Wolters Kluwer

Wolters Kluwer Deutschland GmbH
Geschäftsbereich Recht Software
Robert-Bosch-Straße 6
50354 Hürth

Vereinbarung zur Auftragsverarbeitung

Bitte unterschrieben und vollständig zurücksenden

- per Fax: 0221 / 94373-16030
- per E-Mail: dsgvo.software-recht@wolterskluwer.com
- oder im Rahmen der Auftragserteilung mit den Auftragsdokumenten

Vereinbarung zur Auftragsverarbeitung

- gemäß Art. 28 DSGVO -

für den Geschäftsbereich Legal Software für cloudbasierte Dienste: Kleos, effacts und OnPremise-Software: AnNoText, winra, TriNotar, DictaPlus / DictNow mit optionalen Online-Erweiterungen: Smarte AnwaltsAkte, OnlineAkte, DictNow Diktier-App

Vereinbarung

zwischen

WOLTERS KLUWER Deutschland GmbH

Robert-Bosch-Str. 6
50354 Hürth

(im Folgenden: „WOLTERS KLUWER“)

und

Kundenname: _____

Straße und Hausnr.: _____

PLZ und Ort: _____

Kundennr.: _____

(im Folgenden: „Kunde“)

1. Anwendungsbereich und Zweckbestimmung

1.1 Diese Vereinbarung regelt die Rechte und Pflichten des Kunden und von WOLTERS KLUWER (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag. Die Vereinbarung gilt dabei sowohl für Software, die auf Systemen des Kunden installiert ist (AnNoText, winra, TriNotar und DictaPlus / DictNow, insgesamt als „OnPremise-Software“ bezeichnet) als auch für „cloudbasierte Dienste“ (effacts und Kleos). Soweit nicht im Einzelfall abweichend angegeben, gelten die einzelnen Bestimmungen dieser Vereinbarung sowohl für OnPremise-Software als auch für cloudbasierte Dienste.

1.2 Diese Vereinbarung findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter von WOLTERS KLUWER oder durch ihn beauftragte Unterauftragnehmer („Unterauftragsverarbeiter“) personenbezogene Daten des Kunden verarbeiten.

1.3 In dieser Vereinbarung verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung („DSGVO“) zu verstehen. Soweit Erklärungen im Folgenden schriftlich zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

1.4 Diese Vereinbarung entspricht den Anforderungen an einen Vertrag über die Verarbeitung im Auftrag nach den Vorschriften der DSGVO und tritt am 25.05.2018 in Kraft. Sie ersetzt ab diesem Zeitpunkt sämtliche Vereinbarungen, die die Parteien im Hinblick auf die Auftragsverarbeitung von personenbezogenen Daten getroffen haben.

1.5 Im Rahmen der Erfüllung des Hauptvertrages kann WOLTERS KLUWER Zugriff auf personenbezogene Daten des Kunden oder sonstiger Dritter erhalten. Die personenbezogenen Daten werden nachfolgend einheitlich „Kundendaten“ genannt. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien bei der Durchführung des Hauptvertrages.

1.6 Die datenschutz- sowie IT-sicherheitsrechtlichen Bestimmungen nach Maßgabe dieser Vereinbarung tragen gleichfalls dem Umstand Rechnung, dass wesentliche Kundendaten der anwaltlichen Schweigepflicht des Kunden als Berufspflicht unterliegen; der umfassende Schutz der infolge bestehenden Berufsgeheimnisses auch strafrechtlich geschützten Kundendaten durch WOLTERS KLUWER insbesondere vor unbefugter Offenbarung bildet insoweit ebenfalls eine zentrale Grundlage für die Regelungen in dieser Vereinbarung.

2. Auftragsverarbeitung

2.1 WOLTERS KLUWER erhebt, verarbeitet und/oder nutzt die Kundendaten ausschließlich im Auftrag und nach Weisung des Kunden („Auftragsverarbeitung“). Der Kunde bleibt im datenschutzrechtlichen Sinn verantwortliche Stelle und ist für die Rechtmäßigkeit der auftragsgemäßen Erhebung, Verarbeitung und/oder Nutzung der Kundendaten verantwortlich.

2.2 Die Dauer der Auftragsverarbeitung richtet sich nach dem Hauptvertrag.

3. Umfang, Art und Zweck der Datenverarbeitung, Art der Kundendaten und Kreis der Betroffenen

3.1 Umfang, Art und Zweck der Auftragsverarbeitung

a. Während der Beratungs- und Implementierungsphase führt WOLTERS KLUWER, je nach genauem Leistungsinhalt des Hauptvertrages, die folgenden Datenverarbeitungen durch:

- Planungs- und Beratungsleistungen
- Installation von OnPremise-Software
- Schulungen bzw. Online-Schulungen
- Telefonischer Service und Kundensupport
- Fehlerbehebung
- Datenmigration
- Datenübertragungen
- Datenbereinigung

b. WOLTERS KLUWER übernimmt den Support in der Betriebsphase. Dieser umfasst die folgenden Datenverarbeitungen:

- Online-Schulungen
- Fehlerbehebung
- bei cloudbasierten Diensten auch Remotezugriff auf das Benutzerkonto des Kunden in den dem Service zugrundeliegenden IT-Systemen
- bei cloudbasierten Diensten auch Umgang mit einem Echtdaten enthaltenen Dump/ Snapshot / Backup

c. Die Datenerhebung erfolgt in der Regel durch Remote-Zugriff von WOLTERS KLUWER auf die Daten des Kunden bzw. per Telefon, Fax oder E-Mail.

d. Des Weiteren stellt WOLTERS KLUWER dem Kunden im Rahmen der cloudbasierten Dienste Rechnerkapazität über ein Rechenzentrum zur Verfügung, über die die mit dem Kunden vertraglich vereinbarten Dienste bzw. Lösungen bereitgestellt werden und auf denen der Kunde Daten speichern kann. Hierzu zählen insbesondere der Betrieb der den Service zur Verfügung stellenden Front- und Backend-Systeme inklusive der Datenbanksysteme und Portalsysteme/Apps, sowie die Pflege der Hardwaresysteme, auf denen die Dienste basieren.

3.2 Art der Kundendaten, die WOLTER KLUWER erhebt, verarbeitet und nutzt

Die Datenverarbeitung betrifft, je nach genauem Leistungsinhalt des Hauptvertrages, folgende Daten der Betroffenen:

- Vor- und Nachname (ggf. Titel), Anrede
- Geburtsdatum
- Beruf/Tätigkeit
- Interessen
- Kontaktdaten und –historie
- Daten zur Geschäftshistorie
- Daten zu finanziellen Transaktionen
- Daten zu Bankverbindungen und Zahlungsarten
- Daten zur Vermögens und Ertragssituation
- Sonstige personenbezogenen Daten der Kontakte und Mitarbeiter
- Korrespondenz mit Mandanten und Dritten
- Mandantendaten und mandatsbezogene Akten bzw. Dokumente

3.3 Kreis der von der Auftragsverarbeitung Betroffenen

Die Datenverarbeitung betrifft folgenden Kreis von Betroffenen:

- Mandanten und sonstige Vertragspartner des Kunden
- Gesellschafter, Partner, Angestellte und sonstige Mitarbeiter des Kunden, einschließlich Referendare, wissenschaftliche Mitarbeiter und Hilfskräfte
- sonstige Personen, von denen der Kunde Daten in das System eingepflegt hat, wie Gegner von Mandanten

4. Pflichten von WOLTERS KLUWER

4.1 WOLTERS KLUWER verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Kunden angewiesen, es sei denn, WOLTERS KLUWER ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt WOLTERS KLUWER diese dem Kunden vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. WOLTERS KLUWER verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

4.2 WOLTERS KLUWER verpflichtet sich dazu und kontrolliert regelmäßig, dass die Verarbeitung der im Auftrag verarbeiteten Daten in seinem Verantwortungsbereich in Übereinstimmung mit den jeweils geltenden datenschutzrechtlichen Bestimmungen, und dieser Vereinbarung, einschließlich der technisch-organisatorischen Maßnahmen nach Ziffer 5, sowie mit den Weisungen des Kunden erfolgt. WOLTERS KLUWER hat seine Kontrollen zu dokumentieren und dem Kunden die Dokumentationen auf Verlangen vorzulegen.

