Bestätigung zum Vertrag zur Verarbeitung im Auftrag nach Art. 28 Abs. 3 DSGVO	
Kundennummer	**E-Mail-Adresse**
ghjhjghjghjghj	
Vorname	**Nachname**
Firma	**Adresse**
PLZ	**Ort**
IP-Adresse	**Zeitstempel**

Vereinbarung zur Verarbeitung im Auftrag

- gemäß Art. 28 DSGVO -

(im Folgenden „AVV“)

zwischen

Wolters Kluwer Tax & Accounting Deutschland GmbH

Kammererstraße 39

71636 Ludwigsburg

(im Folgenden: „WOLTERS KLUWER oder Auftragsverarbeiter“)

und

(im Folgenden: „**Kunde**“)

Dieser Auftragsverarbeitungsvertrag ("AVV") und dessen Anlagen sind integraler Bestandteil des zwischen dem Kunden und dem Auftragsverarbeiter geschlossenen Vertrages. Es gelten die Bestimmungen der AGB und der Leistungsbeschreibungen, soweit sie nicht durch diese AVV geändert werden.

1. Definitionen

Für die Zwecke dieser AVV bedeuten

Anwendbares Datenschutzrecht	bezeichnet die auf die Parteien anwendbaren Gesetze und Vorschriften über personenbezogene Daten (einschließlich der DSGVO);
Verantwortlicher	Ist der Kunde, der als natürliche oder juristische Person allein oder gemeinsam mit anderen über die Rechtmäßigkeit, Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet;
Datenschutzgrundverordnung oder "DSGVO"	bezeichnet die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr;
Internationale Organisation:	eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde;
Mitgliedstaat:	ein Land, das der Europäischen Union angehört;
Personenbezogene Daten	sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („Betroffene Person“) beziehen;
Betroffene Person	ist eine identifizierbare Person, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;
Datenschutzverletzung	ist eine Verletzung der Sicherheit, die zur unbeabsichtigten oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung oder zum Zugang auf übermittelte, gespeicherte oder anderweitig verarbeitete personenbezogene Daten führt;
Verarbeitung	Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;
Auftragsverarbeiter	Auftragsverarbeiter ist Wolters Kluwer, der personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;
Unterauftragsverarbeiter	bezeichnet jeden Auftragsverarbeiter als natürliche oder juristische Person, die vom Auftragsverarbeiter beauftragt wird und sich bereit erklärt, vom Auftragsverarbeiter personenbezogene Daten zu erhalten, die für Verarbeitungstätigkeiten bestimmt sind, die im Auftrag des Verantwortlichen gemäß dessen Anweisungen und den Bestimmungen eines schriftlichen Vertrags mit dem Auftragsverarbeiter durchgeführt werden sollen;
Aufsichtsbehörde	ist eine unabhängige öffentliche Stelle, die von einem Mitgliedstaat gemäß Artikel 51 DSGVO eingerichtet wurde;
Technische und organisatorische Maßnahmen	sind diejenigen geeigneten Maßnahmen, die darauf abzielen, personenbezogene Daten vor Datenschutzverletzungen zu schützen, um ein dem Risiko angemessenes Maß an Sicherheit zu gewährleisten;

2. Gegenstand und Einzelheiten der Verarbeitung

Dieser AVV legt die Bedingungen fest, auf Basis derer der Auftragsverarbeiter, die im Rahmen des zwischen ihm und dem Verantwortlichen geschlossenen Vertrags festgelegten und erforderlichen Verarbeitungen von personenbezogenen Daten im Auftrag des Verantwortlichen durchführt.
Der Verantwortliche ist der einzige Ansprechpartner des Auftragsverarbeiters: Sollten eventuell weitere für die Verarbeitung Verantwortliche Rechte gegenüber dem Auftragsverarbeiter haben (im Falle einer gesamtschuldnerischen Haftung), übt der Verantwortliche diese Rechte im Namen der anderen Verantwortlichen aus und gewährleistet, alle erforderlichen Genehmigungen von ihnen eingeholt zu haben. Der Auftragsverarbeiter ist von seinen Informations- und Meldepflichten gegenüber einem anderen für die Verarbeitung Verantwortlichen entbunden, sobald der Auftragsverarbeiter seine Verpflichtungen gegenüber dem Verantwortlichen erfüllt hat.
Die Verarbeitungsvorgänge (Kategorien personenbezogener Daten, Art der betroffenen Personen usw.) und die technischen und organisatorischen Maßnahmen im Zusammenhang mit den im Rahmen des Vertrags erbrachten Leistungen sind in den beigefügten Anlagen beschrieben, die im Zuge der Weiterentwicklung der Leistungen aktualisiert werden können. Zwischen den Vertragsparteien gilt die jeweils aktuelle Fassung der Anlage.

