Beschreibung der Verarbeitung personenbezogener Daten

Kleos SMART Beleg

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 Art der personenbezogenen Daten, die verarbeitet werden

Gegenstand der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten sind folgende Datenarten/ -kategorien:

Personendaten (im Rahmen der Nutzerverwaltung/-berechtigung sowie ggf. im Rahmen der Buchhaltung)

- Vorname und Nachname
- ggf. Position / Funktion
- Kommunikationsdaten (insb. Nutzerverwaltung, Telefon, E-Mail,
- ggf. Fax)
- Zahlungsdaten
- Bankverbindungen (Kontoinhaber, Bankinstitut, IBAN, BIC)
- Transaktionsdaten (u.a. Verwendungszweck, Betrag, Buchungs-datum/zeit, Transaktionsnummer)
- ggf. Bankkonto Anbindung und Nutzung der Überweisungsfunktion
- Daten, die zur Buchhaltung erforderlich sind (abhängig von Umfang)
- Rechnungsdaten
- Angebotsdaten
- Daten von Debitoren
- Kreditoren & Interessenten

1.2 Betroffene / Kategorien von Betroffenen

Die Kategorien betroffener Personen umfassen:

- Ansprechpartner / Nutzer
- Debitoren
- Kreditoren
- Interessenten
- Steuerberater
- Ggf. Geschäftspartner, Mitunternehmer, Gesellschafter u.ä.

Die tatsächlich betroffenen Kategorien betroffener Personen können je nach Kunden und nach Umfang der Verarbeitungstätigkeiten, insbesondere je nach den auf Dokumenten/Belegen angegebenen Daten variieren. Die angegebenen Kategorien decken jedoch i.d.R. die betroffenen Kategorien ab.

1.3 Art und Zweck der Verarbeitung (Beschreibung der Verarbeitung)

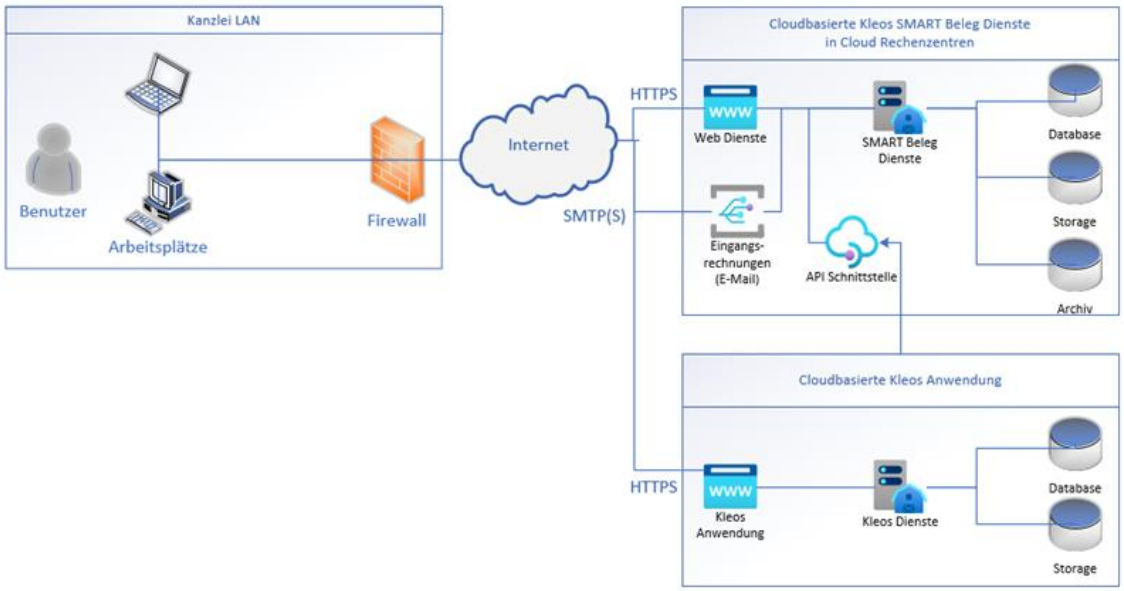
Der Gegenstand des Auftrags ergibt sich aus dem dazugehörigen mit dem Dienstleister geschlossenen Vertrag über entsprechende Nutzungsrechte an der Software Kleos Finanzbuchhaltung (im Folgenden Leistungsvereinbarung). Sofern der Dienstleister zu einem späteren Zeitpunkt weitere Nutzungsrechte oder sonstige zusätzliche Leistungen beauftragt, so gilt diese Vereinbarung entsprechend auch für diese Leistungen.

