Beschreibung der Verarbeitung personenbezogener Daten

DictNow

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

In seiner Standardkonfiguration bietet DICTNOW 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 DICTNOW erstellten, eingegebenen und hochgeladenen personenbezogenen Daten erfolgen nach eigenem Ermessen und auf eigenes Risiko des Verantwortlichen.

1.2 Kategorien von betroffenen Personen

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

A. Nutzerdaten

- Vorname, Nachname
- Geschlecht*
- Passwort
- Funktion
- Arbeitgeber / Organisationseinheit beim Arbeitgeber

B. Daten von Kunden/Mandanten/Patienten, Fallbezogen:

- Daten in dem Umfang, wie sie vom Nutzer angegeben werden

C. Kreis der von der Verarbeitung Betroffenen, Fallbezogen:

- Mitarbeiter des Kunden
- Kunden/Mandanten/Patienten und sonstige Vertragspartner des Kunden

- Sonstige Personen, von denen der Kunde Daten in DictNow 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 DICTNOW durchführten Verarbeitungszwecks. DICTNOW kann für folgende Zwecke eingesetzt werden:

- Erfassen von gesprochenen Wörtern und Umwandlung in strukturierte Texte und Daten.
- Übermittlung von Diktaten
- Adaption des in der Applikation gespeicherten Wörterbuchs zur Verbesserung der Erkennungsleistung

Für den ordnungsgemäßen Einsatz von DICTNOW 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 DICTNOW 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 DICTNOW verwalteten persönlichen Daten (Vertragsdateien, Fälle, Informationen zur Identifizierung von Kontaktpersonen, zugehörige Dokumente...).

Im On-Premises-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:

- Persönliche 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 Rahmen der im Vertrag vorgesehenen Reversibility-Services werden die Kundendaten im vereinbarten Format an den Kunden übermittelt. Der Dienstleister hält sodann die entsprechenden Datenbanken für zwei (2) Monate (oder einen anderen, im Vertrag festgelegten Zeitraum) auf seinen Servern vor; dann werden sie vollständig vernichtet.

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.

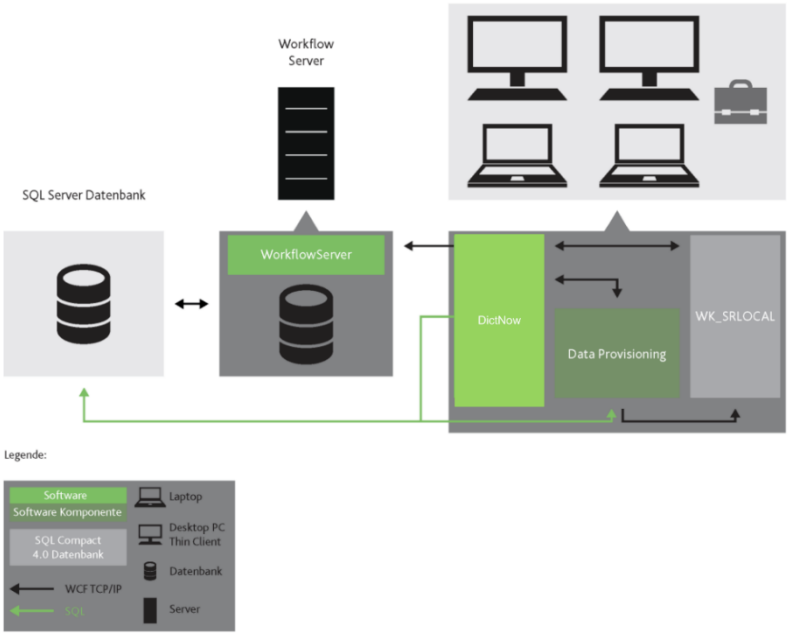
2.1 Datenverschlüsselung und Schutz des Datenaustauschs: DictNow

