ANHANG 2BIS: BESCHREIBUNG DER VERARBEITUNG PERSONENBEZOGENER DATEN

Software-Dienste: LEGISWAY

Dieser Anhang "Beschreibung der Verarbeitung personenbezogener Daten" ist dem Datenverarbeitungszusatz (DPA) beigefügt, der Bestandteil der Vereinbarung zwischen dem Kunden (Verantwortlicher) und dem Anbieter (Auftragsverarbeiter) ist, der in der Vereinbarung genannt ist, und gilt ausschließlich für Legisway. Dieser Anhang kann von Zeit zu Zeit vom Anbieter aktualisiert werden, wenn neue Versionen der Software-Dienste im Rahmen der Wartungsdienste, die dem Kunden gemäß der Vereinbarung bereitgestellt werden, verfügbar sind und wie im Anhang "Wartungsdienste und Service Level Agreement" beschrieben. Die aktualisierten Bedingungen dieses Anhangs gelten zwischen den Parteien ab dem Datum der Verfügbarkeit der neuen Version der Software-Dienste.

1. Verarbeitung personenbezogener Daten

A. Zwecke der Verarbeitung

Der Anbieter kann als Auftragsverarbeiter im Auftrag des Kunden und gemäß den Anweisungen des Kunden personenbezogene Daten des Kunden im Rahmen der Ausführung der Vereinbarung verarbeiten, um Software-Dienste und/oder professionelle Dienstleistungen bereitzustellen, einschließlich, falls zutreffend, für:

- Installation
- Datenmigration, Implementierung, Konfiguration und Testen
- Hosting, Speicherung und Überwachung
- Backup und Notfallwiederherstellung
- Wartungsdienste

Als Verantwortlicher stellt der Kunde sicher, dass keine personenbezogenen Daten an den Auftragsverarbeiter übermittelt werden, wenn er einen Fehler an den Support-Dienst des Anbieters meldet (in Form von Screenshots usw.).

Der Kunde ist als Verantwortlicher dafür verantwortlich, die Zwecke der Verarbeitung festzulegen, die er mit LEGISWAY durchführt.

B. Arten der verarbeiteten personenbezogenen Daten

Als Verantwortlicher kann der Kunde Kundendaten, einschließlich personenbezogener Daten, in LEGISWAY eingeben oder anderweitig personenbezogene Daten des Kunden im Zusammenhang mit seinem Abonnement für Legisway bereitstellen, deren Umfang vom Kunden nach eigenem Ermessen bestimmt und kontrolliert wird, die jedoch in ihrer Standardkonfiguration die folgenden grundlegenden Kategorien personenbezogener Daten umfassen können:

- Vor- und Nachnamen natürlicher Personen

- Titel
- Kontaktinformationen (einschließlich Wohn- und Arbeitsadressen, E-Mail-Adressen, Telefonnummern, IP-Adressen)
- Berufliche Daten usw.

LEGISWAY kann Freitextfelder und/oder Kommentarfelder enthalten.

C. Kategorien betroffener Personen

Als Verantwortlicher kann der Kunde Kundendaten, einschließlich personenbezogener Daten, in LEGISWAY eingeben oder anderweitig personenbezogene Daten des Kunden im Zusammenhang mit seinem Abonnement für Legisway bereitstellen, deren Umfang vom Kunden nach eigenem Ermessen bestimmt und kontrolliert wird, die jedoch Informationen zu den folgenden Kategorien betroffener Personen umfassen können: Mitarbeiter, unabhängige Auftragnehmer, Führungskräfte, Direktoren, Berater, Parteien und Gegenparteien von Verträgen, Anspruchsteller und Lieferanten.

D. Art der Verarbeitung

Die Art der Verarbeitung hängt von den vom Anbieter im Rahmen der Vereinbarung erbrachten Dienstleistungen ab und kann das Aufzeichnen, Organisieren, Ändern, Extrahieren, Konsultieren, Offenlegen durch Übermittlung, Speichern, Einschränken, Löschen oder Vernichten umfassen.