2. Technische und organisatorische Sicherheitsmaßnahmen

Nachfolgend stellt der Dienstleister die technischen und organisatorischen Maßnahmen dar, die jeweils in seinem Verantwortungsbereich oder im Rechenzentrum des in Nr. 3. genannten Unterauftragnehmers getroffen worden sind.

Die Kommunikation zwischen dem Arbeitsplatz / Server des Kunden und den Rechenzentren des Dienstleisters erfolgt grundsätzlich über gesicherte Übertragungswege wie z.B.: das HTTPS Protokoll (TLS 1.2 oder höher). Hierdurch werden die Vertraulichkeit und Integrität der Daten während der Übertragung sichergestellt

2.1 IT Architektur (Schematisch)



2.2 Zugangskontrolle: Rechenzentrum / Hosting IT-Infrastruktur

A) Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen (geeignete Maßnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet, zu verwehren):

- Schließsystem mit Codesperre
- Chipkarten / Transpondersysteme
- Besucher: Anmeldung und Protokoll am Empfang
- Besucher nur in Begleitung durch Mitarbeiter
- Empfang, 24/7 Security im Eingangs- und Außenbereich

Die eigenen Büro- und Geschäftsräume des Unterauftragnehmers sind mit verschlossenen Türen und Schließsystemen versehen, so dass ein unbefugter Zutritt von Dritten wirksam unterbunden werden kann. Während der Geschäftszeiten gibt es eine Besucherregelung, die unter anderem vorsieht, dass jeder Besucher sich nicht ohne Begleitung durch die Büroräume bewegen kann.

Im Rechenzentrum sind folgende Maßnahmen getroffen:

- Zutritt zum Gebäude nur durch Legitimation über eine persönliche Code-Karte (RFID)
- Besucher können nur nach vorheriger Anmeldung das Gebäude betreten. Während des gesamten Aufenthalts begleitet mindestens ein Mitarbeiter die Gäste, welche einen gesonderten Ausweis erhalten, der jedoch keinen Zutritt zu geschützten Bereichen ermöglicht
- Wachschutz 24h/Tag, 365 Tage im Jahr, Kontrollgänge werden durchgeführt
- Alarmanlagensystem mit Aufschaltung auf örtliche Polizeidienststellen
- abgesichertes Rechenzentrum mit eigenem Eingang, geschützt durch speziell codierte Zugangskarten (personenbezogen, RFID)
- Schleusensystem, Kameraüberwachung und Protokollierung von Zugängen sichern den Aufenthalt ab
- Serverracks sind verschlossen und werden nur im Bedarfsfall geöffnet. Die Schlüssel zu den Racks liegen in einem verschlossenen Safe, zu dem nur autorisierte Personen Zugang haben

B) Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Login mit Benutzername sowie geeignetem Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, bedarfsorientierter Wechsel des Kennworts)
- Einsatz aktueller Antivirus-Client (Endpoint-Security)
- Einsatz aktueller Antivirus-Software für mobile Endgeräte (insbesondere Notebooks)
- Einsatz von VPN-Verbindungen bei Remotezugriffen
- Sperre von externen Schnittstellen (insb. USB)
- Automatische Bildschirm- bzw. Desktopsperre
- Verschlüsselung von Datenträgern (insb. Festplatten)
- Verschlüsselung von Datenträgern in mobilen Endgeraten (u.a. Notebooks, Tablets, Smartphones)
- Einsatz moderner Firewall Technologien (Bsp. Application Layer Firewall, Intrusion Detection System, Intrusion Prevention System etc.)
- Verwalten von Benutzerberechtigungen durch Systemadministratoren
- Erstellen von Benutzerprofilen (insbesondere Einrichtung eines Benutzerstammsatzes pro User)
- Richtlinie für die Erstellung und Verwendung sicherer Passwörter sowie Logindaten
- Richtlinie für einen aufgeräumten Schreibtisch (Clean-Desk-Policy)