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

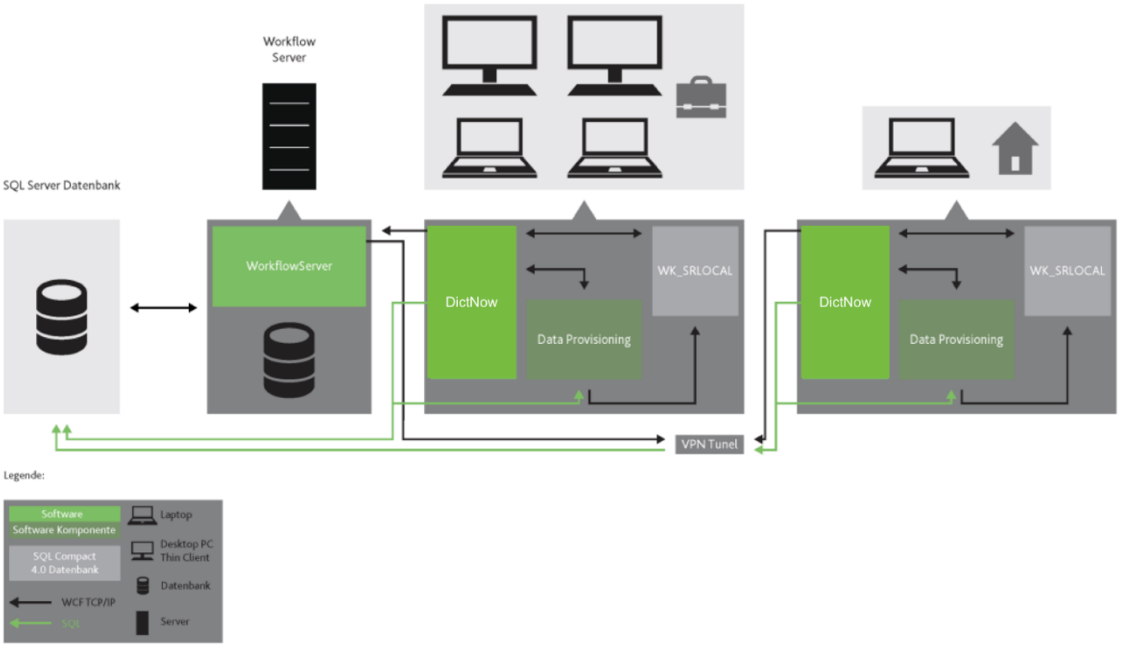
IT-Architektur DictNow

DictNow bildet eine Vielzahl von Installationsszenarien ab, die in den folgenden Darstellungen schematisch dargestellt werden. Details zu den Umgebungsvariablen können in den DictNow IT-Voraussetzungen eingesehen werden.