4.3 WOLTERS KLUWER bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

4.4 WOLTERS KLUWER verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

4.5 WOLTERS KLUWER hat die bei der Erhebung, Verarbeitung und/oder Nutzung von Kundendaten beschäftigten Personen schriftlich auf das Datengeheimnis und zur Vertraulichkeit zu verpflichten und zu gewährleisten, dass jede ihm unterstellte Person die Daten des Kunden ausschließlich nach Maßgabe dieser Vereinbarung sowie den Weisungen des Kunden verarbeitet. Zusätzlich hat WOLTERS KLUWER entsprechend beschäftigte Personen über die dem Kunden obliegende anwaltliche und notarielle Schweigepflicht aufzuklären und die beschäftigten Personen in entsprechender Anwendung von § 43a Abs. 2 BRAO, § 2 BORA sowie § 18 BNotO sinngemäß und umfassend zu verpflichten. WOLTERS KLUWER ist insbesondere verpflichtet, seine Mitarbeiter über rechtliche Folgen aus einer Verletzung der anwaltlichen Schweigepflicht, insbesondere einer möglichen Strafbarkeit gemäß § 203 Abs. 1 Nr. 3 StGB, zu unterrichten. Auf Verlangen des Kunden wird WOLTERS KLUWER ihm die Einhaltung dieser Ziffer durch Vorlage der Verpflichtungserklärungen oder auf andere geeignete Weise nachweisen.

4.6 WOLTERS KLUWER ist dafür verantwortlich, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieser Vereinbarung vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen.

4.7 Im Zusammenhang mit der beauftragten Verarbeitung hat WOLTERS KLUWER den Kunden bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung sowie einer sich gegebenenfalls anschließenden Konsultation der Aufsichtsbehörde i.S.d. Art. 35, 36 DSGVO im Rahmen des Erforderlichen und Zumutbaren zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Kunden auf Anforderung zuzuleiten.

4.8 Wird der Kunde durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich WOLTERS KLUWER den Kunden im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

4.9 Auskünfte an Dritte oder den Betroffenen darf WOLTERS KLUWER nur nach vorheriger Zustimmung durch den Kunden erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Kunden weiterleiten und nicht selbst im Außenverhältnis gegenüber Dritten auftreten.

4.10 Soweit gesetzlich verpflichtet, bestellt WOLTERS KLUWER eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. Die Kontaktdaten des für WOLTERS KLUWER bestellten Datenschutzbeauftragten sind unter https://www.wolterskluwer.de/datenschutz hinterlegt. In Zweifelsfällen kann sich der Kunde direkt an den Datenschutzbeauftragten wenden. WOLTERS KLUWER ist verpflichtet, die Bestellung eines Datenschutz-beauftragten während der Dauer des Hauptvertrags aufrechtzuerhalten.

4.11 Die Auftragsverarbeitung erfolgt ausschließlich innerhalb der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Kunden und unter den in Kapitel V der DSGVO enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieser Vereinbarung erfolgen.

5. Datensicherheit/ Technische und organisatorische Maßnahmen

5.1 Die in Anlage 1 beschriebenen Datensicherheitsmaßnahmen gem. Art. 32 DSGVO werden als verbindlich festgelegt. Sie definieren das von WOLTERS KLUWER geschuldete Minimum.

5.2 Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird.

5.3 Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Kunden nicht oder nicht mehr genügen, benachrichtigt WOLTERS KLUWER den Kunden unverzüglich.

5.4 WOLTERS KLUWER verpflichtet sich dazu, die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt zu halten.

5.5 Kopien oder Duplikate werden ohne Wissen des Kunden nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

5.6 Dedizierte Datenträger, die vom Kunden stammen bzw. für den Kunden genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein.

5.7 WOLTERS KLUWER führt den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen. Der Nachweis ist dem Kunden jederzeit auf Anforderung zu überlassen und kann in Form geeigneter Zertifikate erfolgen.

6. Regelungen zur Berichtigung, Löschung und Sperrung von Daten

6.1 Im Rahmen des Auftrags verarbeitete Daten wird WOLTERS KLUWER nur entsprechend dieser Vereinbarung oder dem Hauptvertrag, gemäß gesetzlicher Vorschriften oder nach Weisung des Kunden berichtigen, löschen oder sperren.

6.2 Den entsprechenden Weisungen des Kunden wird WOLTERS KLUWER jederzeit und auch über die Beendigung des Hauptvertrages oder dieser Vereinbarung hinaus Folge leisten.

7. Mitteilungspflichten

7.1 WOLTERS KLUWER teilt dem Kunden Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle sind mitzuteilen. Die Mitteilung hat mindestens die Angaben nach Art. 33 Abs. 3 DSGVO zu enthalten.

7.2 Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße von WOLTERS KLUWER oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in dieser Vereinbarung getroffenen Festlegungen.

7.3 WOLTERS KLUWER informiert den Kunden unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

7.4 WOLTERS KLUWER verpflichtet sich dazu, den Kunden bei dessen Pflichten nach Art. 33 und 34 DSGVO im erforderlichen Umfang zu unterstützen. WOLTERS KLUWER ist verpflichtet, sämtliche Verletzungen des Schutzes von im Auftrag verarbeitete Daten einschließlich aller damit im Zusammenhang stehenden Fakten in einer Weise zu dokumentieren, die dem Kunden den Nachweis der Einhaltung etwa einschlägiger gesetzlicher Meldepflichten (z.B. nach Art. 33, 34 DSGVO) ermöglicht.

8. Unterauftragsverhältnisse

8.1 WOLTERS KLUWER darf zur Datenverarbeitung die in Anlage 2 aufgeführten Unterauftragsverarbeiter einsetzen.

8.2 Vor der Hinzuziehung weiterer oder der Ersetzung in Anlage 2 aufgeführter Unterauftragsverarbeiter informiert WOLTERS KLUWER den Kunden, um ihm die Möglichkeit zu geben, gegen derartige Änderungen Einspruch zu erheben. Ein solcher Einspruch bedarf eines wichtigen datenschutzrechtlichen Grundes. Im Fall eines wirksamen Einspruchs können beide Parteien den Hauptvertrag außerordentlich kündigen.

8.3 Unterauftragsverarbeitungen im Sinne dieser Vereinbarung sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

8.4 WOLTERS KLUWER wählt Unterauftragsverarbeiter unter besonderer Berücksichtigung von deren Eignung und den von ihnen getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus schließt mit ihnen jeweils vertragliche Vereinbarungen nach Maßgabe des Art. 28 Abs. 2 bis 4 DSGVO, die das im Hauptvertrag oder das in dieser Vereinbarung vereinbarte Schutzniveau nicht unterschreiten.

8.5 Die Verantwortlichkeiten von WOLTERS KLUWER und des Unterauftragsverarbeiters sind eindeutig voneinander abzugrenzen. Werden mehrere Unterauftragsverarbeiter eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen den einzelnen Unterauftragsverarbeiter. WOLTERS KLUWER haftet für ein Verschulden seiner Unterauftragsverarbeiter wie für eigenes Verschulden.

8.6 WOLTERS KLUWER hat die Einhaltung der Pflichten des Unterauftragsverarbeiter regelmäßig, spätestens alle 12 Monate, angemessen zu überprüfen. Die Prüfung und ihr Ergebnis sind so aussagekräftig zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind. Die Dokumentation ist dem Kunden auf Verlangen vorzulegen.

8.7 WOLTERS KLUWER hat auch die Pflicht, zu überprüfen, dass die Mitarbeiter des Unterauftragsverarbeiters vor Beginn der Verarbeitung entsprechend Ziffer 4.5 verpflichtet worden sind.

8.8 Die Verpflichtung und Anhaltung der Mitarbeiter zur Wahrung der Verschwiegenheit entsprechend § 2 Abs. 5 BORA/§ 18 BNotO ist auch bei den Unterauftragsverarbeitern regelmäßig (d.h. mindestens einmal jährlich) in geeigneter Form zu überprüfen.

