Beschreibung der Verarbeitung personenbezogener Daten

TriNotar

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 TRINOTAR Kundendaten einschließlich personenbezogener Daten eingeben, speichern und ändern. Der Dienstleister als Auftragsverarbeiter hat keine Kenntnisse über die in TRINOTAR eingegebenen oder hochgeladenen Arten personenbezogener Daten.

In seiner Standardkonfiguration bietet TRINOTAR Grundfelder an, die vom Kunden ausgefüllt werden können und personenbezogene Daten wie Name, Adresse, Telefonnummer, E-Mail-Adresse, Geburtsdatum beinhalten.
Verwendung sowie Inhalt dieser Felder liegen in der alleinigen Verantwortung des Kunden.

Persönliche Daten werden von Benutzern über die Funktionen der Softwaredienste für die hier beschriebenen Zwecke eingegeben. Personenbezogene Daten werden nicht direkt vom Datensubjekt selbst erhoben. Die vom Verantwortlichen in TRINOTAR erstellten, eingegebenen und hochgeladenen personenbezogenen Daten erfolgen nach eigenem Ermessen und auf eigenes Risiko des Verantwortlichen.

A. Nutzerdaten

- Vorname, Nachname
- Geschlecht
- Passwort
- Funktion
- Optional: Kontaktdaten (E-Mail, Telefon, Anschrift)

A. Daten von Klienten/Verfahrensbeteiligte

- Vor- und Nachname (ggf. Titel), Anrede
- Geburtsdatum
- Beruf/Tätigkeit
- Familienstand
- Kontaktdaten und -historie (insb. Anschrift, E-Mail-Adresse, Telefonnummer)
- Daten zur Geschäftshistorie
- Finanzdaten, Daten zu finanziellen Transaktionen
- Daten zu Bankverbindungen und Zahlungsarten
- Abrechnungsdaten

- Daten zur Vermögens- und Ertragssituation
- Steuerdaten
- Klientenbezogene Akten bzw. Dokumente

1.2. Kategorien von betroffenen Personen

Als Verantwortlicher kann der Kunde in AnNoText persönliche Daten aus den folgenden Betroffenen eingeben, speichern und ändern:

- Mitarbeiter des Kunden, Mandanten und sonstige Vertragspartner des Kunden
- Sonstige Personen, von denen der Kunde Daten in TRINOTAR aufnimmt und speichert (z.B. Verfahrensbeteiligte, Parteien, Rechtsanwälte der Gegenseite, mit einem Fall befasste externe Kollegen, Gutachter, Sachverständige, Zeugen)

1.3. Zweck der Verarbeitung

Dem Kunden als Verantwortlichen obliegt die Festlegung des mit TRINOTAR durchführten Verarbeitungszwecks. TRINOTAR kann für folgende Zwecke eingesetzt werden:

- Fallbearbeitung
- Erfüllung des Klientenauftrages
- Kommunikation mit Klienten
- Rechnungsstellung
- Übermittlung an Gerichte, Versicherungen, Dritte berechtigte Personen

Für den ordnungsgemäßen Einsatz von TRINOTAR ist keine Verbindung mit anderen Systemen erforderlich; insbesondere erfolgt kein Export von Daten aus dem Verzeichnis der natürlichen Personen in andere Systeme. Verbindungen, die auf Wunsch des Kunden zwischen TRINOTAR und anderen, vom Kunden verwalteten Systemen implementiert werden, unterliegen der Beaufsichtigung des Kunden und seiner alleinigen Haftung.

1.4. Die Art der Verarbeitung

Die Art der Verarbeitung hängt von den vom Verantwortlichen im Rahmen des Vertrages vereinbarten Dienstleistungen ab und kann Folgendes enthalten: Aufzeichnung, Organisation, Änderung, Extraktion, Konsultation, Offenlegung durch Übertragung, Speicherung, Einschränkung, Löschung oder Vernichtung.

1.5. Aufbewahrungszeitraum

Als Verantwortlicher bestimmt der Kunde die Aufbewahrungsfrist für die von/in TRINOTAR verwalteten personenbezogenen Daten (Vertragsdateien, Fälle, Informationen zur Identifizierung von Kontaktpersonen, zugehörige Dokumente...).

Im On-Premise-Modus ist der Kunde für die Sicherung und Backup der Kundendaten und die Installation verantwortlich.