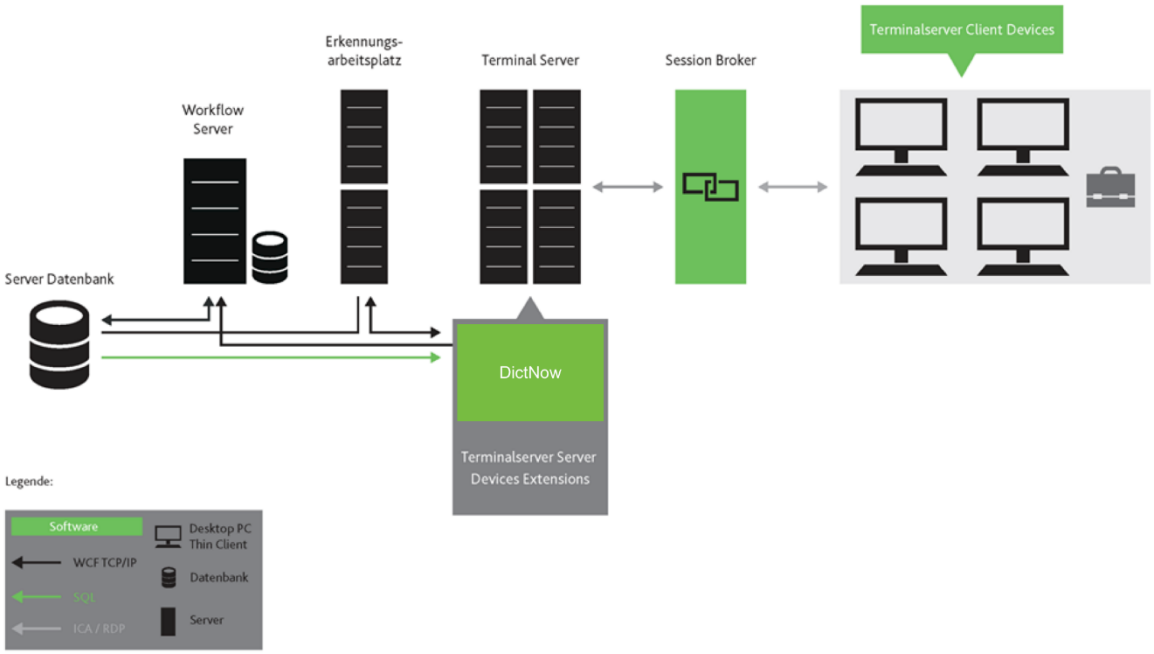
Client Server



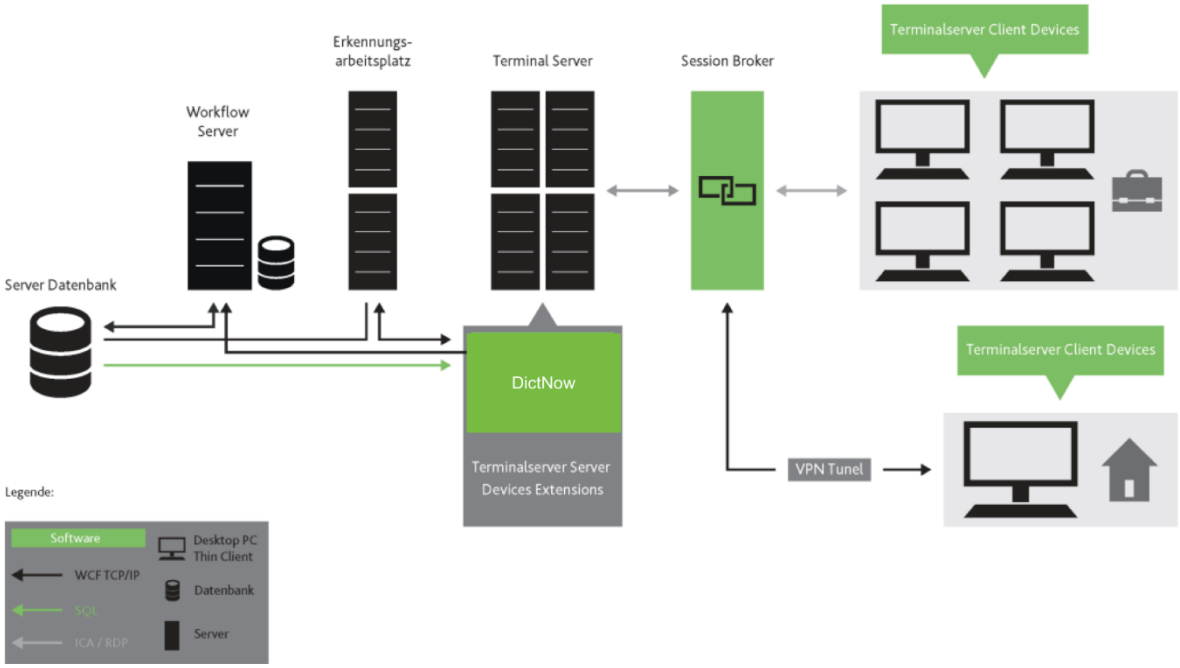
Client Server Betrieb mit Anbindung eines Heimarbeitsplatzes