9. Rechte und Pflichten des Kunden

9.1 Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Kunde verantwortlich.

9.2 Der Kunde erteilt alle Aufträge, Teilaufträge oder Weisungen und dokumentiert sie. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Kunde unverzüglich dokumentiert bestätigen.

9.3 Der Kunde informiert WOLTERS KLUWER unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

9.4 Der Kunde ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen bei WOLTERS KLUWER in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist von WOLTERS KLUWER soweit erforderlich Zutritt und Einblick zu ermöglichen. WOLTERS KLUWER ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.

9.5 Kontrollen bei WOLTERS KLUWER haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Kunden zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten von WOLTERS KLUWER, sowie nicht häufiger als alle 12 Monate statt. Soweit WOLTERS KLUWER den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie unter Ziffer 5.7 vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

9.6 Gemäß den Bestimmungen der DSGVO unterliegen die Parteien öffentlichen Kontrollen durch die zuständige Aufsichtsbehörde. Auf Anforderung durch den Kunden wird WOLTERS KLUWER die gewünschten Informationen an die Aufsichtsbehörde liefern und dieser die Möglichkeit zur Prüfung einräumen; davon umfasst sind Inspektionen bei WOLTERS KLUWER durch die Aufsichtsbehörde. WOLTERS KLUWER gewährt der zuständigen Aufsichtsbehörde in diesem Rahmen die erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte.

10. Weisungen

10.1 Der Kunde behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

10.2 Die Parteien benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 3.

10.3 Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.

10.4 WOLTERS KLUWER wird den Kunden unverzüglich darauf aufmerksam machen, wenn eine vom Kunden erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. WOLTERS KLUWER ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Kunden bestätigt oder geändert wird.

10.5 WOLTERS KLUWER hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

11. Beendigung des Auftrags

11.1 Es ist WOLTERS KLUWER untersagt, die im Auftrag verarbeiteten Daten nach Beendigung des Hauptvertrags aktiv zu verarbeiten. Bei Beendigung des Hauptvertrages oder jederzeit auf Verlangen des Kunden hat WOLTERS KLUWER die im Auftrag verarbeiteten Daten nach Wahl des Kunden entweder zu vernichten oder an den Kunden herauszugeben oder einen Datenexport zu ermöglichen und sodann zu vernichten. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist

11.2 WOLTERS KLUWER ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Unterauftragnehmern herbeizuführen.

11.3 WOLTERS KLUWER hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Kunden unverzüglich vorzulegen.

11.4 Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch WOLTERS KLUWER auch über das Vertragsende hinaus aufzubewahren. Er kann sie dem Kunden zu seiner Entlastung bei Vertragsende übergeben.

12. Vergütung

Die Vergütung für WOLTERS KLUWER ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieser Vereinbarung erfolgt nicht.

13. Sonstiges

13.1 Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

13.2 Sollte Eigentum des Kunden bei WOLTERS KLUWER durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat WOLTERS KLUWER den Kunden unverzüglich zu verständigen.

13.3 Im Falle von Widersprüchen zwischen dieser Vereinbarung und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieser Vereinbarung vor.

13.4 Für Nebenabreden ist die Schriftform erforderlich.

13.5 Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

13.6 Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

(Stand: Mai 2018)

_____, den _____ _____, den _____

_____ _____

[Unterschrift WOLTERS KLUWER] [Unterschrift des Kunden]

Anlage 1 – Technische und organisatorische Maßnahmen
für cloudbasierte Dienste: Kleos, effacts und OnPremise-Software: AnNoText, winra, TriNotar, DictaPlus / DictNow mit optionalen Online-Erweiterungen: Smarte AnwaltsAkte, OnlineAkte, DictNow Diktier-App

Der nachstehende Maßnahmenkatalog beschreibt die von der Wolters Kluwer Deutschland GmbH (nachstehend „WOLTERS KLUWER“) im Rahmen ihrer Tätigkeit für den Kunden zu treffenden technischen und organisatorischen Maßnahmen gemäß Art 32 DSGVO.

Der Schutz von personenbezogenen Daten des Kunden in den Geschäftsräumen von WOLTERS KLUWER wird durch die dort implementierten technischen und organisatorischen Maßnahmen gewährleistet. Diese Maßnahmen sind nachstehend unter den Gliederungsabschnitten „Gebäude / Geschäftsräume“ und „Standort-IT“ dargestellt.

Sofern die Verarbeitung von personenbezogenen Daten durch Dritte (Unterauftragnehmer) erfolgt, werden diese von WOLTERS KLUWER sorgfältig ausgewählt. Von WOLTERS KLUWER beauftragte Rechenzentrumsdienstleister sind zertifiziert und gewährleisten den Schutz von personenbezogenen Daten des Kunden durch entsprechende, dort implementierte technische und organisatorische Maßnahmen.

Sofern Sie die cloudbasierten Dienste Kleos oder effacts nutzen, finden Sie die entsprechenden produktspezifischen Beschreibungen beigefügt.

I. Vertraulichkeit (Art 32 Abs. 1 lit. b) DSGVO

1. Zutrittskontrolle

WOLTERS KLUWER muss für den Zeitraum der Auftragsdatenverarbeitung angemessene Maßnahmen ergreifen, um den Zugang unautorisierter Personen zu personenbezogenen Daten zu verhindern.

1.1 Gebäude / Geschäftsräume

- Das Gebäude und die Geschäftsräume sind durch Videoüberwachung (7 Kameras) 24h gesichert.
  - o Montag - Freitag 00:00 – 24.00 Uhr
  - o Wochenende und Feiertage 00:00 – 24:00 Uhr

- Zutritt zum Gebäude ist nur über Chip und Schlüssel möglich; Etagen und Flurabschnitte innerhalb des Gebäudes sind nur mit Chip zugänglich.

- Besetzung Empfang durch Sicherheitsdienst:
  - o Montag - Freitag 07:00 – 17:00 Uhr

- Chip (hausinternes System) wird nur den Mitarbeitern von WOLTERS KLUWER und den Mitarbeitern des Sicherheitsdienstes zur Verfügung gestellt.

- Besucherregelung: Besucher müssen sich am Empfang anmelden und erhalten einen sichtbar zu tragenden Besucherausweis; Besucher werden von einem Mitarbeiter von WOLTERS KLUWER abgeholt und durch die Geschäftsräume begleitet.

1.2 Rechenzentrum

Die DV-Anlagen befinden sich in Räumen oder Rechenzentren (nachstehend auch Dienstleister) mit Zutrittskontrolle. Die Zutrittskontrolle erfolgt in unterschiedlicher Ausprägung. Der für den Zugang autorisierte Personenkreis für die Rechenzentren wird von WOLTERS KLUWER vorab oder mittels schriftlicher Änderungsmitteilung gegenüber dem Dienstleister festgelegt und vor Ort durch entsprechendes Support-Personal des Rechenzentrumsbetreibers durch Vorlage des Personalausweises authentifiziert. Der Zutritt wird protokolliert. Der Zutritt in weitere Bereiche erfolgt per Magnet- bzw. Chipkarte mit Zahlencode oder Sicherheitsschlüssel (Raumzugang) und Schließanlage (Rack Zugang). Diese Bereiche unterliegen einer Videoüberwachung, sowie erweiterten Maßnahmen zum Einbruchsschutz.

Mitarbeiter von WOLTERS KLUWER erhalten nach denselben Regeln Zutritt zu den Rechenzentren. IT-Verantwortliche des Dienstleisters haben eine permanente Zutrittsberechtigung für die Rechenzentren. Die Zutrittskontrolle der Mitarbeiter zu den DV- Anlagen in den Arbeitsräumen des Dienstleisters oder dessen Subunternehmen erfolgt per Magnet- bzw. Chipkarte mit Zahlencode. Die Zutrittsbereiche unterliegen einer Videoüberwachung.

Personen, die nicht zum Kreis der Mitarbeiter des Dienstleisters oder von WOLTERS KLUWER gehören (beispielsweise Wartungstechniker) erhalten ebenfalls nach denselben Regeln Zutritt zu den Rechenzentren. Der Zutritt wird in diesem Fall außerdem jeweils durch die IT-Verantwortlichen von WOLTERS KLUWER autorisiert und erfolgt nur in Begleitung von Support-Personal des Dienstleisters. Die Kenntnisnahme der Zutritts- und Verhaltensregeln wird protokolliert.