Der Dienstleister als Auftragsverarbeiter speichert Kundendaten, einschließlich, falls zutreffend, personenbezogener Daten, in den folgenden Fällen und für die folgende Aufbewahrungsfrist auf:

- Personenbezogene Daten über den Support/Helpdesks (Informationen, die der Kunde für Wartungstickets zur Verfügung stellt): Kundendaten, einschließlich ggf. personenbezogener Daten werden nach Verjährung etwaiger Ansprüche sowie Ablauf gesetzlicher Aufbewahrungsfristen aus den Support-Datenbanken des Dienstleisters gelöscht. Als Verantwortlicher stellt der Kunde immer sicher, dass bei Meldung bzw. Bearbeitung eines Fehlers keine personenbezogenen Daten an den Auftragsverarbeiter übermittelt werden (in Form von Screenshots, usw.);

- Kopieren von Kundendaten (DUMP) an den Support/Helpdesk: Zur Lösung eines technischen Problems kann es erforderlich sein, dass der Dienstleister einen Teil der Kundendaten, einschließlich ggf. personenbezogener Daten, nach Einholung der Zustimmung des Kunden in eine Testumgebung kopiert. Diese Kundendaten werden nur zur Lösung des bearbeiteten Problems verwendet und maximal zwei (2) Monate nach der Bearbeitung des Vorfalls aus der Testumgebung gelöscht;

- Nach der Datenmigration: Der Dienstleister bewahrt die migrierten Daten für einen Zeitraum von zwei (2) Monaten auf, um in diesem Zeitraum ggf. abzuschließende Korrekturen vorzunehmen. Der Kunde ist für die Kopie/die Sicherung der Daten sowie ggf. nach diesem Zeitraum für deren Übermittlung an den Dienstleister verantwortlich;

- Nach Beendigung/Ablauf der Vereinbarung: Im Falle einer OnPremise Installation liegen die Kundendaten vollständig beim Kunden als Verantwortlicher. Im Rahmen der Beendigung kann der Kunde die Daten im Rohformat (SQL Daten) wie bisher archivieren oder verarbeiten. Für den Dienstleister ergeben sich durch die Beendigung/Ablauf keinerlei Verpflichtungen die Daten in ein anderes Format zu überführen oder zu exportieren, sofern nicht anderweitig vertraglich festgelegt.
  Eine Einflussnahme durch den Dienstleister auf die beim Verantwortlichen gespeicherten Daten erfolgt nicht.

2. Technische und organisatorische Sicherheitsvorkehrungen

Je nach anwendbarem Datenschutzrecht ergreift der Dienstleister die angemessenen technischen und organisatorischen, je nach Stand der Technik bei Vertragsabschluss zu bewertenden, Sicherheitsvorkehrungen („TOMs“), und bewertet diese TOMs im Laufe der Zeit unter Berücksichtigung der Kosten für die Implementierung, der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung sowie der Wahrscheinlichkeit, dass diese zu einem hohen Risiko für die Rechte und Freiheiten der Datensubjekte führen.

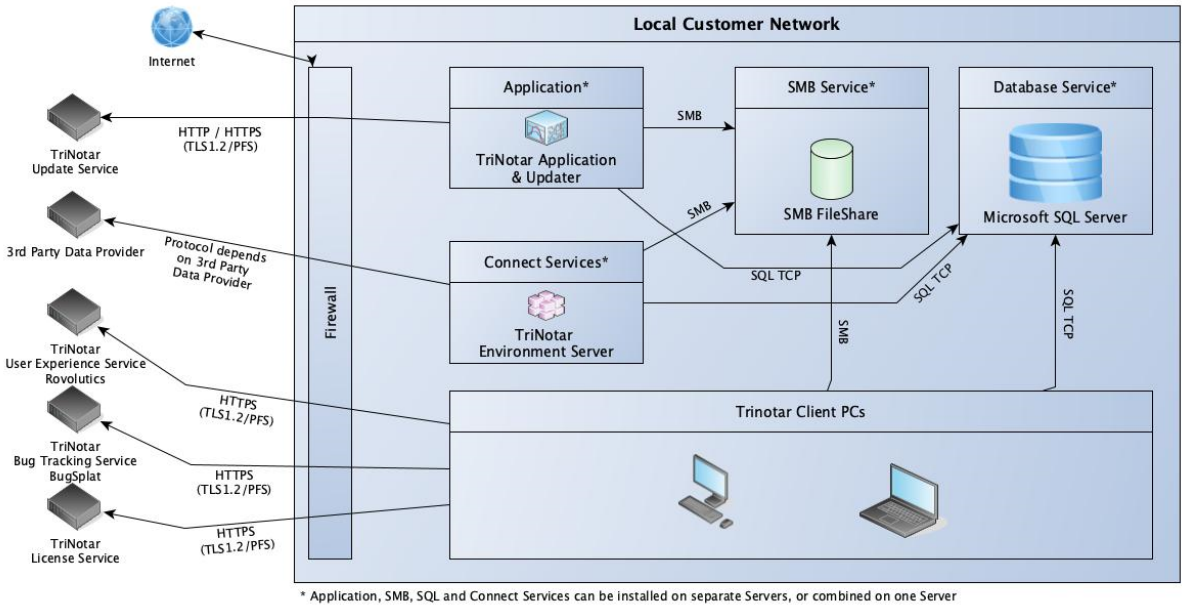
2.1. Datenverschlüsselung und Schutz des Datenaustauschs: TRINOTAR