Alle vorstehenden Punkte werden durch den Unterauftragnehmer erfüllt.
Alle IT-Systeme und Applikationen des Unterauftragnehmers sind erst nach vorheriger Authentifizierung zugänglich.

Die Mindestpasswortlänge beträgt derzeit 20 Zeichen. Passwörter müssen zudem komplex sein (Groß-/Kleinbuchstaben, Ziffern, Sonderzeichen).

Alle Server-Systeme sind mit Firewall-Technologie (Hardware) gesichert. Auf allen Systemen ist moderne Antiviren-Software installiert, bei der eine regelmäßige Aktualisierung gewährleistet ist.

C) Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Aktenvernichter (Sicherheitsstufe 5 nach DIN 66399)
- Einsatz externer Datenvernichter zur Löschung / Vernichtung von Daten und Datenträgern wie Festplatten, PCs, Notebooks und sonstiger Speichermedien (zertifiziert, AVV erforderlich)
- Protokollierung der Zugriffe auf Anwendungen, insbesondere von Eingabe, Änderung und Löschung von Daten
- Einsatz eines Berechtigungskonzepts inkl. Rollendefinition
- Richtlinie zur Verwendung von Datenverarbeitungsanlagen bzw. Datenträgern (u.a. Verbot zur Nutzung privater Geräte)
- Kontrolle der ordnungsgemäßen Löschung von Daten und Vernichtung von Datenträgern anhand von Stichproben
- minimale Anzahl an Administratoren (Begrenzung auf die unbedingt erforderliche Anzahl)

Alle vorstehenden Punkte werden vom Unterauftragnehmer erfüllt. Die Protokollierung erfolgt im jeweiligen System oder, sofern technisch nicht möglich, an separater Stelle.

Ein Berechtigungskonzept ist im Einsatz. Alle Applikationen und Datenbanken sehen eine differenzierte Einräumung von Berechtigungen vor (Profile, Rollen, Transaktionen und Objekte). Im Verantwortungsbereich des Unterauftragnehmers werden Berechtigungen ausschließlich nach dem „Need-to-know-Prinzip“ vergeben.

Bei ausscheidenden Mitarbeitenden wird dafür Sorge getragen, dass die Berechtigungen rechtzeitig wieder entzogen werden. Die Zugriffsrechte von Datenbanknutzern sind auf das Notwendigste reduziert, um die Integrität der Daten bestmöglich zu gewährleisten.

D) Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

- Trennung von Produktiv- und Testumgebung
- Physikalische Trennung von Systemen, Datenbanken und Datenträgern
- Strikte räumliche Trennung von Arbeitsplätzen und Servern
- Mandantenfähigkeit relevanter Anwendungen
- Steuerung über Berechtigungskonzept
- Festlegung/Zuweisung von Datenbankrechten
- Datensätze sind mit Zweckattributen versehen (so dass eine zweckgebundene Verarbeitung jederzeit gewährleistet ist)

Eine Trennung der Daten ist so jederzeit gewährleistet.

E) Pseudonymisierung

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen:

- Soweit Pseudonymisierung verwendet wird: Trennung der jeweiligen Zuordnungsdaten und Aufbewahrung in getrennten und abgesicherten Systemen (unter Verwendung einer geeigneten Verschlüsselung

Eine Pseudonymisierung wird je nach Schutzbedarf der personenbezogenen Daten angewendet.