WOLTERS KLUWER benennt dem Dienstleister nach einem abgestuften Berechtigungskonzept sämtliche Änderungsberechtigte. Für diese sind die Zutrittsprotokolle zu den Rechenzentren jederzeit einsehbar und abrufbar.

Der Zutritt zu DV- und TK-Systemen wird Unbefugten demnach durch folgende Maßnahmen verwehrt:

- Sicherheitszonen/Sperrbereiche
- Automatische Zutrittskontrolle (Magnetkarte / Token mit PIN)
- Schlüsselregelung
- Personenkontrolle durch Pförtner

Lage des Rechenzentrums: DE 89081 Ulm

2. Zugangskontrolle

WOLTERS KLUWER sorgt dafür, dass nur entsprechend autorisierte Personen Zugang zu personenbezogenen Daten haben.

2.1 Standort-IT

Zugriffe auf Clients, Server und Daten unterliegen einem einheitlichen Rollen- und Berechtigungskonzept und sind grundsätzlich personenbezogen passwortgeschützt. Das Passwort muss spätestens nach 3 Monaten erneuert werden, sonst wird das zugehörige Benutzerkonto automatisch gesperrt. Auch nach fünfmaliger Eingabe falscher Anmeldeinformationen erfolgt eine Sperre des Benutzers.

Die Änderung und die damit verbundenen Änderungsregelungen von Passwörtern unterliegen technisch fest definierten Regeln. Es gelten folgende Parameter:

- Passwortlänge mindestens 15 Zeichen
- Sonderzeichen und Ziffern sind erforderlich
- Das Passwort muss sich zu den letzten 30 vergebenen Passwörtern unterscheiden

Alle Berechtigungen werden anhand eines Vier-Augen-Prinzips vergeben, wobei der jeweilige Vorgesetzte die Anforderung des Benutzers oder externen Dienstleisters bestätigen muss. Die Umsetzung der Anforderung obliegt im Rahmen der Aufgabentrennung der IT. Alle Anforderungen werden in einer internen Vorgangsdatenbank protokolliert. Zugriff auf diese Datenbank haben ausschließlich Mitarbeiter der WOLTERS KLUWER IT. Von der IT erstellte initiale Kennwörter werden mit dem Status ‚Abgelaufen' versehen, so dass der Benutzer zunächst sein Kennwort ändern muss. Ab diesem Zeitpunkt ist niemand anderem als dem Benutzer selbst das Kennwort bekannt.

Benutzerkonten werden nach einem abgestuften Berechtigungskonzept erstellt:

- Administratorenkonten haben in der Regel vollen Zugriff auf die DV-Anlagen. Jeder Administrator erhält auch ein reguläres Benutzerkonto und ist gehalten, das Administratorkonto nur für Zwecke zu nutzen, die den erweiterten Berechtigungsumfang zwingend erfordern.

- Benutzerkonten erhalten dedizierten Zugriff (opt-in) auf die zur jeweiligen Tätigkeit bezogenen erforderlichen Dienste und Daten. Das zugrundeliegende Berechtigungssystem ist durchgängig mit 1:1-Beziehungen aufgebaut, eine Bündelung von Berechtigungen für verschiedene Dienste findet nicht statt.

- Konten für Dienstleister erhalten ebenfalls dedizierten Zugriff auf die zur jeweiligen Tätigkeit bezogenen erforderlichen Dienste. Im Unterschied zu internen Benutzern muss aber der jeweilige Auftraggeber des externen Nutzers nach 3 Monaten die Verlängerung des Benutzerkontos explizit bestätigen.

Die Maßnahmen zum Schutz vor unbefugter Nutzung von Diensten, Daten und Applikationen lauten im Einzelnen:

- Lokale Verschlüsselung der Endgeräte
- Lokale Verschlüsselung von Wechseldatenträgern
- Firewall (Cluster)
- Virenschutz mit aktiviertem Zugriffsscanner
- Client-VPN
- Umfangreiches Patchmanagement aller DV-Komponenten und Applikationen
- 2-Faktor-Authentifizierung bei externen Verbindungen (OTP)
- Zahlreiche systemweit implementierte Gruppenrichtlinien

Darüber hinaus gibt es zu Datenschutz und IT-Sicherheit umfangreiche interne Richtlinien, welche allen Mitarbeitern von WOLTERS KLUWER vorgelegt und mindestens jährlich anhand eines Trainings rekapituliert werden. Dazu zählen unter anderem praxisbezogene Aufgaben über die Verhinderung unbefugter Zugriffe am Client, der sachgerechte Umgang mit Mobilgeräten, Datenträgern und Papierinformationen, Sensibilisierung für Betrugsversuche und die Prüfung von E-Mails unbekannter Quelle auf Schadroutinen.

2.2 Rechenzentrum

Der Betreiber des Rechenzentrums hat keinen Zugriff auf Daten, die WOLTERS KLUWER im Rahmen seiner Auftragsverarbeitung erfasst und speichert. Dem Dienstleister obliegt ausschließlich die operative Betreuung der technischen Plattforminfrastruktur. Dazu zählen, neben dem Betrieb des Rechenzentrums selbst, insbesondere die Betreuung der Datenspeicher, der Virtualisierungs-umgebung, sowie der Netzwerk- und Internet-Infrastruktur. Die unbefugte Nutzung von DV-Systemen des Rechenzentrumbetreibers wird hierbei durch folgende Maßnahmen verhindert:

- Dedizierte Glasfaserverbindungen (Site to Site)
- VPN-Verbindungen
- Ausweisleser
- Funktionelle Zuordnung einzelner Datenendgeräte
- Protokollierung der Systemnutzung und Protokollauswertung
- Firewall
- Virenschutz

Darüber hinaus steht dem Betreiber des Rechenzentrums für Notfälle eine nicht personifizierte Systemadministratorkennung zur Verfügung. Diese wird unter Verschluss (Tresor) vom 1stLevel-Support des Dienstleisters verwaltet und in regelmäßigen Abständen geändert. Die Notwendigkeit für den Zugang muss vom 2ndLevel-Support des Dienstleisters qualifiziert werden. Die Kennung wird dann protokolliert vom 1stLevel-Support herausgegeben. Die Verwendungsprotokolle sind durch WOLTERS KLUWER jederzeit einsehbar und abrufbar.

Die nach ISO27001 zertifizierte Umgebung gestattet eine klare Trennung administrativer Zugriffe zwischen dem Plattformmanagement des Rechenzentrumbetreibers und den darauf aufsetzenden Diensten, Daten und Applikationen. Daher müssen die Schutzmaßnahmen getrennt betrachtet werden und können sich je nach Anforderung von den Maßnahmen zum Schutz der Plattforminfrastruktur unterscheiden.

Die Maßnahmen zum Schutz vor unbefugter Nutzung von Diensten, Daten und Applikationen lauten im Einzelnen:

- Firewall (Cluster)
- Loadbalancer (Cluster)
- Virenschutz mit aktiviertem Zugriffsscanner
- Site-to-Site-VPN
- Umfangreiches Patchmanagement aller DV-Komponenten und Applikationen
- Zahlreiche systemweit implementierte Gruppenrichtlinien

3. Zugriffskontrolle

WOLTERS KLUWER trifft geeignete Maßnahmen, um zu verhindern, dass unautorisierte Personen auf personenbezogene Daten des Kunden zugreifen. Außerdem trifft WOLTERS KLUWER angemessene Maßnahmen, die das unautorisierte Lesen, Kopieren oder Löschen der Daten sowie die unautorisierte Speicherung oder Veränderung von gespeicherten personenbezogenen Daten verhindern sollen.

3.1 Standort-IT

- Die Mitarbeiter von WOLTERS KLUWER sind vertraglich verpflichtet, die ihnen zur Verfügung gestellten Datenverarbeitungssysteme ausschließlich für berufliche Zwecke zu nutzen. Die Mitarbeiter im Bereich WOLTERS KLUWER Legal Software werden darüber hinaus schriftlich zur Berufsverschwiegenheit verpflichtet.