TRINOTAR ermöglicht die Umsetzung der Datenschutzgrundsätze und Einhaltung von Betroffenenrechten durch die nachstehend dargestellten technischen und organisatorischen Maßnahmen:

2.1.1. Verschlüsselung

Kommunikation zwischen Client und Server	Microsoft SQL- Server Native Protokoll. Authentifizierungsdaten zum Aufbau einer Verbindung sind immer vollverschlüsselt. Datenstromverschlüsselung kann optional im SQL Server aktiviert werden.
Verwaltungsinformationen / Metadaten	Speicherung im SQL-Server
Transportverschlüsselung	Eine verbindliche Transportverschlüsselung kann separat im SQL-Server mittels Flag „ForceEncryption“ aktiviert werden. Diese ist kein Bestandteil der Standardinstallation. Weitere Details zur Transportverschlüsselung im SQL-Server entnehmen Sie den entsprechenden Produktdokumentationen.

2.1.2. IT-Architektur TRINOTAR



2.1.3. Zugriffsberechtigung TriNotar

Authentifizierung durch Passwort	Die Anmeldung in TRINOTAR erfolgt mittels Benutzernamen und Passwort. Die Passwörter werden verschlüsselt in der Datenbank gespeichert. Eine Speicherung des Passwortes im Klartext erfolgt nicht. Das Passwort ist auf 12 Zeichen begrenzt.
Einstellbare Nutzerrechte	Das vorhandene Rollen- und Berechtigungskonzept unterstützt komplexe Berechtigungsstrukturen: <u>Voreinstellungen:</u> • Standard-Konfiguration sieht beschränkte Rollen und Berechtigungsschablonen vor. Die Vergabe individueller Berechtigungen anhand frei definierter Berechtigungsschablonen sowie erweiterter Berechtigungen ist möglich wie z.B. für die Assistenz oder Sachbearbeiter etc.

2.1.4. Datenspeicherung und Datenlöschung

Datenminimierung	**Anlage von Nutzern:** Zur Nutzeranlage werden lediglich Anrede, Name, Vorname, Kennwort sowie Kürzel benötigt.
Limitierung der Speicherdauer	**Nutzerdaten:** Anonymisierung der Daten bei Löschung des Zugangs durch Kunden.

2.1.5. Betroffenenrechte

Auskunft über Daten	Über den Umfang der gespeicherten Daten kann jederzeit Auskunft erteilt werden. Die Erteilung der Auskunft erfolgt nur an die dazu berechtigte Anwender.
Berichtigung von Daten	Adressen von natürlichen Personen können jederzeit von berechtigten Anwendern geändert werden.

2.2. Support

Die Zugriffskontrolle auf persönliche Daten erfolgt gemäß den internen Kontrollrichtlinien, einschließlich der Richtlinie zum Datenzugriff von Wolters Kluwer, der Implementierung des Nutzerverwaltungssystems sowie der Zugriffsrechte, der Sensibilisierung der Mitarbeiter in Bezug auf Verwaltung von Daten bzw. ihren Passwörtern, der Kontrolle des Netzwerkzugriffs sowie der zugrunde liegenden Anwendungen. Die Maßnahmen sind:

- eine schriftliche/programmierte Berechtigungsstruktur;
- differenzierte Zugriffsrechte, z.B. zum Lesen, Ändern oder Löschen von Daten;
- eine Festlegung von Rollen;
- ein Aktivitäts- und Audit-Protokoll

Persönliche Daten sind partitioniert. Zu den Maßnahmen gehören:

- die Trennung von Funktionen (Produktions-/Testdaten);
- die Isolierung sensibler Daten;
- die Einschränkung der Verarbeitungszwecke; Bereichsbildung
- Regeln/Maßnahmen zur Gewährleistung der getrennten Speicherung, Änderung, Löschung und Übertragung von Daten.