E. Aufbewahrungsfrist

Der Anbieter als Auftragsverarbeiter wird personenbezogene Daten des Kunden für den Zeitraum verarbeiten, der für die Erfüllung der Vereinbarung angemessen ist. Der Anbieter speichert Kundendaten und erstellt während der Laufzeit der Vereinbarung Backups gemäß den Bestimmungen der Vereinbarung. Der Anbieter bewahrt Kundendaten, einschließlich gegebenenfalls personenbezogener Daten, in den folgenden Fällen und für die folgenden Aufbewahrungsfristen auf (vorbehaltlich gesetzlicher Verpflichtungen oder Verjährungsfristen):

- Kopie der Kundendaten (DUMP) zur Unterstützung: Um ein technisches Problem zu lösen, kann der Anbieter nach Einholung der Zustimmung des Kunden Kundendaten, einschließlich gegebenenfalls personenbezogener Daten, in eine Testumgebung kopieren. Diese Kundendaten werden nur zur Lösung des angesprochenen Problems verwendet und spätestens zwei (2) Monate nach der Bearbeitung des Vorfalls aus der Testumgebung gelöscht;
- Nach der Datenmigration: Der Anbieter bewahrt die migrierten Daten für einen Zeitraum von zwei (2) Monaten auf, um während dieses Zeitraums gegebenenfalls Korrekturen vorzunehmen. Der Kunde ist dafür verantwortlich, die Daten zu kopieren/sichern und dem Anbieter nach diesem Zeitraum bei Bedarf zur Verfügung zu stellen;
- Nach Beendigung/Ablauf der Vereinbarung: Im Rahmen der in der Vereinbarung vorgesehenen Reversibilitätsdienste, falls vorhanden, werden die Kundendaten dem Kunden im vereinbarten Format zurückgegeben. Der Anbieter bewahrt die entsprechenden Datenbanken für vier (4) Monate (oder einen anderen in der Vereinbarung festgelegten Zeitraum) auf seinen Servern auf, bevor sie vollständig gelöscht werden;

Als Verantwortlicher legt der Kunde die Aufbewahrungsfrist für die in LEGISWAY verwalteten personenbezogenen Daten fest.

2. Technische und organisatorische Maßnahmen

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung sowie der Risiken für die Rechte und Freiheiten betroffener Personen ergreifen der Anbieter und der Kunde die geeigneten technischen und organisatorischen Sicherheitsmaßnahmen ("TOMs"), um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten. Vom Anbieter implementierte TOMs sind mindestens wie folgt:

A. Zugangskontrolle - Gebäude des Anbieters

Der Zugang zu den Gebäuden des Anbieters wird durch technische und organisatorische Maßnahmen kontrolliert: Zugangskontrolle mit personalisierten Ausweisen, Verriegelung von Türen und Empfangsverfahren für Besucher.

B. Zugangskontrolle – Systeme

Der Zugang zu den Netzwerken, Betriebssystemen, Benutzerverwaltung und Anwendungen des Anbieters benötigt die erforderlichen Berechtigungen: Erweiterte Passwortverfahren, automatische Timeout- und Sperrung bei falschem Passwort, individuelle Konten mit Verlauf, Zugriffsüberprüfung, Verschlüsselung, Hardware- und Software-Firewalls.

C. Zugangskontrolle – Daten

Der Anbieter implementiert die folgenden Maßnahmen: Benutzerverwaltung und Benutzerkonten mit spezifischem Zugriff, geschultes Personal in der Datenverarbeitung und Sicherheit, Trennung zwischen Betriebssystemen und Testumgebungen, Gewährung spezifischer Rechte und Führung von Nutzungs-, Zugriffs- und Löschprotokollen.

D. Datenverschlüsselung und Schutz von Übertragungen

Verschlüsselungen im Ruhezustand und während der Übertragung sind verfügbar, um Daten vor unbefugtem Zugriff zu schützen und die Datenintegrität zu gewährleisten. Die HTTPS-Datenübertragung zwischen den LEGISWAY-Servern und dem Kunden ist mit dem TLS 1.3-Protokoll verschlüsselt.

E. Mittel zur Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und kontinuierlichen Belastbarkeit von Verarbeitungssystemen und -diensten

Der Zugang zu personenbezogenen Daten erfolgt in Übereinstimmung mit den internen Kontrollrichtlinien, einschließlich der Informationszugriffsrichtlinie von Wolters Kluwer, der Implementierung eines Benutzerverwaltungssystems und Zugriffsrechten, der Sensibilisierung der Mitarbeiter im Umgang mit Informationen und deren Passwörtern, der Kontrolle des Netzwerkzugriffs und der zugrunde liegenden Anwendungen. Maßnahmen bestehen aus:

- Einer schriftlichen/programmierten Autorisierungsstruktur;
- Differenzierten Zugriffsrechten, z.B. zum Lesen, Ändern oder Löschen von Daten;
- Einer Definition von Rollen;
- Einem Aktivitäts- und Auditprotokoll

Personenbezogene Daten sind partitioniert. Maßnahmen umfassen:

- Trennung von Funktionen (Produktions-/Testdaten);
- Begrenzung der Verarbeitungszwecke; Segmentierung
- Regeln/Maßnahmen zur Gewährleistung der getrennten Speicherung, Änderung, Löschung und Übertragung von Daten. LEGISWAY erfordert, dass der Benutzer ein Passwort verwendet, um auf LEGISWAY zuzugreifen, was die Vertraulichkeit aller in das System eingegebenen Daten gewährleistet.

