, diese Datenübertragung abzuschalten.

4. Unterauftragnehmer

Ein angemessenes Schutzniveau für die Handhabung und Verarbeitung personenbezogener Daten wird durch die sorgfältige Auswahl von Unterauftragnehmern und den Abschluss von Auftragsverarbeitungsverträgen gemäß Art. 28 GDPR.

Der Kunde akzeptiert, dass der Dienstleister als Auftragsverarbeiter Unterauftragsverarbeiter mit der Durchführung bestimmter Datenverarbeitungstätigkeiten (einschließlich der Verwaltung von Cloud-Diensten, Hosting-Diensten, Softwareentwicklung, Support- und Wartungsdiensten usw.) im Auftrag des Kunden beauftragen kann:

Zu den in der gruppeninternen Übertragungsvereinbarung innerhalb der Wolters-Kluwer-Gruppe genannten Anbietern gehören die folgenden:

Name	**Adresse**	**Tätigkeit**	**Lokalisierung von Daten**
Wolters Kluwer Technology B.V.	Zuidpoolsingel 2 2408 ZE Alphen aan den Rijn, Die Niederlande	Softwareentwicklung und 2nd-Level-Support	Niederlande
Wolters Kluwer Italia S.r.L	Centro Direzionale Milanofiori Strada 1, Palazzo 6 20090 Assago Italien	IT-Betrieb, 2nd Level Support	Daten Wohnsitz: Deutschland
Wolters Kluwer Global Business Services Italia.	Via dei Missaglia 97, 20142 Mailand, Italien	Cloud-Management	Primäres Rechenzentrum: Microsoft Azure Deutschland West Central - Frankfurt am Main Sekundäres Rechenzentrum: Microsoft Azure Deutschland Deutschland Nord - Berlin Web Application Firewall (WAF): Microsoft Azure Deutschland Cloudflare Regional Services begrenzte Verkehrsabwicklung innerhalb der EU Daten-Residenz: Deutschland Wolters Kluwer Technology B.V. , Zuidpoolsingel 2 2408 ZE Alphen aan den Rijn, Die Niederlande , Softwareentwicklung und 2nd-Level-Support , Niederlande
Wolters Kluwer Global Business Services B.V.	Zuidpoolsingel 2 2408 ZE Alphen aan den Rijn, Die Niederlande	SMS & Email-Massenversand	Niederlande

Dritte Sub-Verarbeiter

Name	Adresse	Tätigkeit	Lokalisierung von Daten
T-Systems International GmbH	Rechenzentrum München/Allach Dauchauer Straße 665 80995 München Rechenzentrum München/Eip Elisabeth Selbert Straße 1 80939 München	Cloud-Management	Deutschland
Teleperformance Portugal SA	Av. Alvaro Pais 2 1600-873 Lissabon Portugal	1st Level Software-Unterstützung	Portugal
Salesforce.com	Floor 26 Salesforce Tower, 110 Bishopsgate, EC2N 4AY London, Vereinigtes Königreich	Supportticket-Verwaltung	Vereinigtes Königreich
TeamViewer	TeamViewer GmbH Jahnstr. 30 73037 Göppingen, Deutschland	Fernunterstützung	Europa

Kleos

Wolters Kluwer Legal Software Deutschland GmbH

Wolters-Kluwer-Straße 1
D-50354 Hürth

Tel.: +49 (2233) 2055 - 000
Fax: +49 (2233) 2055 - 010
E-Mail: vertrieb.software-recht@wolterskluwer.com

wolterskluwer.de