- Die Vergabe von Zugriffsrechten erfolgt nach Aufgaben- und Verantwortungsbereichen. Für die Benutzerverwaltung wird die Benutzerverwaltung „Active Directory“ von Microsoft eingesetzt.

- Unterlagen und Datenträger mit personenbezogenen Daten werden intern in Datenschutzcontainern entsorgt. Die weitere Entsorgung und Vernichtung werden von einem Dienstleister nach DIN 66399 datenschutzgerecht entsorgt und vernichtet.

- Berechtigungen werden nach dem need-to-know-Prinzip vergeben. Jeder Benutzer erhält nur die Zugriffsrechte, die er zwingend zur Erledigung seiner Aufgaben benötigt. Dafür sind zahlreiche Gruppenrichtlinien im Verzeichnisdienst vordefiniert. Die Vorgaben nach denen ein Benutzer angelegt wird, bestimmt die Personalabteilung sowie der Vorgesetzte des Benutzers. Die IT-Abteilung steht beratend zur Seite. Regelmäßig finden interne Qualitätskontrollen in unterschiedlicher Ausprägung statt. Außerdem stellt die IT bei internen und externen Audits sowie bei Prüfungen durch Kunden die nötigen Informationen entsprechend der Anfrage und unter Beachtung des Datenschutzes gesammelt zur Verfügung.

- Ein- und Austrittsprozesse sowie Änderungen in Rollen und Berechtigungen unterliegen einem festgelegten Prozess. Zugriff auf sensible Daten und Applikationen werden nur auf gezielte Anforderung erteilt. Lokale Administrationsrechte sind nur in Ausnahmefällen zulässig und möglichst nicht mit dem Standardbenutzer zu verknüpfen. Die Installation von Programmen auf dem Client durch den Benutzer ist nur über ein zentrales Softwareportal möglich, welches von der IT kuratiert wird und dem globalen Standardkatalog für bei WOLTERS KLUWER zulässige Software entspricht.

- Systemanmeldungen und Zugriffe auf Daten werden dezentral protokolliert und im Bedarfsfall ausgewertet.

3.2 Rechenzentrum

Die Verwaltung der Zugriffsrechte des Rechenzentrumsbetreibers obliegt dem Dienstleister. Dabei ist eine klare Trennung nach Verantwortlichkeiten und Rollen gegeben. Vom Dienstleister verwaltete Zugänge zum Betrieb des Rechenzentrums stehen WOLTERS KLUWER zu keiner Zeit zur Verfügung. Von WOLTERS KLUWER verwaltete Zugänge werden dem Dienstleister nicht zur Verfügung gestellt.

3.3 Fernwartung der Vertragssoftware

Die Fernwartung erfolgt durch Mitarbeiter von WOLTERS KLUWER oder durch Partnerunternehmen. Zwischen WOLTERS KLUWER und ihren Partnerunternehmen (Unterauftragnehmern) werden schriftlich oder in einem elektronischen Format Vereinbarungen zur Auftragsverarbeitung von personenbezogenen Daten geschlossen.

Der Zugriff auf die Rechner des Kunden erfolgt nur aufgrund ausdrücklicher Einwilligung des Kunden.

4. Trennungskontrolle

WOLTERS KLUWER trifft geeignete Maßnahmen um sicherzustellen, dass eine getrennte Verarbeitung von Daten erfolgt, die zu unterschiedlichen Zwecken erhoben wurden.

4.1 Standort-IT

Neben dem abgestuften Rollen- und Berechtigungskonzept werden unterschiedliche Techniken zur Abgrenzung unterschiedlicher Prozesse implementiert.

Bei Diensten, die über das Internet erreichbar sind, werden Backendsysteme, wie z.B. Datenbanken vom Frontend logisch über separate VLANs abgetrennt. Der Datenfluss zwischen Front- und Backend ist über das zentrale Firewallcluster abgesichert. Üblicherweise sind diese Systeme zur Sicherung der Abgrenzung von Kundendaten dediziert für den einzelnen Dienst angelegt. Test- und Stagingsysteme laufen auf logisch und physikalisch getrennten Hosts.

Zusätzliche VLANs sorgen auch für eine Trennung nach Dienstmerkmalen. So gibt es neben den Client-VLANs an den Betriebsstätten noch separate VLANs für Routing, Server und Hardware-Remote-Management. Auch nicht dem Verzeichnisdienst zugehörige Clients werden automatisch in ein VLAN mit stark eingeschränkten Zugriffsrechten eingebucht. Öffentlich zugängliche Bereiche wie Konferenzräume sind ebenfalls mit Netzen mit beschränkten Zugriff ausgestattet. Anmeldungen ins interne Netz über WLAN muss für Besucher einzeln von einem internen Mitarbeiter akkreditiert werden.

4.2 Rechenzentrum

Kunden des Rechenzentrumsbetreibers werden logisch, technisch auf Ebene der Infrastruktur und teilweise auch räumlich voneinander abgetrennt. Dabei ist insbesondere sichergestellt, dass es zu keiner Zeit zum Zugriff, Einsicht oder Überschneidung zwischen den Instanzen kommt.

5. Verschlüsselung

5.1 Standort-IT/Rechenzentrum

Verschlüsselung kommt in unterschiedlichen Szenarien zum Einsatz. Neben der Verschlüsselung von Client- und Wechseldatenträgern wird, sowohl intern wie auch extern, insbesondere die Datenübertragung umfangreich verschlüsselt.

Unternehmensübergreifende Dienstvernetzung über entsprechende Schnittstellen werden üblicherweise mit einem IPSec Tunnel realisiert. Das gilt sowohl für Standorte der WOLTERS KLUWER außerhalb Deutschlands als auch für Dienstleister sowie in einigen Fällen auch Verbindungen zu Kunden.

Nahezu alle Online-Angebote werden mit TLS Zertifikaten ausgestattet und leiten alle unverschlüsselten Anfragen auf die entsprechende https Variante um.

Auch der E-Mailverkehr ist bis zum SMTP-Gateway TLS verschlüsselt. Müssen Daten in größerem Umfang übertragen werden, muss dies ebenfalls verschlüsselt per sFTP oder NextCloud (TLS+AES) erfolgen.

Remote-Dienste für die Mitarbeiter von WOLTERS KLUWER unterliegen ebenfalls einer VPN- oder TLS-Verschlüsselung (Citrix). Passwörter werden verschlüsselt gespeichert.

II. Integrität (Art 32 Abs. 1 lit. a) und b) DSGVO

1. Weitergabekontrolle

WOLTERS KLUWER ergreift Maßnahmen um sicherzustellen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, verändert, kopiert oder vernichtet werden können. WOLTERS KLUWER ermöglicht weiterhin die Überprüfung und Bestimmung der Stellen/Orte, an die personenbezogene Daten der Betroffenen übermittelt werden.

1.1 Standort-IT

Es sind umfangreiche interne Bestimmungen und Regelungen zum Einsatz sensibler Daten, mobiler Datenträger, mobiler und stationärer Arbeitsplatzrechner, E-Mail-Kommunikation usw. implementiert. Diese werden mindestens einmal jährlich allen Mitarbeitern gegenüber im Rahmen einer Trainingsmaßnahme aktualisiert.

Die Mitarbeiter sind grundsätzlich zur Verschwiegenheit verpflichtet.

1.2 Rechenzentrum

Die Mitarbeiter des von WOLTERS KLUWER beauftragten Rechenzentrums haben keine Möglichkeit, Daten in die dort gehostete Vertragssoftware und Datenverarbeitungssysteme einzugeben. Sie haben insbesondere keine Möglichkeit, personenbezogene Daten des Kunden einzusehen, zu verändern oder zu entfernen.

2. Eingabekontrolle

WOLTERS KLUWER muss dafür Sorge tragen, dass nachträglich geprüft und festgestellt werden kann, ob und wann personenbezogenen Daten in Datenverarbeitungssysteme eingegeben, geändert oder entfernt worden sind.

2.1 Standort-IT

An den Betriebsstätten von WOLTERS KLUWER findet keine Eingabe, Änderung oder Löschung der Daten statt, eine Zugriffsprotokollierung ist nicht erforderlich.

