Vereinbarung zur Auftragsverarbeitung

- Für Produkte und Leistungen des Geschäftsbereichs Legal Software -

zwischen

Wolters Kluwer Deutschland GmbH

Wolters-Kluwer-Straße 1
50354 Hürth

(im Folgenden: „WOLTERS KLUWER“)

und

Kundenname: _____

Straße und Hausnr.: _____

PLZ und Ort: _____

Kundennr.: _____

(im Folgenden: „Kunde“)

1. Auftragsverarbeitung

1.1 WOLTERS KLUWER erbringt für den Kunden Leistungen im Bereich Softwarenutzung und Support. Auf den entsprechenden, zwischen den Parteien geschlossenen Vertrag („Hauptvertrag“) wird Bezug genommen.

1.2 Im Rahmen der Leistungserbringung verarbeitet WOLTERS KLUWER Daten des Kunden, Mitarbeitern des Kunden sowie von Kunden des Kunden (“Kundendaten”). Umfang und Zweck der Datenverarbeitung durch WOLTERS KLUWER ergeben sich aus dem Hauptvertrag und – sofern Bestandteil des Hauptvertrages – aus den dazugehörigen Leistungsbeschreibungen. Bei Supportdienstleistungen (“Fernwartung”) besteht die Möglichkeit, dass WOLTERS KLUWER vom Kunden stammende personenbezogene Daten einsehen, auf diese zugreifen oder hiermit in Berührung kommen kann.

1.3 Diese Vereinbarung konkretisiert die beiderseitigen datenschutzrechtlichen Rechte und Pflichten in Bezug auf die Verarbeitung der Kundendaten durch WOLTERS KLUWER.

1.4 Diese Vereinbarung findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter von WOLTERS KLUWER oder beauftragte Unterauftragnehmer („Unterauftragsverarbeiter“) Kundendaten verarbeiten.

1.5 Die nachstehenden Vereinbarungen tragen dem Umstand Rechnung, dass es sich bei dem Kunden um einen Berufsgeheimnisträger im Sinne des § 203 StGB handelt und die Kundendaten einer gesetzlichen Geheimhaltungspflicht unterliegen und insbesondere vor unbefugter Offenbarung geschützt sind.

1.6 Die Dauer der Auftragsverarbeitung richtet sich nach dem Hauptvertrag.

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

2. Art der Datenverarbeitung, Art der Kundendaten und Kategorien betroffener Personen

2.1 Art Datenverarbeitung

Die Art der Verarbeitung ist abhängig von der Leistung, die WOLTERS KLUWER für den Kunden auf der Grundlage des Hauptvertrages erbringt. Umfasst können folgende Arten einer Datenverarbeitung sein:

Erheben, erfassen, organisieren, ordnen, speichern, online-speichern und zum Abruf durch den Kunden bereithalten, anpassen, verändern, auslesen, abfragen, analysieren, offenlegen durch Übermittlung, abgleichen, verknüpfen, einschränken, berichtigen, löschen oder vernichten, sichern von Kundendaten.

2.2 Art der verarbeiteten Daten

Im Rahmen der Erbringung der Leistungen für den Auftraggeber erhält WOLTERS KLUWER Zugriff auf die in **Anlage 1** näher spezifizierten Kundendaten.

2.3 Kategorien betroffener Personen

Der Kreis der von der Datenverarbeitung Betroffenen ist in **Anlage 1** beschrieben.

3. Pflichten von WOLTERS KLUWER

3.1 WOLTERS KLUWER verarbeitet Kundendaten 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.

3.2 WOLTERS KLUWER verpflichtet sich dazu und kontrolliert regelmäßig, dass die Verarbeitung der im Auftrag verarbeiteten Kundendaten in seinem Verantwortungsbereich in Übereinstimmung mit den jeweils geltenden datenschutzrechtlichen Bestimmungen und dieser Vereinbarung, einschließlich der technisch-organisatorischen Maßnahmen nach Ziffer 4 sowie in Übereinstimmung mit den Weisungen des Kunden erfolgt. WOLTERS KLUWER hat seine Kontrollen zu dokumentieren und dem Kunden die Dokumentationen auf Verlangen vorzulegen.