3. Pflichten des Verantwortlichen

3.1 Der Kunde ist und bleibt für die Dauer des Vertrags der für die Verarbeitung Verantwortliche und muss dem Auftragsverarbeiter dokumentierte Weisungen in Bezug auf die Verarbeitung erteilen. Diese Weisungen sind insbesondere in dem Vertrag, diesem AVV und den beigefügten Leistungsbeschreibungen enthalten.
Der Kunde kann dem Auftragsverarbeiter zusätzliche angemessene Weisungen erteilen. Erfordert die Ausführung einer zusätzlichen Weisung die Durchführung von auf den Verantwortlichen zugeschnittenen technischen und organisatorischen Sicherheitsmaßnahmen, die nach dem anwendbaren Datenschutzrecht nicht erforderlich sind, und entstehen dadurch zusätzliche Kosten, so wird der Auftragsverarbeiter den

Verantwortlichen über diese Kosten informieren. Der Auftragsverarbeiter wird den Anweisungen erst nach Erhalt einer schriftlichen Bestätigung des für die Verarbeitung Verantwortlichen, dass dieser die zusätzlichen Kosten übernimmt, nachkommen. Die Weisungen des Verantwortlichen werden dem Auftragsverarbeiter in schriftlicher Form (E-Mail ausreichend) übermittelt. Die Weisungen werden grundsätzlich schriftlich (per E-Mail) erteilt, es sei denn, ein Notfall oder andere besondere Umstände erfordern eine mündliche Mitteilung. Nicht schriftlich erteilte Weisungen müssen so schnell wie möglich, spätestens jedoch vierundzwanzig (24) Stunden nach Erteilung, vom Verantwortlichem schriftlich bestätigt werden. Wenn der Verantwortliche nicht in dem Land ansässig ist, in dem der Auftragsverarbeiter seinen Sitz hat, muss der Verantwortliche den Auftragsverarbeiter über die spezifischen Verpflichtungen informieren, die nach den für den Verantwortlichen geltenden lokalen Gesetzen zwingend vorgeschrieben sind, damit die Parteien eventuell erforderliche Maßnahmen festlegen können.

3.2 Der Verantwortliche ist verpflichtet, die betroffenen Personen über die Verarbeitungsvorgänge zu informieren. Der Verantwortliche ist dafür verantwortlich, die Anfragen der betroffenen Personen auf Ausübung ihrer Rechte zu beantworten. Ist es dem Verantwortlichen nicht möglich, die Informationen und Daten, die für die Bearbeitung der Anfrage einer betroffenen Person auf Ausübung ihrer Rechte erforderlich sind, direkt zu beschaffen, fordert der Verantwortliche alle erforderlichen Informationen und Daten beim Auftragsverarbeiter an, der den Verantwortlichen so weit wie möglich bei der Erfüllung seiner Verpflichtung, den Anfragen auf Ausübung der Rechte der betroffenen Person nachzukommen, unterstützt.