2.2 Rechenzentrum

Änderungen an personenbezogenen Daten werden den jeweiligen Dienstanforderungen entsprechend protokolliert und bei Bedarf ausgewertet.

Die Mitarbeiter des von WOLTERS KLUWER beauftragten Rechenzentrums haben keine Möglichkeit, Daten in die dort gehostete Vertragssoftware und Datenverarbeitungssysteme einzugeben. Sie haben insbesondere keine Möglichkeit, personenbezogene Daten des Kunden einzusehen, zu verändern oder zu entfernen.

III. Verfügbarkeit und Belastbarkeit (Art 32 Abs. 1 lit. b) DSGVO)

1. Verfügbarkeitskontrolle

WOLTERS KLUWER hat zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

1.1 Standort-IT

Das Speichern von personenbezogenen Kundendaten oder sonstiger sensibler Daten auf lokalen Clients ist in der Regel nicht vorgesehen und dem Mitarbeiter untersagt. Diese Daten sind grundsätzlich auf Netzlaufwerken und zentralen Servern im Rechenzentrum vorgesehen. Um dennoch einen Zugriffsschutz im Falle eines Diebstahls von Clients zu gewährleisten, sind die lokalen internen und externen Speichermedien verschlüsselt.

1.2 Rechenzentrum

Ein Ausfall des zentralen ERP-Systems ist mit einem cold-standby-System im getrennten Brandabschnitt mit geringer Ausfallzeit überbrückbar.

Die Hauptdatenspeicher sind ebenfalls redundant ausgelegt. Alle Daten liegen in einem mehrfach kreuzangebundenen doppelten Kopf auf RAID-gespiegelten Diskshelfs. Das gilt sowohl für Netzlaufwerkspeicher als auch für virtuelle Server.

Darüber hinaus sind zentrale Netzwerkkomponenten (Switche, Router, Backbone, Firewall, Loadbalancer, zahlreiche Front- und Backendsysteme) ebenfalls redundant ausgelegt.

IV. Maßnahmen zur schnellen Wiederherstellbarkeit (Art 32 Abs. 1 lit. c) DSGVO)

WOLTERS KLUWER ergreift Maßnahmen, um die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

1.1 Standort-IT

Die Netzwerkverbindung der größten Standorte von WOLTERS KLUWER zum zentralen Rechenzentrum ist über eine zweifache Anbindung mit automatischem Failover vor einem Ausfall geschützt.

1.2 Rechenzentrum

WOLTERS KUWER sichert seine Daten im Rahmen eines einheitlichen Backupkonzepts. Datenlaufwerke und Server werden nach folgendem Schema gesichert:

- Vollständiges Backup aller Systeme an Wochenenden
- Inkrementelle Backups täglich
- Snapshot-Sicherungen der Server
- Aufbewahrungsfristen je nach Anforderung zwischen 4 Wochen und einem Jahr
- Langzeitarchivierung von Kunden- und kaufmännischen Daten auf dediziertem, georedundanten Archivsystem gemäß gesetzlich vorgeschriebenen Zeiträumen

Die Backup-Infrastruktur besteht aus einer gemischten Festplatten- und Tape-Infrastruktur. Diese befindet sich von den Produktivsystemen getrennt in einem separaten Brandabschnittsbereich des Rechenzentrums. Zugang und Zugriff haben ausschließlich IT-Mitarbeiter von WOLTERS KLUWER sowie der Rechenzentrumsbetreiber.

WOLTERS KLUWER hält darüber hinaus einen Notfallplan zur Wiederherstellung der Umgebung bereit. Abhängigkeiten und Prioritäten der Dienste sind dokumentiert, ein Test zur Wiederherstellung kritischer Systeme findet mindestens einmal jährlich statt. Jede Anfrage zur Wiederherstellung von Daten wird von der IT geprüft und freigegeben. Dabei wird sichergestellt, dass der Anfragende entsprechende Berechtigungen auf die zu wiederherstellenden Daten hat.

V. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art 32 Abs. 1 lit. d) DSGVO, Art 25 Abs. 1 DSGVO)

1. Auftragskontrolle

1.1 WOLTERS KLUWER und Kunde

Zwischen WOLTERS KLUWER und ihren Kunden werden schriftlich oder in einem elektronischen Format Vereinbarungen zur Auftragsverarbeitung von personenbezogenen Daten geschlossen.

WOLTERS KLUWER verarbeitet personenbezogene Daten des Kunden aufgrund der von dem Kunden erteilten Weisungen. Weisungen erfolgen schriftlich oder in Textform, mündlich erteilte Weisungen werden schriftlich oder in Textform dokumentiert.

1.2 WOLTERS KLUWER und Unterauftragnehmer

Unterauftragnehmer werden von WOLTERS KLUWER sorgfältig ausgewählt.

Zwischen WOLTERS KLUWER und ihren Unterauftragnehmern werden schriftlich oder in einem elektronischen Format Vereinbarungen zur Auftragsverarbeitung von personenbezogenen Daten geschlossen, die ein angemessenes Schutzniveau für den Umgang mit und die Verarbeitung von personenbezogenen Daten gewährleisten.

2. Datenschutzmanagement

WOLTERS KLUWER hat einen externen Datenschutzbeauftragten bestellt.

WOLTERS KLUWER hat eine interne Datenschutzorganisation bestehend aus einen zentralen Datenschutzkoordinator und Single Point of Contacts für die Unternehmensbereiche eingerichtet.

Mitarbeiter von WOLTERS KLUWER werden für den Umgang mit personenbezogenen Daten sensibilisiert und geschult.

Bei WOLTERS KLUWER bestehen Regelungen für den Umgang mit Datenschutz- und Sicherheitsvorfällen.

Bei WOLTERS KLUWER sind Verfahren für den Umgang mit Betroffenenrechten (z.B. Anfragen von Betroffenen) eingerichtet.

Anlage 2 – Unterauftragsverarbeiter

Name	Anschrift	Auftragsinhalt
Wolters Kluwer Technology B.V.	Zuidpoolsingel 2 2408 ZE Alphen aan den Rijn Niederlande	2nd Level Support und Softwareentwicklung für Kleos und effacts Bereitstellung des Systems für die Incident-Verwaltung
Wolters Kluwer Italia S.r.L.	Centro Direzionale Milanofiori Strada 1, Palazzo 6 20090 Assago Italien	2nd & 3rd Level Support und IT Operations für Kleos und effacts
Wolters Kluwer Nederland B.V.	Zuidpoolsingel 2 2408 ZE Alphen aan den Rijn Niederlande	2nd Level Support, Entwicklung und Consulting effacts
Teleperformance Portugal SA	Cais dos Argonautas Lote 2.34.01 Lisbon Portugal	1st Level Software Support
NTT DATA Romania SA	19-21 Constanta St. 400158 Cluj-Napoca Rumänien	Softwareentwicklung AnNoText und winra
Schleupen AG	Otto-Hahn-Str. 20 76275 Ettlingen	Software Installationsdienstleistungen für AnNoText, TriNotar, DictaPlus / DictNow und winra
Kurth EDV Beratung	Von Kühlmannstr. 11 82327 Tutzing	Softwareentwicklung AnNoText
Grundig Business Systems GmbH	Emmericher Straße 17 90411 Nürnberg	Hardwarelieferant für Diktierhardware für DictaPlus / DictNow
Speech Processing Solutions Germany GmbH	Tauentzienstraße 9-12 Europa-Center 10789 Berlin	Hardwarelieferant (Philips) für Diktierhardware für DictaPlus / DictNow
Recognosco GmbH	Tech Gate Donau-City-Straße 1 1220 Wien Österreich	Lizenzgeber der Spracherkennungssoftware für DictaPlus / DictNow
Deltavista GmbH	Freisinger Landstr. 74 80939 München	Angebot von Dienstleistungen von Deltavista durch die Software AnNoText
EURO-PRO Gesellschaft für Data Processing mbH	Lindenhof 1-3 61279 Grävenwiesbach	Angebot von Dienstleistungen von EURO-PRO (Supercheck) durch die Software AnNoText
eConsult AG	Robert-Koch-Straße 18 66119 Saarbrücken	Angebot von Dienstleistungen von eConsult durch die Software AnNoText