3.3 WOLTERS KLUWER bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind und beachtet diese.

3.4 WOLTERS KLUWER ist verpflichtet, die mit der Verarbeitung von Kundendaten befassten Beschäftigten sowie die von WOLTERS KLUWER insoweit beauftragten Unterauftragsverarbeiter auf die Pflicht zur Verschwiegenheit nach § 203 StGB zu verpflichten. Auf Wunsch wird WOLTERS KLUWER dem Kunden Kopien der vorgenommenen Verschwiegenheitsverpflichtungen zur Verfügung stellen. Es dürfen nur zur Verschwiegenheit verpflichtete Mitarbeiter von WOLTERS KLUWER und Mitarbeiter der von WOLTERS KLUWER beauftragten Unterauftragsverarbeiter im Rahmen der Auftragsverarbeitung der Kundendaten tätig werden, es sei denn, diese sind aufgrund Gesetz und/oder berufsrechtlicher Vorgabe selbst gemäß § 203 StGB zur Verschwiegenheit verpflichtet.

3.5 WOLTERS KLUWER ist dafür verantwortlich, dass die 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.

3.6 Im Zusammenhang mit der beauftragten Verarbeitung hat WOLTERS KLUWER den Kunden 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 in geeigneter Weise mitzuteilen.

3.7 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.

3.8 Ist der Kunde ein **Berufsgeheimnisträger** im Sinne von § 203 StGB und tritt eine Aufsichtsbehörde an WOLTERS KLUWER mit der Aufforderung heran, Informationen zur Verarbeitung personenbezogener Daten im Zusammenhang mit dieser Vereinbarung zu erteilen oder Zugang zu solchen Daten und Informationen zu gewähren und würde diese Inanspruchnahme von WOLTERS KLUWER einen Verstoß gegen Geheimhaltungspflichten für den Kunden bedeuten, ist WOLTERS KLUWER verpflichtet, diese Aufforderung unter Verweis auf § 29 Abs. 3 BDSG abzulehnen. WOLTERS KLUWER wird den Kunden unverzüglich über eine solche Aufforderung informieren, sofern nicht gesetzliche Bestimmungen eine solche Information untersagen. Das weitere Vorgehen gegenüber der Aufsichtsbehörde stimmen der Kunde und WOLTERS KLUWER gemeinsam ab.

3.9 Für die Wahrung der Rechte betroffener Personen ist alleine der Kunde verantwortlich. Auskünfte an Dritte oder Betroffene 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. Unabhängig davon wird WOLTERS KLUWER den Kunden bei seiner Pflicht zur Beantwortung von Anträgen auf

Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person im erforderlichen Umfang unterstützen, sofern die betroffene Person entsprechende Rechte geltend macht.

3.10 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 in **Anlage 3** dokumentiert oder können unter https://www.wolterskluwer.de/datenschutz eingesehen werden. In Zweifelsfällen kann sich der Kunde direkt an den Datenschutzbeauftragten wenden. WOLTERS KLUWER ist verpflichtet, die Bestellung eines Datenschutzbeauftragten während der Dauer dieses Vertrages aufrechtzuerhalten.

4. Technische und organisatorische Maßnahmen

4.1 Die in **Anlage 2** beschriebenen technischen und organisatorischen Maßnahmen gelten hinsichtlich der Räumlichkeiten und der von den Mitarbeitern genutzten IT-Infrastruktur von WOLTERS KLUWER.

Technische und organisatorische Maßnahmen, die für die Verarbeitung von personenbezogenen Daten bei der Nutzung von Produkten und der Erbringung von Leistungen implementiert sind, werden in den **Leistungsbeschreibungen der Produkte und Leistungen** vereinbart.

4.2 Die technischen und organisatorischen Maßnahmen können der technologischen Weiterentwicklung entsprechend angepasst werden, solange das vereinbarte Niveau nicht unterschritten wird.

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

4.4 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.

4.5 WOLTERS KLUWER führt den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen.

5. Regelungen zur Berichtigung, Löschung und Sperrung von Daten

5.1 Im Rahmen des Auftrags verarbeitete Daten wird WOLTERS KLUWER nur entsprechend dieser Vereinbarung oder nach Weisung des Kunden berichtigen, löschen oder sperren.

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

6. Mitteilungspflichten

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

6.2 Ebenfalls unverzüglich mitzuteilen sind Verstöße von WOLTERS KLUWER oder der bei ihr beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in dieser Vereinbarung getroffenen Festlegungen.

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

6.4 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.