4. Verpflichtungen des Auftragsverarbeiters

4.1 Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten im Auftrag des Verantwortlichen nur gemäß den dokumentierten Weisungen des Verantwortlichen, es sei denn, er ist nach dem Recht der Europäischen Union oder dem Recht eines Mitgliedstaats dazu verpflichtet. Diese Verpflichtung zur Befolgung der Weisungen des für die Verarbeitung Verantwortlichen gilt auch für die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation.
Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn eine Weisung seiner Ansicht nach einen Verstoß gegen das geltende Datenschutzrecht darstellt. In einem solchen Fall kann der Auftragsverarbeiter die Erbringung der vertraglichen Leistungen aussetzen und ist nicht verpflichtet, die betreffende Weisung zu befolgen, bis die Weisung des Kunden so weit geklärt ist, dass sie nicht mehr gegen das geltende Datenschutzrecht verstößt. Der Auftragsverarbeiter wird den Verantwortlichen auch informieren, wenn er aus irgendeinem Grund nicht in der Lage ist, einer Weisung des Verantwortlichen nachzukommen.
4.2 Der Auftragsverarbeiter stellt sicher, dass die von ihm zur Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen ermächtigten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verpflichtung zur Vertraulichkeit unterliegen und dass diese Personen, die Zugang zu den personenbezogenen Daten haben, diese personenbezogenen Daten gemäß den Weisungen des Verantwortlichen verarbeiten. Verarbeitet ein Unterauftragsverarbeiter Kundendaten, so gelten darüber hinaus die Bestimmungen von Abschnitt 5.
4.3 Der Auftragsverarbeiter hat die technischen und organisatorischen Maßnahmen im Rahmen seiner Verantwortung umzusetzen, wobei er die Art der Verarbeitung, den Stand der Technik und die Kosten der Umsetzung sowie das Risiko für die betroffenen Personen berücksichtigt. Diese technischen und organisatorischen Maßnahmen können sich, insbesondere aufgrund des technischen Fortschritts, ändern. Der Auftragsverarbeiter behält sich das Recht vor, die technischen und organisatorischen Maßnahmen zu ändern, sofern der Betrieb und die Sicherheit, der im Rahmen des Vertrags erbrachten Dienstleistungen, nicht beeinträchtigt und das vereinbarte Schutzniveau nicht unterschritten werden. Der Verantwortliche bestätigt, dass die technischen und organisatorischen Maßnahmen ein angemessenes Schutzniveau für seine personenbezogenen Daten bieten.
4.4 Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten und ist insbesondere verpflichtet:
(a) ein schriftliches Verzeichnis der Kategorien von Verarbeitungstätigkeiten, die im Auftrag des Verantwortlichen durchgeführt werden, zu führen, wenn diese Verpflichtung gemäß Artikel 30 DSGVO anwendbar ist;
(b) Zur Unterrichtung des Verantwortlichen:
i. über jedes rechtsverbindliche Ersuchen einer Strafverfolgungsbehörde um Offenlegung der personenbezogenen Daten, sofern dies nicht anderweitig untersagt ist, wie z. B. ein strafrechtliches Verbot zur Wahrung der Vertraulichkeit einer strafrechtlichen Untersuchung;
ii. über alle Beschwerden und Anfragen, die direkt von betroffenen Personen eingehen (z. B. in Bezug auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit, Widerspruch gegen die Verarbeitung von Daten, automatisierte Entscheidungsfindung), ohne dass der Auftragsverarbeiter auf diese Anfragen antwortet, es sei denn, er wurde anderweitig dazu ermächtigt;
iii. wenn der Auftragsverarbeiter nach dem Recht der Europäischen Union (EU) oder der Mitgliedstaaten, dem er unterliegt, verpflichtet ist, die personenbezogenen Daten über die Weisungen des Verantwortlichen hinaus zu verarbeiten, bevor er eine solche vornimmt, es sei denn, dass das Recht der EU oder der Mitgliedstaaten eine solche Unterrichtung aus wichtigen Gründen des öffentlichen Interesses verbietet; in einer solchen Meldung ist die rechtliche Anforderung nach dem Recht der EU oder der Mitgliedstaaten anzugeben;
(c) den für die Verarbeitung Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen bei allen Datenschutz-Folgenabschätzungen gemäß Artikel 35 der DSGVO und/oder bei allen vorherigen Konsultationen gemäß Artikel 36 der DSGVO unterstützen, die sich auf die vom Auftragsverarbeiter für den Verantwortlichen erbrachten Leistungen und die vom Auftragsverarbeiter im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten beziehen;
(d) auf Verlangen des Verantwortlichen oder in dem Umfang, in dem der Auftragsverarbeiter nach dem anwendbaren Datenschutzrecht dazu verpflichtet ist, die im Rahmen dieses AVV verarbeiteten personenbezogenen Daten zu berichtigen oder zu löschen.

4.5 Der Auftragsverarbeiter benachrichtigt den Verantwortlichen unverzüglich, nachdem er von einer Verletzung des Datenschutzes bei dem Auftragsverarbeiter Kenntnis erlangt hat. Diese Meldung wird vom Auftragsverarbeiter an die vom Verantwortlichen in dem Vertrag angegebene Kontaktstelle (oder, falls keine angegeben ist, an den Unterzeichner der Vereinbarung) gesandt und enthält alle dem Auftragsverarbeiter gemäß Artikel 33 der DSGVO zur Verfügung stehenden Informationen, um die Datenschutzverletzung zu dokumentieren.