Smartsheet.com Inc.	10500 NE 8th St., Suite 1300, Bellevue WA 98004 USA	Software zur gemeinsamen Erstellung und Bearbeitung von Projektplänen in der Onboarding-Phase des Kunden
BugSplat LLC.	1023 Walnut St Boulder, CO 80302 USA	Implementierte Software in AnNoText, winra und TriNotar zur Meldung und Analyse von Systemabstürzen
LogMeIn Inc.	320 Summer Street Boston, MA 02210 USA	Software zur Durchführung von Webinaren
TeamViewer GmbH	Jahnstr. 30 73037 Göppingen	Software für Remote-Support
T-Systems International GmbH	Data Centre Munich/Allach Dauchauer Strasse 665 80995 München Data Centre Munich/Eip Elisabeth Selbert Strasse 1 80939 München	Hosting des cloudbasierten Dienstes Kleos
scanplus GmbH (Telekom Deutschland GmbH)	Lise-Meitner-Strasse 5 89081 Ulm	Hosting der internen Systeme von Wolters Kluwer Deutschland sowie Hosting des cloudbasierten Dienstes Smarte AnwaltsAkte
NTT DATA Deutschland GmbH	Königsberger Straße 1 60487 Frankfurt a. M.	Hosting des cloudbasierten Dienstes effacts
rockenstein AG	Ohmstraße 12 97076 Würzburg	Hosting des cloudbasierten Dienstes OnlineAkte und DictNow Diktier-App
DocuSign, Inc.	1301 Second Avenue, Suite 2000 Seattle, WA 98101 USA	Elektronische Signatur der Legal Dokumente bei effacts

Anlage 3 – Weisungsberechtigte Personen
- vom Kunden auszufüllen -

Folgende Personen des Kunden sind zur Erteilung von Weisungen befugt:

Name	**Funktion**

Productsheet effacts

1. **Nature of the Processing**
   Cloud-based platform offering a database for storing and managing legal documents, including contracts management and corporate housekeeping.

2. **Categories of Personal Data that are processed**
   Processor will process the following categories of Personal Data from the Controller exclusively in the context of the Service Agreement:

   - Identity data (last name, first name, login name)
   - Contact information (address, e-mail, IP address, telephone, fax)
   - Behavioural data (user history)

   In addition, the Processor may process the Personal Data originated by the Controller. The Personal Data originated, entered and uploaded in effacts by the Controller will be at the Controller's sole discretion and risk. The Processor will not have access to or be able to be aware of what kind of Personal Data has been originated by the Controller and as such the Processor cannot know in advance what kind of personal data will be originated, entered and uploaded in effacts by the Controller. However, within the purpose of the performance of the Services Agreement categories of data originated by the Controller may include the following:

   - Identity data (name, address, mobile phone, e-mail, date of birth, ...)
   - Identity data issued by the government (national register number, passport number, ...)
   - Social status (family situation, ...)
   - Financial information (bank account number, ...)

3. **Categories of data subjects involved in the Processing of personal data in Kleos**

   - Clients and partners of the Controller
   - Shareholders, partners, employees and other staff members of the Controller, including trainees, research assistants, etc;
   - Other persons whose data are processed by the Controller, such as counterparties.

4. **Purposes of the processing**
   Processor stipulates that you can use effacts for the purposes below:

   - Central management of dossiers, contact data and documents
   - Linking to your internal and external sources
   - Extensive search and reporting possibilities
   - Exporting information for reports and so forth.

5. **Retention period**
   As Controller, you yourself determine the retention period of your client information (dossiers, identity data, documents, etc.)

   Wolters Kluwer makes a backup of all client databases daily. This backup is kept for 30 days.

   Personal data will be processed and kept for the following periods:

   - **After migration of your data from another software package**: we keep no information after migration from the former software package. The Controller itself is responsible for copying/backup of this information and make it available to Wolters Kluwer if necessary
   - **Personal data via support/helpdesk**: contacts are anonymised six months after the termination of the contract. As Controller you make sure not to transmit sensible data during the ticket resolution (screenshot etc)

- **Copy of your data in connection with support/helpdesk**: to resolve a technical problem, we move a copy of a specific portion of your data to an encrypted test environment. Data from production to test environment are transported with encrypted backups, and also test environment have both transport and file encryption in place.
  Your permission is requested in advance for this. These data are only used to resolve the problem that has occurred and will be deleted from the test environment after the procedure.
- **After the end of the Agreement**: we provide the data in a general and accessible file format. Subsequently we keep the data on our servers for three months.

6. Support / Helpdesk / Consultants

To resolve an issue or carry out additional configuration, Wolters Kluwer needs access to the database of the Controller.

- The Controller can give the Processor's employee access to effacts by giving consent for a determinate purpose. For some systems, Controller can give access to effacts to Processor's employee by activating the Support Access option in the database. The Controller can switch off this option at all times.
- If access to the technical systems of the Controller is required, Processor will obtain access to the computer of the Controller via PC sharing. Activation by the Controller is required for remote access; this is done by entering a code provided by Processor or by a pop-up requiring your consent. The Controller is responsible for blocking/protecting all confidential information before granting access.

7. Security measures

In accordance with the GDPR regulations, Processor will take appropriate technical and organisational measures, to be assessed on the basis of the state of the art at the time the Service Agreement is concluded, and will evaluate these measures over time, taking into account the costs of implementation, nature, scope, context and objectives of processing, and the risk of differences in the degree of probability and seriousness for the rights and freedoms of natural persons.

DETAILED TECHNICAL AND ORGANISATIONAL MEASURES

7.1 Access control: buildings

Access to the buildings of Processor is controlled by both technical and organisational measures: access control with personalised badges, electronic locking of doors, reception procedures for visitors.

7.2 Access control: systems

As Processor, any access to networks, operational systems, user administration and applications requires the necessary authorisations: advanced password procedures, automatic timeout and blocking for incorrect passwords, individual accounts with histories, encryption, hardware and software firewalls.

The Controller must also ensure that adequate security measures for their passwords and other electronic access information are taken.

7.3 Access control: data

As Processor access to data by Processor itself is controlled by organisational measures: user administration and user accounts with specific access, personnel trained with regard to data processing and security, separation of the operational systems and the test environments, allocation of specific rights and maintaining histories of use, access and deletion.

7.4 Data encryption:

- Transport
  The HTTPS data transmission is encrypted with a 2048-bit PKI certificate and is certified by Norton.
- At rest
  We are encrypting databases on disks with a specific certificate / private key, using AES algorithm

7.5 Ability to guarantee ongoing confidentiality, integrity, availability and resilience of processing systems and services

Access control for personal data follows the guidelines for internal control, including the policy for access to information of the organisation, implementation of a user administration system and access rights, creation of awareness among employees on dealing with information and their passwords, network access control, including separation of sensitive networks, and control of access to the operating system and underlying applications. Specifically, the measures include:

- written/programmed authorisation structure;
- differentiated access rights (including for reading, modifying, deleting);
- definition of roles;
- logging/auditing.
- Personal data are segregated. The measures include:
- separation of functions (production/test data);
- segregation of highly sensitive data;
- purpose limitation/compartmentalisation;
- policy/measures to ensure separate storage, modification, deletion and transfer of data.

For the Controller, effacts requires the user to use a password to access the effacts system, which ensures the confidentiality of all data entered in the management system. effacts also offers the possibility of managing the user rights to segment the information accessible within the effacts system. The Controller is therefore required to establish confidentiality rules within the company.

7.6 Ability to restore the availability of and access to the Personal Data promptly in the event of a physical or technical incident

The availability of data is controlled by means of a permanent network monitoring system. To prevent data loss, a daily data backup with defined retention periods is conducted. Further measures include:

- backup procedures;
- overvoltage protection;
- physically separate storage of backup data carriers;
- mirroring of server hard drives (RAID);
- antivirus systems/SPAM filters/firewall/intrusion detection system/disaster recovery plan;
- fire/water protection systems (including fire extinguishing system, fire doors, smoke/fire detectors).