7. Unterauftragsverhältnisse

7.1 Die von WOLTERS KLUWER zur Datenverarbeitung eingesetzten Unterauftragsverarbeiter werden in der entsprechenden **Leistungsbeschreibung** für ein Produkt und/oder eine Leistung vereinbart.

7.2 WOLTERS KLUWER informiert den Kunden rechtzeitig vorab über die Beauftragung von weiteren oder der Ersetzung der aufgeführten Unterauftragsverarbeiter (Textform ist ausreichend). Der Kunde kann bei Vorliegen eines wichtigen Grundes der Unterbeauftragung innerhalb von zwei Wochen nach Zugang der Information widersprechen (Textform ist ausreichend). Ein wichtiger Grund liegt insbesondere vor, wenn ein begründeter Anlass zu Zweifeln über die datenschutzkonforme Leistungserbringung durch den betreffenden Unterauftragsverarbeiter besteht. Im Fall eines fristgemäßen und begründeten Einspruchs können beide Parteien diese Vereinbarung und den Hauptvertrag außerordentlich kündigen.

7.3 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.

7.4 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.

7.5 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 Unterauftragsverarbeitern. WOLTERS KLUWER haftet für ein Verschulden seiner Unterauftragsverarbeiter wie für eigenes Verschulden.

7.6 WOLTERS KLUWER hat die Einhaltung der Pflichten des Unterauftragsverarbeiter regelmäßig angemessen zu überprüfen. Die Prüfung und ihr Ergebnis sind zu dokumentieren.

7.7 WOLTERS KLUWER hat auch die Pflicht, zu überprüfen, dass die Mitarbeiter des Unterauftragsverarbeiters vor Beginn der Verarbeitung entsprechend Ziffer 3.4 verpflichtet worden sind.

8. Rechte und Pflichten des Kunden

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

8.2 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.

8.3 Kontrollen bei WOLTERS KLUWER haben ohne vermeidbare Störungen des 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.

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

9. Weisungen

9.1 Die beim Kunden zur Erteilung von Weisungen befugten Personen und die bei WOLTERS KLUWER zur Entgegennahme von Weisungen befugten Personen sind in **Anlage 3** benannt.

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

9.3 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.

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

10. Beendigung des Auftrags

10.1 Bei Beendigung des Hauptvertrages oder jederzeit auf Verlangen des Kunden hat WOLTERS KLUWER die im Auftrag verarbeiteten Kundendaten 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 Kundendaten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist.

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

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

10.4 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.

11. Haftung

Die Haftung für schuldhafte Verletzungen dieses Vertrags bestimmt sich nach den gesetzlichen Bestimmungen. Etwaige an anderer Stelle vereinbarte Haftungsbegrenzungen gelten nicht für diese Vereinbarung.

12. Sonstiges

12.1 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 hinaus 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.

12.2 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.

12.3 Im Falle von Widersprüchen zwischen dieser Vereinbarung und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieser Vereinbarung vor, soweit die betreffende Regelung dieser Vereinbarung die Verarbeitung von personenbezogenen Daten betrifft.

12.4 Für Nebenabreden ist die Schriftform erforderlich.

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

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

(Stand: August 2020)

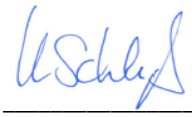
Unterschrift WOLTERS KLUWER

Hürth, den

_____

Ralph Vonderstein
Geschäftsführer
Leiter Geschäftsbereich Legal Software

Hürth, den



_____

Kristina Schleß
Rechtsanwältin
Director Legal, Assistant General Counsel

Unterschrift des Kunden

_____, den _____

_____

Anlage 1 – Art der personenbezogenen Daten, Betroffene, Zweck (Ziff 2.2 und 2.3 der AVV)

1. Art der Kundendaten, Kategorien betroffener Personen

1.1 Art der Kundendaten, die WOLTER KLUWER verarbeitet

Verarbeitet werden personenbezogenen Daten, die der Kunde von seinen Kunden* in dem Produkt gespeichert hat bzw. Gegenstand der vom Kunden beauftragten Migration sind.