5. Unterauftragsverarbeiter

5.1 Der Verantwortliche berechtigt den Auftragsverarbeiter Unterauftragsverarbeiter mit der Erbringung der vereinbarten Leistungen zu beauftragen. Die Unterauftragsverarbeiter, die in der dieser AVV beigefügten Liste aufgeführt sind, werden von dem

Verantwortlichen akzeptiert. Die Unterauftragsverarbeiter unterstehen der Verantwortung des Auftragsverarbeiters und stehen ausschließlich mit dem Auftragsverarbeiter in einer vertraglichen Beziehung. Der Auftragsverarbeiter bleibt gegenüber dem Verantwortlichen für die Nichterfüllung der Pflichten eines Unterauftragsverarbeiters haftbar.

5.2 Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Änderung hinsichtlich der Hinzuziehung oder des Austauschs eines Unterauftragsverarbeiters unter Angabe der Identität des vorgesehenen Unterauftragsverarbeiters und der Verarbeitungstätigkeiten, die ausgeführt werden sollen. Der Verantwortliche kann innerhalb von vierzehn (14) Tagen nach der Benachrichtigung Einspruch erheben. Erhebt der Verantwortliche innerhalb dieser Frist einen begründeten Einspruch, so bemüht sich der Auftragsverarbeiter in angemessener Weise, Änderungen an den vereinbarten Leistungen vorzunehmen, um die Verarbeitung personenbezogener Daten durch den beanstandeten neuen oder zusätzlichen Unterauftragsverarbeiter zu vermeiden. Sollte dies nicht möglich sein, kann der Verantwortliche (i) seine Zustimmung zur Wahl des zuvor beanstandeten Unterauftragsverarbeiters bestätigen oder (ii) den Vertrag ganz oder teilweise mit einer Frist von mindestens drei (3) Monaten schriftlich gegenüber dem Auftragsverarbeiter kündigen, ohne dass diese Kündigung zu einer Entschädigung des Kunden führt.

5.3 Der Auftragsverarbeiter schließt mit allen Unterauftragsverarbeitern einen Vertrag, der dem Unterauftragsverarbeiter die festgelegten Verpflichtungen zum Schutz personenbezogener Daten auferlegt, und stellt sicher, dass er ausreichende Garantien für die Anwendung der technischen und organisatorischen Maßnahmen bietet, die für die vom Unterauftragsverarbeiter erbrachten Dienstleistungen relevant sind.

5.4 Darüber hinaus dürfen Unterauftragsverarbeiter in Drittländern nur beauftragt werden, wenn die besonderen Anforderungen der Artikel 44 ff. der DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltenskodizes). Dies kann dazu führen, dass der Auftragsverarbeiter und der Unterauftragsverarbeiter weitere Maßnahmen ergreifen müssen, um den Schutz der personenbezogenen Daten der für die Verarbeitung Verantwortlichen zu gewährleisten.

6. Inspektionen und Audits

Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der in diesem AVV vorgesehenen Verpflichtungen nachzuweisen. Zusätzliche Informationen (soweit sie nicht für den Auftragsverarbeiter vertraulich sind oder unter das Geschäftsgeheimnis fallen) werden dem Verantwortlichen auf schriftliche Anfrage (E-Mail ausreichend) zur Verfügung gestellt. Sollten die oben genannten Informationen nicht ausreichen, um dem Verantwortlichen nachzuweisen, dass der Auftragsverarbeiter seinen Verpflichtungen nachkommt, können sich die Parteien auf die Bedingungen einer zusätzlichen Inspektion einigen. Der für die Verarbeitung Verantwortliche ist sich bewusst, dass persönliche Vor-Ort-Prüfungen den Geschäftsbetrieb des Auftragsverarbeiters stören und einen hohen Kosten- und Zeitaufwand mit sich bringen können. Ferner weist der Verantwortliche den Auftragsverarbeiter an, die Kontrollen und Prüfungen bei den Unterauftragsverarbeitern selbst durchzuführen, und der Auftragsverarbeiter stellt dem für die Verarbeitung Verantwortlichen die Informationen über die Unterauftragsverarbeiter zur Verfügung, die erforderlich sind, um die Einhaltung der hier und in Artikel 28 DSGVO genannten Verpflichtungen nachzuweisen. Der Verantwortliche kann in diesem Zusammenhang dem Auftragsverarbeiter schriftlich alle aus seiner Sicht erforderlichen Fragen und Anfragen stellen.
Darüber hinaus verpflichten sich die Parteien, im Falle einer Kontrolle durch eine Aufsichtsbehörde miteinander und mit der Aufsichtsbehörde zusammenzuarbeiten und sich gegenseitig die erforderlichen Informationen zu übermitteln.