7.7 Process for regularly testing, assessing and evaluating the efficacy of technical and organisational measures to guarantee the security of the processing:

7.7.1 Monitoring

The effacts system is continuously monitored:

- In the framework of the 24/7 monitoring, both the health of the system and the performance of the application carefully monitored for each client individually.
- An independent external business conducts intrusion tests every year.
- Moreover, the intrusion detection system is always active and gives real-time warnings.
- The Kleos website is also certified.
- McAfee Security carefully monitors Kleos every day.
- Certifies that the website is secure, resistant to viruses and intrusion attempts, and protected from attacks of hackers on servers and data transmission.
- We are informed of any risks in real time, so that we can block attacks immediately.
- Norton Symantec continuously monitors our encrypted data transmission via the SSL certificate.
- A vulnerability scan takes place monthly and we receive the associated report.

7.7.2 Audits

Processor will make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this DPA and under Art. 28 GDPR, including the possibility to review the biannual audit reports on-site at the designated Processor office. The Controller is aware that any in-person on-site audits may significantly disturb the Processor’s business operations and may entail high expenditure in terms of cost and time.

7.8 Available certification

ISO/IEC 27001 certification

Productsheet Kleos

1. Nature of the Processing

Online management software for lawyers.

2. Categories of Personal Data that are processed

Wolters Kluwer will process the following categories of Personal Data exclusively in the context of this Addendum:

- Identity data (last name, first name, login name)
- Contact information (address, e-mail, IP address, telephone, fax)
- Behavioural data (user history)

As Controller you have the opportunity to enter additional personal information from your customers in Kleos. Basic fields which are provided in Kleos and may be filled in by you are:

- Identity data (name, address, mobile phone, e-mail, date of birth, etc.)
- Identity data issued by the government (national registration number, etc.)
- Social status (family situation, etc.)
- Financial information (bank account number, etc.)
- You can always add other additional personal data via the "additional fields" function.

3. Categories of data subjects involved in the Processing of personal data in Kleos

- Clients and partners of the Controller
- Shareholders, partners, employees and other staff members of the Controller, including trainees, research assistants, etc;
- Other persons whose data are processed by the Controller, such as counterparties.

4. Purposes of the processing

Wolters Kluwer stipulates that you can use Kleos for the purposes below:

- Central management of cases, contact data and documents
- Certified connection with the DPA, Digital Platform for Attorneys
- Kleos Connect: secure exchange of your files with your customers and other parties
- Accounting and invoicing: On the basis of the recorded services and costs you automatically draw up your statements of fees and invoices with Kleos, send reminders, make the VAT declaration and create client listings.
- Linking to your internal and external sources
- Extensive search and reporting possibilities
- Exporting information for reports

5. Retention period

As Controller, you yourself determine the retention period of your client information (dossiers, identity data, documents, etc.). Wolters Kluwer makes a backup of all client databases daily. This backup is kept for 30 days.

Personal data will be processed and kept for the following periods:

- **After migration of your data from another software package**: we keep no information after migration from the former software package. The Controller itself is responsible for copying/backup of this information and make it available to Wolters Kluwer if necessary
- **Personal data via support/helpdesk**: contacts are anonymised six months after the termination of the contract. As Controller you make sure not to transmit sensible data during the ticket resolution (screenshot etc)

- **Copy of your data in connection with support/helpdesk**: to resolve a technical problem, we move a copy of a specific portion of your data to an encrypted test environment. Data from production to test environment are transported with encrypted backups, and also test environment have both transport and file encryption in place.
  Your permission is requested in advance for this. These data are only used to resolve the problem that has occurred and will be deleted from the test environment after the procedure.
- **After the end of the Agreement**: we provide the data in a general and accessible file format. Subsequently we keep the data on our servers for three months.

6. Support / Helpdesk

To resolve an issue or carry out additional configuration, Wolters Kluwer needs access to the database of the Controller.

- The Controller can give the Wolters Kluwer employee access to Kleos by activating the Support User in the database. The Controller can switch off this option at all times.
- If access to the technical systems of the Contoller is required, Wolters Kluwer will obtain access to the computer of the Controller via PC sharing. Activation by the Controller is required for remote access; this is done by entering a code provided by Wolters Kluwer. The Controller is responsible for blocking/protecting all confidential information before granting access.

7. Security measures

In accordance with the GDPR regulations, Wolters Kluwer will take appropriate technical and organisational measures, to be assessed on the basis of the state of the art at the time the Service Provision Agreement is concluded, and will evaluate these measures over time, taking into account the costs of implementation, nature, scope, context and objectives of processing, and the risk of differences in the degree of probability and seriousness for the rights and freedoms of natural persons.

DETAILED TECHNICAL AND ORGANISATIONAL MEASURES

7.1 Access control: buildings

Access to the buildings of Wolters Kluwer is controlled by both technical and organisational measures: access control with personalised badges, electronic locking of doors, reception procedures for visitors.
The Controller must also ensure that adequate security measures and access to their buildings are taken.

7.2 Access control: systems

As processor access to networks, operational systems, user administration and applications Wolters Kluwer requires the necessary authorisations: advanced password procedures, automatic timeout and blocking for incorrect passwords, individual accounts with histories, encryption, hardware and software firewalls.

The Controller must also ensure that adequate security measures for their passwords and other electronic access information are taken

7.3 Access control: data

As Processor access to data by Wolters Kluwer itself is controlled by organisational measures: user administration and user accounts with specific access, personnel trained with regard to data processing and security, separation of the operational systems and the test environments, allocation of specific rights and maintaining histories of use, access and deletion.

7.4 Data encryption:

- Transport
  The HTTPS data transmission is encrypted with a 2048-bit PKI certificate and is certified by Norton.
- At rest
  We are encrypting databases on disks with a specific certificate / private key, using AES algorithm

7.5 Ability to guarantee ongoing confidentiality, integrity, availability and resilience of processing systems and services

Access control for personal data follows the guidelines for internal control, including the policy for access to information of the organisation, implementation of a user administration system and access rights, creation of awareness among employees on dealing with information and their passwords, network access control, including separation of sensitive networks, and control of access to the operating system and underlying applications. Specifically, the measures include:

- written/programmed authorisation structure;
- differentiated access rights (including for reading, modifying, deleting);
- definition of roles;
- logging/auditing.
- Personal data are segregated. The measures include:
- separation of functions (production/test data);
- segregation of highly sensitive data;
- purpose limitation/compartmentalisation;
- policy/measures to ensure separate storage, modification, deletion and transfer of data.

For the controller, Kleos requires the user to use a password to enter, which ensures the confidentiality of all data entered in the management system. Kleos also offers the possibility of managing the user rights to segment the information accessible within the data controller's office, if the Controller so wishes. The controller is therefore required to establish confidentiality rules within the firm.

7.6 Ability to restore the availability of and access to the Personal Data promptly in the event of a physical or technical incident

The availability of data is controlled by means of a permanent network monitoring system. To prevent data loss, a daily data backup with defined retention periods is conducted. Further measures include:

- backup procedures;
- overvoltage protection;
- physically separate storage of backup data carriers;
- mirroring of server hard drives (RAID);
- antivirus systems/SPAM filters/firewall/intrusion detection system/disaster recovery plan;
- fire/water protection systems (including fire extinguishing system, fire doors, smoke/fire detectors).

7.7 Process for regularly testing, assessing and evaluating the efficacy of technical and organisational measures to guarantee the security of the processing:

The Kleos system is continuously monitored:

- In the framework of the 24/7 monitoring, both the health of the system and the performance of the application carefully monitored for each client individually.
- An independent external business conducts intrusion tests every year.
- Moreover, the intrusion detection system is always active and gives real-time warnings.
- The Kleos website is also certified.
- McAfee Security carefully monitors Kleos every day.
- Certifies that the website is secure, resistant to viruses and intrusion attempts, and protected from attacks of hackers on servers and data transmission.
- We are informed of any risks in real time, so that we can block attacks immediately.
- Norton Symantec continuously monitors our encrypted data transmission via the SSL certificate.
- A vulnerability scan takes place monthly and we receive the associated report.

7.8 Available certification

ISO/IEC 27001 certification