2.2.1. Fernzugriff auf IT-System des Kunden

Zugriffskontrolle	Der Zugriff ist erst nach Freigabe durch den Kunden möglich (Freigabe erfolgt durch Austausch eines bei dem Kunden generierten Schlüssels). Der Supportmitarbeiter von WOLTERS KLUWER weist vor jeder Freigabe darauf hin, dass laufende Anwendungen mit sichtbaren Kundendaten oder anderen vertraulichen Informationen vor dem Zugriff geschlossen werden. Der Zugriff kann kundenseitig jederzeit unterbrochen werden.
Verschlüsselung	Externe Kommunikationsverbindungen laufen über gesicherte Datenkanäle, die mit einem RSA Public/Private Key Exchange aufgebaut und mit 256-Bit-AES verschlüsselt sind.

2.2.2. Supportmitarbeiter

Berufsverschwiegenheit	Supportmitarbeiter von WOLTERS KLUWER und eingesetzten Unterauftragnehmern sind zur Berufsverschwiegenheit verpflichtet.

3. Absturzberichte

Für die Absturzberichtsübermittlung („Crash Reporting“) setzen wir das Produkt BugSplat der BugSplat, LLC ein.
Die Übermittlung von Daten erfolgt nur dann, wenn der Anwender im jeweiligen Einzelfall der Übermittlung zustimmt.
Rechtsgrundlage für die Verarbeitung ist Art 6 Abs. 1 Satz 1 lit. a DSGVO sowie Art. 49 Abs. 1 S. 1 lit. a) DSGVO, indem die Verarbeitung der nachstehenden Daten auch in einem Drittland ohne Angemessenheitsbeschluss oder geeignete Garantie verarbeitet werden könnte.

Welche Daten sammelt BugSplat von Anwendern?
Die Daten umfassen unter anderem: Computerstatusinformationen, Informationen, die sich darauf beziehen, wie eine Anwendung funktioniert, den Typ der verwendeten Computerhardware, das verwendete Betriebssystem, die externe IP-Adresse sowie die Lizenznummer.
Zusätzlich kann uns der Anwender freiwillig personenbezogene Daten und ein Feedback zur Verfügung stellen. Hierzu bietet die Übermittlungsplattform entsprechende Eingabefelder (Name, E-Mail-Adresse, Fehlerbeschreibung) an.

Wie nutzt BugSplat die gesammelten Informationen?
Für die Daten, die BugSplat über die Aktivitäten der Anwender und die die Anwender ggf. hierüber zur Verfügung stellen, ist ausschließlich die Wolters Kluwer Deutschland GmbH verantwortlich, nicht die BugSplat, LLC. Die gesammelten Daten und Informationen werden verwendet, um unseren Entwicklern einen Einblick in die Funktionalität und den Umgang mit ihren Anwendungen zu geben, einschließlich auftretender Probleme.
Die BugSplat, LLC selbst sammelt nichtpersonenbezogene Daten und Informationen, die aggregiert und anonymisiert werden. Solche aggregierten und anonymisierten Informationen werden von BugSplat, LLC verwendet, um (i) die Dienste zu verbessern, (ii) eine Analyse von Trends oder Verhaltensweisen und (iii) andere ähnliche Verwendungen zu erstellen, jedoch immer in einer aggregierten und anonymen Weise.

Gibt es eine Möglichkeit, dass Anwender die Erfassung von Daten und Informationen verhindern können?
Ja, der Anwender kann vor der Versendung des Absturzberichts seine Einwilligung in die Übermittlung der Daten verweigern.