2.3 Integrität

A) Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Einsatz von VPN geschützten Verbindungen (Virtual Private Network)
- E-Mail-Verschlüsselung (i.d.R. SSL/TLS)
- Bereitstellung von Daten mittels verschlüsselter Verbindungen wie sftp, https etc.
- https verschlüsselte Datenübertragung über Website und Webapp
- Einsatz von aktueller Firewall

Alle vorstehenden Punkte werden vom Unterauftragnehmer erfüllt.
Der Unterauftragnehmer gibt grundsätzlich keine Daten an Dritte weiter, sofern dies nicht zu den Vertragspflichten gegenüber dem Dienstleister gehört.
Es werden verschlüsselte Verbindungen zur Nutzung der Applikation verwendet.

B) Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

- Stichproben und Anlass basierte Kontrolle von Protokollen
- Sicherstellung durch Übersicht mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
- Die Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten wird durch individuelle Benutzernamen mit einem Benutzer gewährleistet
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Klare Zuständigkeiten für Vornahme/Kontrolle/Protokollierung von Löschungen
- Protokollierung und Nachvollziehbarkeit von Eingaben, Änderungen und Löschung von Daten (durch Logfiles). Der Zugriff auf Datenbestände erfolgt anhand von Berechtigungen. Das Verfahren gewährleistet, dass keine Datenveränderungen unbemerkt vorgenommen werden können

Die Eingabe, Änderung und Löschung von Daten werden, soweit technisch und unter angemessenem Aufwand möglich, protokolliert. Vornahmen von Eingaben oder Datenveränderungen können Nutzern zugeordnet werden.

2.4 Verfügbarkeit und Belastbarkeit

A) Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Maßnahmen zur Datensicherung (physikalisch/logisch):

- Moderne Feuer- und Rauchmeldeanlage (Büros / Rechenzentrum)
- Inertgas-Löschanlage (Rechenzentrum)
- Klimatisierter Serverraum (Rechenzentrum)
- USV (Unterbrechungsfreie Stromversorgung, insbesondere Rechenzentrum)
- RAID-System (gespiegelte Festplatten, Rechenzentrum)
- Serverräume sind hochwassergeschützt errichtet (Rechenzentrum)
- Videoüberwachung Serverraum (Rechenzentrum)
- Alarmmeldung bei unberechtigtem Zutritt zu Serveräumen (Rechenzentrum)
- Sprinkleranlage (Rechenzentrum)
- Brandklasseneinteilung (Kennzeichnung besonders gefährdeter Räume, Rechenzentrum)
- Feuerlöscher an/in den PC-Arbeitsräumen (Rechenzentrum / Büros)
- Einsatz eines geeigneten Antiviren-Programms
- Bestehendes Backup & Recovery-Konzept
- Regelmäßige Test zur Datenwiederherstellung und Protokollierung der Ergebnisse
- Backups und Sicherungsmedien werden örtlich getrennt aufbewahrt
- Keine sanitären Anschlüsse im oder oberhalb der Serverräume
- Vorliegen eines geeigneten Notfallplans
- Getrennte Partitionen für Betriebssysteme und Daten

Alle eingesetzten Serversysteme arbeiten mit gespiegelten Festplattensystemen (RAID). Das Backup-Konzept sieht mindestens eine tägliche inkrementelle und eine wöchentliche Vollsicherung vor. Die Backups werden örtlich getrennt aufbewahrt. Ausgelagerte Backups werden zudem verschlüsselt.

Alle Serversysteme im Rechenzentrum verfügen über eine unterbrechungsfreie Stromversorgung (Akkus und Dieselgeneratoren).

Ein Inergen-Gas basierendes Feuerlöschsystem mit Aufschaltung auf örtliche Feuerleitstellen ist im Einsatz.

2.5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

A) Datenschutz-Management

- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Intranet, Collaboration-Software etc.)
- Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt
- Bestehende Sicherheitszertifizierung nach ISO 27001, BSI-Grundschutz, ggf. weitere oder sonstige Zertifizierungen, u.a. VdS-Zertifikat)
- Externer Datenschutzbeauftragter bestellt – dessen Kontaktdaten sind auf der Website des Verantwortlichen jederzeit einsehbar

- Regelmäßige und dem individuellen Bedarf angepasste Schulung der Mitarbeiter zum Datenschutz
- Durchführung Datenschutz-Folgenabschätzung soweit erforderlich
- Erfüllung sämtlicher Informationspflichten nach Art. 13 und 14 DSGVO
- Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen durch Betroffene

Alle vorgenannten Maßnahmen werden umgesetzt und regelmäßig überprüft und bei Änderungsbedarf entsprechend angepasst. Die getroffenen Maßnahmen werden entsprechend protokolliert.