7. Auswirkungen der Beendigung

Bei Beendigung der Vereinbarung, aus welchem Grund auch immer, löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten oder gibt sie an den Verantwortlichen zurück (unter Einhaltung der eventuell vereinbarten Beendigungsmaßnahmen) und löscht alle vorhandenen Kopien, es sei denn, der Auftragsverarbeiter ist nach den Rechtsvorschriften der EU oder eines Mitgliedstaats verpflichtet, diese personenbezogenen Daten aufzubewahren.

(Stand: Dezember 2023)

ANLAGE ZUM AUFTRAGSVERARBEITUNGSVERTRAG TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

- Stand: Dezember 2023 -

Der nachstehende Maßnahmenkatalog beschreibt die bei WOLTERS KLUWER getroffenen technischen und organisatorischen Maßnahmen gemäß Art 32 DSGVO.

Der Schutz von personenbezogenen Daten von Mitarbeitern, Kunden und anderen Betroffenen (z.B. Besucher) wird durch die in den Geschäftsräumen implementierten technischen und organisatorischen Maßnahmen gewährleistet. Diese Maßnahmen sind nachstehend unter den Gliederungsabschnitten „Standort-IT“ dargestellt.

Sofern personenbezogen Daten extern verarbeitet werden, arbeitet WOLTERS KLUWER mit einem sorgfältig ausgewählten Rechenzentrumsdienstleister zusammen. Der Schutz der personenbezogenen Daten bei diesem Rechenzentrumsdienstleister wird durch die dort implementierten technischen und organisatorischen Maßnahmen gewährleistet. Diese technischen und organisatorischen Maßnahmen sind nachstehend unter den Gliederungsabschnitten „Rechenzentrum“ dargestellt. Der Rechenzentrumsdienstleister ist ISO27001-zertifiziert.

Die hier beschriebenen technischen und organisatorischen Maßnahmen gelten hinsichtlich der Räumlichkeiten und der von den Mitarbeitern genutzten IT-Infrastruktur von WOLTERS KLUWER. Weitere 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.

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.

1.1 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 & DE 60326 Fankfurt

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
- Zusätzliche Advanced Threat Protection
- Wöchentlicher Prüfprozess der Endgeräteabsicherung und Konformität

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 Virtualisierungsumgebung, 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

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 und die Vertraulichkeit im Umgang mit personenbezogenen Daten zu wahren (Datengeheimnis). Die Mitarbeiter von WOLTERS KLUWER, die in einem Bereich arbeiten, bei dem Sie Berührungspunkte mit Daten haben, die der Berufsverschwiegenheit unterliegen, 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. Am Hauptstandort wurde darüber hinaus ein PIN-gesichertes Druckkonzept implementiert, welches sukzessive auch auf weitere Standorte ausgerollt wird.

- 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 können bei Bedarf dezentral protokolliert und ausgewertet werden.

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. Das Gäste-Netzwerk ist mit beschränktem 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. 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 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/wkcloud (TLS+AES) erfolgen.

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

WOLTERS KLUWER unterstützt grundsätzlich eine sichere TLS Verschlüsselung. Sofern in der wechselseitigen Kommunikation unterstützt, ist eine TLS Verschlüsselung in der Version 1.2 grundsätzlich verfügbar.

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

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

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:

- Inkrementelle Backups täglich
- Snapshot-Sicherungen der Server
- Aufbewahrungsfristen je nach Anforderung zwischen 2 Wochen und einem Jahr
- 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 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 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 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) und Informationspflichten eingerichtet.

- WOLTERS KLUWER führt eine Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO) und führt soweit erforderlich Datenschutzfolgenabschätzungen (Art. 35 DSGVO) durch.

- Bei WOLTERS KLUWER bestehen Richtlinien/Anweisungen zur Aufrechterhaltung der Datenschutzorganisation und Datensicherheit.

- Jährliches internes Review der technischen und organisatorischen Maßnahmen, inklusive Erstellung eines Prüfberichtes.