Umfasst können folgende Arten von Daten sein:

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

*Kunden können - abhängig vom Einsatzbereich – Mandanten, Patienten, Versicherungsnehmer u.a. sein

Bei der Erbringung von Supportdienstleistungen werden folgende Daten der Mitarbeiter des Kunden verarbeitet:

- Vorname, Nachname
- E-Mail-Adresse
- Ort der Tätigkeit
- Ggf. Beruf/Funktion

1.2 Kreis der von der Auftragsverarbeitung betroffenen Personen

Betroffen sind Personen deren Daten der Kunde innerhalb des Produkts verarbeitet. Dies können sein:

- Kunden und sonstige Vertragspartner des Kunden
- Gesellschafter, Angestellte und sonstige Mitarbeiter des Kunden, einschließlich zu Ausbildungszwecken tätige Personen, Praktikanten und Hilfskräfte
- Sonstige Personen, von denen der Kunde Daten in dem Produkt gespeichert hat (z.B. Vertragsparteien, Kontaktpersonen, unmittelbar oder mittelbar an einem Fall beteiligte Parteien)

2. Zweck der Verarbeitungen

2.1 **Durchführung von Supportdienstleistungen** (On-Premises und Cloud Produkte)

- Unterstützung des Kunden bei Fragen im Zusammenhang mit der Anwendung der Produkte
- Lösung/Behebung der von dem Kunden gemeldeten Probleme und Störfälle und/oder Weiterleitung der Meldung an den 2nd-Level-Support

2.2 **Migration von Daten** (On-Premises und Cloud Produkte)

- Übertragung von Daten von der Anwendung eines Drittanbieters in eine Anwendung von WOLTERS KLUWER
- Übertragung von Daten in eine neue Version einer Anwendung von WOLTERS KLUWER („Upgrade-Migration“)

2.3 **Hosting des Produkts** (nur Cloud Produkte)

- Bereitstellung von Daten, Funktionalitäten und Anwendungen auf einer externen IT-Infrastruktur („Cloud“), um dem Kunden den Zugriff auf und die Nutzung von Daten mittels eines Browsers bzw. über eine mobile Applikation zu ermöglichen

Anlage 2 – Technische und organisatorische Maßnahmen

-Gebäude/Geschäftsräume, Standort-IT, Rechenzentrum-

Sofern die Wolters Kluwer Deutschland GmbH (nachstehend „WOLTERS KLUWER“) im Zusammenhang mit der Erbringung Ihrer Leistungen personenbezogene Daten verarbeitet, sind die nachstehend beschriebenen technischen und organisatorischen Maßnahmen („TOM“) implementiert.

Eine Beschreibung der technischen und organisatorischen Maßnahmen, die für die Verarbeitung von personenbezogenen Daten

- in dem von dem Kunden genutzten **Produkt** und/oder
- im Rahmen der Erbringung von **Leistungen** für den Kunden (z.B. Fernwartung, Datenmigration)

implementiert sind, finden Sie in der entsprechenden **Leistungsbeschreibung** des Produkts und der Leistung.

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

1. Zutrittskontrolle

WOLTERS KLUWER ergreift angemessene Maßnahmen, um den Zugang unautorisierter Personen zu personenbezogenen Daten zu verhindern.

An den jeweiligen Standorten von WOLTERS KLUWER sind die im **Anhang A** jeweils aufgeführten Zutrittskontrollen für die Gebäude / Geschäftsräume eingerichtet.

1.2 Rechenzentrum

Die DV-Anlagen befinden sich in Räumen oder Rechenzentren 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 dann per Magnet- bzw. Chipkarte mit Zahlencode oder Sicherheitsschlüssel (Raumzugang) und Schließanlage (Rack Zugang). Diese Bereiche unterliegen einer Videoüberwachung (Art. 32 DSGVO), sowie erweiterten Maßnahmen zum Einbruchsschutz.

Mitarbeiter von WOLTERS KLUWER erhalten nach denselben Regeln Zutritt zu den Rechenzentren. IT-Verantwortliche des Auftragnehmers haben eine permanente Zutrittsberechtigung für die Rechenzentren. Die Zutrittskontrolle der Mitarbeiter zu den DV- Anlagen in den Arbeitsräumen des Auftragnehmers 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 der WOLTERS KLUWER autorisiert und erfolgt nur in Begleitung von Support-Personal des Auftragnehmers. 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, Servern 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 der 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 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 und bei Prüfungen durch Kunden/Auftraggeber 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.

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 personenbezogenen Daten 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.

WLAN Nutzung von Besuchern: Anmeldungen an das W-LAN sind für nicht durch WOLTERS KLUWER verwaltete Geräte nur mit Zugangscode (Voucher) möglich. Die Gültigkeit des Zugangs ist zeitlich auf einen Tag begrenzt.