B) Incident-Response-Management

- Einsatz von Firewall und regelmäßige Aktualisierung (s. auch Zugriffskontrolle)
- Einsatz von Spamfilter und regelmäßige Aktualisierung
- Einsatz geeigneter sowie regelmäßig aktualisierter Antivirus-Software (mit Virenscanner)
- Einsatz eines Intrusion Detection Systems (IDS) zur Aufdeckung von Sicherheitsvorfällen (Netzwerk)
- Einsatz eines Intrusion Prevention Systems (IPS) zur Behebung und Einleitung von Gegenmaßnamen bei Sicherheitsvorfällen
- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (dieser berücksichtigt ebenfalls Meldepflicht gegenüber Aufsichtsbehörde und Betroffenen)
- Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- Einbindung von DSB und der IT-Sicherheit in Sicherheitsvorfälle und Datenpannen
- Dokumentation von Sicherheitsvorfällen und Datenpannen (u.a. Ticketsystem)
- Definierter Prozess sowie Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

Sämtliche genannten Maßnahmen werden umgesetzt sowie die Verfahren in einem angemessenen Umfang auf Aktualität und insbesondere deren Wirksamkeit hin überprüft.

C) Datenschutzfreundliche Voreinstellungen

Privacy by design & Privacy by default:

- Die Gestaltung und Voreinstellungen von Softwares und anderen Verarbeitungsvorgängen gewährleisten, dass lediglich solche personenbezogenen Daten verarbeitet, die für den jeweiligen Zweck auch tatsächlich erforderlich sind
- Technische Maßnahmen gewährleisten die einfache Ausübung des Widerrufsrechts von Betroffenen

D) Auftragskontrolle (Outsourcing)

- Vorherige Prüfung der vom Unterauftragnehmer getroffenen Sicherheitsmaßnahmen sowie der Dokumentation (Vorabüberzeugungspflicht)
- Sorgfältige Auswahl des Unterauftragnehmers (insbesondere hinsichtlich Datenschutzes und Datensicherheit)
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln
- Weisungen an den Unterauftragnehmer erfolgen grundsätzlich ausschließlich schriftlich oder in Textform (mündliche Weisungen werden zusätzlich entsprechend schriftlich oder in Textform erteilt)
- Verpflichtung der Mitarbeiter des Unterauftragnehmers auf den Datenschutz & Vertraulichkeit
- Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Unterauftragnehmer bei Vorliegen einer Bestellpflicht
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Unterauftragnehmer
- Regelung zum Einsatz weiterer Subunternehmer
- Laufende Überprüfung des Unterauftragnehmers und seines Schutzniveaus bei längerer Zusammenarbeit
- Sicherstellung der Löschung /Vernichtung von Daten nach Beendigung des Auftrags

3. Unterauftragnehmer

Name	Adresse	Tätigkeit	Lokalisierung von Daten
BuchhaltungsButler GmbH	Spreestraße 5 15913 Märkische Heide	Softwareentwicklung und 3rd-Level-Support für Kleos SMART Beleg Umgebung	Deutschland

Dritte Sub-Verarbeiter

Name	Adresse	Tätigkeit	Lokalisierung von Daten
ABBYY Europe GmbH	Landsberger Str. 300 80687 München	Bild und Texterkennung	Processing Location : EU / Niederlande
Bayerische Landesamt für Steuern	Dienststelle München 80284 München	ELSTER-Schnittstelle, Übermittlung u.a. der USt.-Voranmeldung	Deutschland
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy L-1855 Luxemburg	Hosting der Kleos SMART Beleg Umgebung	AWS Zone : EU-Central Serverstandort : EU / Frankfurt a. M.

KLEOS SMART Beleg

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