Anhang A.1
Zutrittskontrolle an den Standorten der WOLTERS KLUWER DEUTSCHLAND GMBH

Standorte

Hürth, Münster und Neuwied

- Zutritt zu den Gebäuden ist nur über Chip möglich. Der Zutritt zu den Etagen innerhalb des Gebäudes in Hürth ist ebenfalls nur mit Chip zugänglich.

- Der Zugangs-Chip wird nur den Mitarbeitern und externen Mitarbeitern von WOLTERS KLUWER und den Mitarbeitern des Sicherheitsdienstes und des Reinigungsdienstes zur Verfügung gestellt.

- Besucherregelung: Besucher müssen angemeldet sein. Am Empfang in Hürth erhalten sie einen sichtbar zu tragenden Besucherausweis; Besucher werden immer von einem Mitarbeiter von WOLTERS KLUWER begleitet.

- Die Gebäude und die Außenanlagen in Hürth und Neuwied sind durch Videoüberwachung gesichert. In Neuwied außerhalb der Arbeitszeiten und in Hürth 24/7.

- Das Gebäude in Hürth verfügt über eine Einbruchmeldeanlage (EMA) mit Direktaufschaltung zum Wachdienst. In Neuwied ist das Rechenzentrum über eine Alarmanlage geschützt. Die EMA in Hürth ist aktiv außerhalb der Geschäftszeiten bis 30 Minuten vor Antritt und 24h an Wochenenden und Feiertagen.

- Besetzung Empfang in Hürth durch eigene Mitarbeiter und Sicherheitsdienst:
    - Montag - Freitag 07:30 – 17:00 Uhr

- Brandmeldeanlage vorhanden mit akustischer Alarmierung - in Neuwied mit Aufschaltung zur Alarmzentrale.

Anhang A.2
Zutrittskontrolle an den Standorten der

WOLTERS KLUWER TAX & ACCOUNTING DEUTSCHLAND GMBH
AKADEMISCHE ARBEITSGEMEINSCHAFT VERLAGSGESELLSCHAFT MBH (Mannheim)
WOLTERS KLUWER AGROSOFT GMBH (Ravensburg)

Standorte:

Berlin, Bretten, Dresden, Hamburg, Hannover, Ludwigsburg, Mainz, Mannheim, Ravensburg, Salzwedel und Unterschleißheim

- Zutritt zu den Gebäuden ist nur über Chip oder Schlüssel möglich.
- Der Zugang wird nur den Mitarbeitern und externen Mitarbeitern sowie den Mitarbeitern des Sicherheitsdienstes zur Verfügung gestellt.
- Besucherregelung: Besucher müssen angemeldet sein und werden immer von einem Mitarbeiter begleitet.
- Die Standorte verfügen über eine Einbruchmeldeanlage (EMA) mit Ausnahme der Standorte Münster, Hamburg, Mannheim, und Ravensburg. Die EMA ist aktiv außerhalb der Geschäftszeiten und an Wochenenden und Feiertagen.
- Die Standorte werden außerhalb der Geschäftszeiten regelmäßig durch einen Sicherheitsdienst überwacht, mit Ausnahme der Standorte Berlin, Hannover, Mannheim, Salzwedel und Ravensburg
- Brandmeldeanlage vorhanden mit akustischer Alarmierung mit Ausnahme der Standorte Hannover, Mannheim und Ravensburg.