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 von WOLTERS KLUWER innerhalb und außerhalb Deutschlands als auch für Dienstleister sowie in einigen Fällen auch Verbindungen zu Kunden/Auftraggebern.

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 Rechenzentrum haben keine Möglichkeit, Daten in die dort gehosteten Applikationen und Datenverarbeitungssysteme einzugeben. Sie haben insbesondere keine Möglichkeit, personenbezogene Daten von Betroffenen 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

Die Mitarbeiter des von WOLTERS KLUWER beauftragten Rechenzentrum haben keine Möglichkeit, Daten in die dort gehosteten Applikationen und Datenverarbeitungssysteme einzugeben. Sie haben insbesondere keine Möglichkeit, personenbezogene Daten von Betroffenen 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 Daten 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 der WOLTERS KLUWER, sowie der Rechenzentrumsbetreiber.

WOLTERS KLUWER hält darüber hinaus einen Notfallplan zur Wiederherstellung der Umgebung bereit. Abhängigkeiten und Prioritäten der Dienste sind mitdokumentiert, 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 von Kunden aufgrund der von den 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 regelmäßig 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.

Anhang A
Zutrittskontrolle an den Standorten von WOLTERS KLUWER

1. Standort Hürth

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

2. Standort Köln

- Gebäude ist durch Videoüberwachung (5 Kameras) 24h gesichert.
  - Montags - Freitag 00:00 – 24.00 Uhr
  - Wochenende und Feiertage 00:00 – 24:00 Uhr
- Besetzung Empfang durch Sicherheitsdienst:
  - Montags - Freitag 07:00 – 17:00 Uhr

- Zutritt zu den Gebäuden über Chip und Schlüssel möglich
- Chip (MTZ System) nur für Mitarbeiter und Sicherheitsdienst
- Chip ist zeitlich begrenzt (7.00 -20.00), Aufhebung der Begrenzung über Antrag mit Zustimmung des Vorgesetzten möglich.
- Schlüssel nur für spezielle Mitarbeiter nach Schlüsselliste erfasst.
- Besucherregelung: Gäste melden sich am Empfang an, bekommen einen Besucherausweis und werden von dem Mitarbeiter abgeholt.
- Alarmanlage keine vorhanden.
- Brandmeldeanlage nicht vorhanden.

3. Standort Neuwied

- Gebäude ist durch Videoüberwachung (2 Kameras) außerhalb der Arbeitszeiten gesichert.
  - Montags - Freitag 19.00 – 7.00 Uhr
  - Wochenende und Feiertage 00:00 – 24:00 Uhr
- Zutritt zu den Gebäuden über Chip und Schlüssel möglich
- Chip (MTZ System) nur für Mitarbeiter und Reinigungsfirma
- Chip ist zeitlich begrenzt (6.00 -20.00), Aufhebung der Begrenzung über Antrag mit Zustimmung des Vorgesetzten möglich.
- Schlüssel nur für spezielle Mitarbeiter nach Schlüsselliste erfasst.
- Besucherregelung: Gäste werden an der Haustür abgeholt- melden sich über Klingelanlage an.
- Alarmanlage für Rechenzentrum (für Sabotage, Feuer und Wassereinbruch) vorhanden.
- Brandmeldeanlage vorhanden mit akustischer Alarmierung und Aufschaltung auf die Alarmzentrale.

Anlage 3 – Befugte Personen zur Erteilung und Entgegennahme von Weisungen, Datenschutzbeauftragter von WOLTERS KLUWER

Folgende Personen sind zur Erteilung und Entgegennahme von Weisungen befugt:

I. Weisungsbefugte Person(en) beim Kunden (vom Kunden auszufüllen)

Name: _____

Anschrift: _____

E-Mail: _____

Name: _____

Anschrift: _____

E-Mail: _____

II. Entgegennahme von Weisungen bei WOLTERS KLUWER

Name: Ralph Vonderstein

Anschrift: Wolters-Kluwer-Straße 1, 50354 Hürth

E-Mail: ralph.vonderstein@wolterskluwer.com

Name: Maria Pia Critelli

Anschrift: Wolters-Kluwer-Straße 1, 50354 Hürth

E-Mail: maria.critelli@wolterskluwer.com

III. Datenschutzbeauftragter bei WOLTERS KLUWER

TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD
IT Security, Business Security & Privacy
Langemarckstraße 20
45141 Essen

Telefon: 0201 - 8999-899
E-Mail: dsb@wolterskluwer.com