Terminal-Server



Terminal Server Betrieb mit Anbindung eines Heimarbeitsplatzes



Verschlüsseldung

Kommunikation zwischen Client und Server	.NET WCF 3.0-Bibliothek unter Verwendung von TCP zur Nachrichtenübermittlung. Die Daten werden binär ohne Sicherheits-, Anmelde- und Verschlüsselungsmethoden übertragen.
Diktate in DictNow	Rijndael-Algorithmus mit einer Schlüsselgröße von 256 Bit
Verwaltungsinformationen / Metadaten	Verschlüsselte Speicherung im SQL-Server

Zugriffsberechtigung

Authentifizierung durch Passwort	Die Anmeldung in DictNow erfolgt mittels Benutzernamen und Passwort. Die Passwörter werden als Hashwerte mit jeweils einem Saltwert in der Datenbank gespeichert. Eine Speicherung des Passwortes im Klartext erfolgt nicht. Das Passwort ist auf 20 Zeichen begrenzt.
Einstellbare Nutzerrechte	Das vorhandene Rollen- und Berechtigungskonzept unterstützt komplexe Berechtigungsstrukturen: <u>Voreinstellungen:</u> • Standard-Konfiguration sieht beschränkte Rollen und Berechtigungen vor. • Nur Autoren können auf eigene Diktatinformationen zugreifen.

	Die Vergabe individueller Berechtigungen anhand frei definierter Rollen ist möglich wie z.B. für die Assistenz oder einen sogenannten Wörterbuchpfleger etc. Die Löschung von Diktaten ist nur durch den Autor möglich.

Datenspeicherung und Datenlöschung

Datenminimierung	**Anlage von Nutzern:** Zur Nutzeranlage werden lediglich Anmeldename, Passwort und Geschlecht (Zweck der Angabe des Geschlechts ist die Ausrichtung des Spracherkenners) benötigt. **Diktate:** • Sounddatei (mit Daten im vom Kunden bestimmten Umfang) • Stimmcharakteristika* • Anlagen, die vom Kunden dem Diktat angehängt werden* • Textdatei mit umgewandelten Sounddaten* **Wörterbuch*:** • Nutzerbezogenes Wörterbuch • Nutzer bestimmt die Aufnahme neuer Daten in das eigene Wörterbuch. *Nur bei Spracherkennung
Limitierung der Speicherdauer	**Nutzerdaten:** Anonymisierung der Daten bei Löschung des Zugangs durch Kunden. **Diktate:** • Die Voreinstellung sieht einen 30-tägigen Aufbewahrungszeitraum für fertiggestellte Diktate vor. Nach Ablauf werden die Daten automatisch gelöscht. • Abweichende Einstellungen der Speicherdauer können vom Nutzer vorgenommen werden. • Die in DictNow integrierte Löschfunktion ermöglicht die jederzeitige Löschung durch den Autor zu einem individuell gewählten Zeitpunkt (Löschvorgang erfolgt nach Bestätigung).

Betroffenenrechte

Löschung von Daten	Nutzerdefinierte Fristen für die automatische Löschung von Daten (Sound Dateien, Dokumente und Anlagen)

2.2 In DictNow Diktier-App

Datencenter / Hosting IT-Infrastruktur der App

Ort des Datencenters	Innerhalb EU / EWR
Zertifizierung	ISO 27011, SAS-70 Typ II

Verschlüsselung

Smartphone App	Dateiverschlüsselung durch SSL Encryption

2.3 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.

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.

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.

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.

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

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
Recognosco GmbH	Tech Gate, Donau-City-Straße 1 1220 Wien, Österreich	Lizenzgeber der Spracherkennungssoftware für DictNow und 3rd Level Support	Österreich	
Telekom Deutschland GmbH	Landgrabenweg 151 53227 Bonn Germany	Hosting der internen Systeme von Wolters Kluwer Deutschland sowie Hosting des cloudbasierten Dienstes für DictNow	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	

DictNow

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