Anlage 2 – Unterauftragsverarbeiter gem. Art. 28 DS-GVO

Service	Firma, Anschrift	Auftragsinhalt	Produkt / Leistung
Microsoft Azure Services (in Deutschland gehosted) Workplace Infrastruktur für Mitarbeiter	Wolters Kluwer Deutschland GmbH Wolters-Kluwer-Straße 1 50354 Hürth Deutschland	• Bereitstellung von Rechenzentrumsleistungen (Betrieb/Hosting) • Unterstützung bei Betriebsmaßnahmen des Rechenzentrums, z. B. Securityreviews, Audits und andere Sicherheitsmaßnahmen *Erläuterung: Die Wolters-Kluwer- Gruppe bezieht die Azure Services über einen konzernweit abgeschlossenen Vertrag mit Microsoft Corporation. Zu den bestehenden EU-Standardvertragsklauseln wurden zusätzliche Schutzmaßnahmen vereinbart. Es wird der in Deutschland gehostete Azure Service genutzt. Wolters Kluwer Deutschland GmbH erbringt für Wolters Kluwer Tax & Accounting Deutschland GmbH Rechenzentrums- und Hostingleistungen und stellt die Azure Services für Deutschland zur Verfügung.*	• ADDISON • AKTE/ SBS Software • SBS Lohn plus • Support/ Professional Services Betrieb/Hosting nur bei Verwendung von ADDISON Online Funktionen oder ADDISON Online Diensten und Applikationen
Druckdienstleistungen	DATEN_PARTNER Gesellschaft für Direktmarketing und Informations-Technologie mbH Feldheider Straße 39-45 40699 Erkrath Deutschland	• Druckdienstleistungen beispielsweise für Lohnabrechnungen, die als Brief versandt werden • Kunden können diesen Service beauftragen, wenn sie keine elektronische Bereitstellung der Lohnabrechnungen oder anderer Dokumente wünschen	• ADDISON • AKTE/ SBS Software • SBS Lohn plus Nur bei Verwendung der DATEN_PARTNER Druckdienstleistungen
Basecone	Basecone Wolters Kluwer Company Eemweg 8 3742 LB Baarn Niederlande	• Bereitstellung der Basecone Applikationen im Bereich Pre-Accounting inklusive Rechenzentrumsleistungen (Betrieb/Hosting)	• ADDISON • AKTE/ SBS Software Nur bei Verwendung der Basecone App über den Konfigurator
eurodata AG	eurodata AG Großblittersdorfer Str. 257-259 66119 Saarbrücken Deutschland	• Einlesen und Auswerten von Finanzbuchhaltungsdokumenten • Generierung von Kontierungsvorschlägen	• ADDISON • AKTE/ SBS Software Nur bei Verwendung von ADDISON SMART Connect/ Buchungsautomatisierung
finAPI	finAPI GmbH Adams-Lehmann-Str. 44 80797 München Deutschland	• Ermöglicht Zugriff auf Kontendaten von Mandanten, um Kontobewegungen abzufragen • Übermitteln von Zahlungsinformationen/SEPA-Überweisungen an die Banken-Rechenzentren	• ADDISON • AKTE/ SBS Software • SBS Lohn plus Nur bei Verwendung von ADDISON OneClick Online-Banking

Windata	windata GmbH & Co.KG Gegenbaurstraße 4 88239 Wangen im Allgäu Deutschland	• Übermitteln von Zahlungsinformationen/SEPA-Überweisungen an die Banken-Rechenzentren	• SBS Lohn plus Nur bei Verwendung von Online-Banking Rechenzentrum-Dienstleistung (RZDL) im Rahmen des Produktes SBS Lohn plus
EFiS AG	EFiS AG Am Weiher 1 63303 Dreieich Deutschland	• Ermöglicht Zugriff auf Kontendaten von Mandanten, um Kontobewegungen abzufragen • Übermitteln von Zahlungsinformationen/SEPA-Überweisungen an die Banken-Rechenzentren	• ADDISON • AKTE/ SBS Software Nur bei Verwendung von ADDISON Servicerechenzentrum-Dienstleistung
Flowmailer	Flowmailer N.V. Van Nelleweg 1 3044 BC Rotterdam Niederlande	• Versand der Benachrichtigungs- und Passwortwiederherstellungs-E-Mails aus dem ADDISON OneClick-Portal heraus • Flowmailer bekommt die Daten aus dem ADDISON OneClick-Portal und stellt den Versand an Kunden und Mandanten sicher	• ADDISON • AKTE/ SBS Software • SBS Lohn plus Nur bei Verwendung von ADDISON OneClick
DocuWare Cloud	DocuWare Europe GmbH Therese-Giehse-Platz 2 82110 Germering Deutschland	• Dokumentenmanagement (Cloudlösung) • Bei Bedarf technische/beratungsseitige Unterstützung, wenn der Kunde Support oder Professional Service in Anspruch nimmt	• ADDISON • AKTE/ SBS Software • SBS Lohn plus • ADDISON Handwerk • Support/ Professional Services Nur bei Verwendung von DocuWare Cloud
DocuWare On-Premise	DocuWare Europe GmbH Therese-Giehse-Platz 2 82110 Germering Deutschland	• Remote Support für das Produkt DocuWare zur Problemlösung auf Kundensystemen durch DocuWare • Bei Bedarf technische/beratungsseitige Unterstützung, wenn der Kunde Support oder Professional Service in Anspruch nimmt	• ADDISON • AKTE/ SBS Software • SBS Lohn plus • ADDISON Handwerk • Support/ Professional Services Nur bei Verwendung von DocuWare On-Premise