LEGISWAY bietet auch die Möglichkeit, die Benutzerrechte zu verwalten, um die innerhalb von LEGISWAY zugänglichen Informationen zu segmentieren. Der Kunde ist daher verpflichtet, innerhalb seiner Organisation Vertraulichkeitsregeln festzulegen.

F. Fähigkeit zur schnellen Wiederherstellung der Verfügbarkeit und des Zugriffs auf personenbezogene Daten im Falle eines physischen oder technischen Vorfalls

Die Verfügbarkeit der Daten wird durch ein permanentes Netzwerküberwachungssystem kontrolliert. Um Datenverlust zu verhindern, wird eine Datensicherung mit definierten Aufbewahrungsfristen durchgeführt. Weitere Maßnahmen umfassen:

- Backup-Verfahren;
- Überspannungsschutz;
- Physische Trennung der Speicherung von Backup-Datenträgern;
- Spiegelung von Serverfestplatten (RAID);
- Endpoint Detection and Response/SPAM-Filter/Firewall/Intrusion Detection System/Notfallwiederherstellungsplan/Business Continuity Plan;
- Feuer-/Wasserschutzsysteme (einschließlich Feuerlöschsystem, Feuerschutztüren, Rauch-/Feuermelder).
- Verfahren zur Verwaltung von Sicherheitsvorfällen: Der Anbieter implementiert Prozesse zur Verwaltung von Sicherheitsvorfällen mit Benachrichtigungen über Datenschutzverletzungen gemäß dem Datenverarbeitungszusatz.

G. Verfahren zur regelmäßigen Überprüfung, Bewertung und Bewertung der Effizienz technischer und organisatorischer Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

LEGISWAY wird kontinuierlich überwacht:

- Gesundheits- und Leistungsüberwachung wird in allen Computersystemen durchgeführt
- Der Anbieter führt regelmäßig interne und externe Schwachstellen- und Penetrationstests von Legisway und der Infrastruktur durch.

Darüber hinaus ist das Intrusion Detection System immer aktiv und gibt in Echtzeit Warnungen aus.

H. Hosting

LEGISWAY wird in Deutschland in AWS Europe-Rechenzentren und in Irland (Backup) gehostet.

3. Unterauftragsverarbeiter

Der Kunde akzeptiert, dass der Anbieter als Auftragsverarbeiter Unterauftragsverarbeiter beauftragen kann, um bestimmte Datenverarbeitungsaktivitäten (einschließlich der Verwaltung von Cloud-Diensten, Hosting-Diensten, Wartungsdiensten usw.) im Auftrag des Kunden durchzuführen:

- Anbieter-Affiliates, die im konzerninternen Transferabkommen innerhalb der Wolters Kluwer-Gruppe identifiziert sind, umfassen die folgenden:

Anbieter-Affiliate	**Datenlokalisierung**
Wolters Kluwer Legal Software France SAS (außer wenn als Auftragsverarbeiter tätig)	Frankreich
Wolters Kluwer Italia S.R.L	Italien
Wolters Kluwer Global Business Services B.V.	Niederlande
Wolters Kluwer Technology B.V.	Niederlande

- Dritte Unterauftragsverarbeiter

Dritter Unterauftragsverarbeiter	**Aktivität/Datenlokalisierung**
ABBYY Europe Landsberger Str. 300 80687 München, Deutschland	OCR: Anbieter von Service und Support Level 2/Irland (auf MS Azure)
Keynit SAS, 121 rue d'Aguesseau, 92100 Boulogne Billancourt, Frankreich	Hosting (Projektphase Frankreich)
Claranet SAS, 2 rue Breguet, 75011 Paris, Frankreich	Hosting und Rechenzentrumsmanagement für Mail to Legisway/Frankreich
Teleperformance Portugal Edificio Marconi, Av. Alvaro Pais 2, 1600-873 Lissabon, Portugal	Support Level 1 & Level 2/Portugal
VP&White SAS, 62 bis avenue André-Morizet, 92100 Boulogne Billancourt, Frankreich	Professionelle Dienstleistungen/Frankreich, UK
NEA IDF SAS 41 rue de Bayern, 75017 Paris, Frankreich	Professionelle Dienstleistungen/Frankreich