3.1. Nutzungsanalyse

Für die Analyse der Nutzung setzen wir das Tool Revulytics der Revulytics Inc. ein und erheben dabei die folgenden Daten:

Systemdaten

- Arbeitsspeichergröße
- Betriebssystem (Windows 7, 8, 10 etc.)
- Office Version
- Betriebssystem-Architektur (32- oder 64-Bit Betriebssystem)
- CPU-Architektur (32- oder 64-Bit Prozessor)
- CPU-Anzahl
- CPU-Kern-Anzahl
- CPU-Name
- ClientID
- Lizenznummer
- GPU-Name (Name der Grafikkarte)
- Information, ob das System über eine Batterie verfügt (trifft i.d.R. nur auf Laptops zu)

- Installierte .NET-Framework-Versionen
- MAC-Adresse der Netzwerkkarte
- Monitor-Anzahl
- Monitor-Auflösung
- Produkt samt eingesetzter Version
- Spracheinstellungen (deutsch, englisch, niederländisch, etc.)
- Systemart (Desktop-PC, Laptop)
- Zeitzone

Nutzungsdaten

- Öffnen der Anwendung
- Schließen der Anwendung
- Wie oft wurde eine Funktion genutzt oder eine bestimmte Option der Funktion ausgewählt.

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.

Die Datenübermittlung erfolgt stets verschlüsselt per https. Die Daten werden bis zu ihrer Übertragung unverschlüsselt auf der Festplatte des jeweiligen PCs eines Anwenders gespeichert. Jeder Anwender hat hierdurch die Möglichkeit, genau zu analysieren und festzustellen, dass keine personenbezogenen Daten übertragen werden.
Rechtsgrundlage für die Datenverarbeitung

Rechtsgrundlage für die Verarbeitung ist Art. 6 Abs. 1 Satz 1 lit. f DSGVO.

Zweck der Datenverarbeitung

Der Einsatz von Analysetools dient der Verbesserung unserer Produkte unter anderem im Hinblick auf Nutzerfreundlichkeit, Effektivität und Sicherheit. Hierzu benötigen wir Informationen über die in Ihrer Kanzlei vorhandene Hard- und Software und das Nutzungsverhalten der Anwender.

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

Dauer der Speicherung

Die Daten werden gelöscht, sobald sie für die Erreichung des Zweckes ihrer Erhebung nicht mehr erforderlich sind. Im Falle der hier übermittelten Daten ist dies der Fall, wenn der Datensatz statistisch ausgewertet worden ist.

Widerspruchsmöglichkeit

Sofern sie mit dieser Datenerhebung nicht einverstanden sind, können die Kunden in der Administration des jeweiligen Produktes die Übermittlung für alle Arbeitsplätze zentral abschalten.

4. Unterauftragnehmer

Ein angemessenes Schutzniveau für den Umgang mit und die Verarbeitung von personenbezogenen Daten wird durch die sogfältige Auswahl von Unterauftragnehmern und den Abschluss von Auftragsverarbeitungsvereinbarungen gemäß Art 28 DSGVO sichergestellt.

Name	Anschrift	Auftragsinhalt	Datenlokalisierung	Unterauftragnehmer
Telekom Deutschland GmbH	Landgrabenweg 151 53227 Bonn Germany	Hosting der internen Systeme von Wolters Kluwer Deutschland sowie Hosting des cloudbasierten Dienstes Smarte AnwaltsAkte	Deutschland	Scanplus GmbH Lise-Meitner Str.5 89081 Ulm Data Residence : Germany
Teleperformance Portugal SA	Av. Alvaro Pais 2 1600-873 Lisbon Portugal	1st Level Software Support	Portugal	
TeamViewer Germany GmbH	Bahnhofsplatz 2, 73033 Göppingen	Fernwartungswerkzeug für Supportzwecke	Deutschland	
Salesforce.com EMEA Limited	Floor 26 Salesforce Tower, 110 Bishopsgate, EC2N 4AY London, United Kingdom	Bereitstellung des Systems für die Supportticket-Verwaltung	United Kingdom	
QNC GmbH	Schwarzer Bär 4 30449 Hannover	Bereitstellung des Tools und dessen API für eine Funktionserweiterung in TriNotar	Die Datenverarbeitung erfolgt innerhalb der EU / des EWR und in Drittstaaten.	Microsoft Deutschland GmbH, Amazon Web Services EMEA SARL, Digital Ocean/Paperspace, Google LLC
Founders1 GmbH	Adelheidstraße 93, 65185 Wiesbaden	Bereitstellung des Tools und dessen API für eine Funktionserweiterung in TriNotar	Irland, Niederlande, Deutschland	Company.info BI GmbH, Klippa App B.V., Northdata GmbH, Microsoft Ireland Operations Ltd., MongoDB Ltd.

TriNotar

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

Wolters Kluwer