Lansol Hosting Services	LANSOL GmbH Rheingönheimer Weg 13 67117 Limburgerhof Deutschland	• Rechenzentrumsleistungen: Hosting Provider für Endkunden, also Betrieb der Anwendungen (für die Leistungen Mandantenbrief und Homepagebaukasten erbringt Lansol GmbH Hosting Services für den Auftragsverarbeiter Implenity GmbH)	• ADDISON • AKTE/SBS Software • ADDISON Handwerk • Mandantenbrief • Homepage-Baukasten Nur bei Verwendung des ASP-Angebotes
Lansol Datentransferleistungen	LANSOL GmbH Rheingönheimer Weg 13 67117 Limburgerhof Deutschland	• Datentransferleistung im Rahmen der Migration von Kunden des ASP-Angebotes von On-Premise auf ASP	• Support/ Professional Services Nur bei Verwendung des ASP-Angebotes und Datentransferleistungen
BDV	BDV Branchen-Daten-Verarbeitung GmbH Ziegelstr. 1 59439 Holzwickede Deutschland	• Remote Support für das Produkt SBA (Scannen-Buchen-Archivieren) zur Problemlösung auf Kundensystemen durch BDV • Bei Bedarf technische/beratungsseitige Unterstützung, wenn der Kunde Support oder Professional Service in Anspruch nimmt	• ADDISON • AKTE/ SBS Software • Support/ Professional Services Nur bei Verwendung des Produktes SBA
Digitalbar Produkte scan|bar collect|bar	Digitalbar GmbH & Co. KG Fritz-Kotz-Str.14 51674 Wiehl Deutschland	• Remote Support • Bei Bedarf technische/beratungsseitige Unterstützung, wenn der Kunde Support oder Professional Service in Anspruch nimmt	• ADDISON • AKTE/ SBS Software • SBS Lohn plus • Support/ Professional Services Nur bei Verwendung von Digitalbar-Produkten
TeamViewer	TeamViewer GmbH Jahnstr. 30 73037 Göppingen Deutschland	• Remote Support • Support-Mitarbeiter können sich mit dem expliziten Einverständnis des Kunden auf deren Systeme verbinden, um dort bei der Problemanalyse und Fehlerbehebung zu unterstützen	• ADDISON • AKTE/ SBS Software • SBS Lohn plus • ADDISON Handwerk • Support/ Professional Services

ADDISON Portal Plus	Wolters Kluwer Global Business Services B.V. Zuidpoolsingel 2 2408 ZE Alphen aan den Rijn Niederlande	• Bereitstellung des Systems für die Supportticket-Verwaltung und Bearbeitung von Supportanfragen für Kunden. • Der Kunde kann einen eigenen Supportfall erstellen (inklusive Dateianhängen) und bereitgestellte Knowledge-Artikel einsehen. *Erläuterung: Die Wolters Kluwer Gruppe bezieht das System für die Supportticket-Verwaltung (in Deutschland und Frankreich gehosted) über einen konzernweit abgeschlossenen Vertrag mit salesforce.com EMEA Limited, Floor 26 Salesforce Tower, 110 Bishopsgate, London, EC2N 4AY, Großbritannien.*	• ADDISON • AKTE/SBS Software • SBS Lohn plus • ADDISON Handwerk • Support/ Professional Services Nur bei Registrierung und Verwendung des ADDISON Portal Plus.

Anlage 3 – Weisungsberechtige Personen

Weisungsberechtigte Anfragen im Sinne dieser ADV sind an addison@wolterskluwer.com zu richten.

Sonstige Kontaktdaten:

Datenschutzbeauftragter
TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD
Fachstelle für Datenschutz
IT Security
Business Security & Privacy
Telefon: +49 201 8999899
E-Mail: dsb@wolterskluwer.de

Informationssicherheitsbeauftragter
Wolters Kluwer Tax & Accounting Deutschland GmbH
ADDISON Zentrale
Kammererstraße 39
71636 Ludwigsburg
E-Mail: Addison-ZKD@wolterskluwer.com

Anlage 4 – Art der verarbeiteten Kundendaten

Art der Daten	
Kunden- und Lieferantendaten	Für das Rechnungswesen und die Auftrags-/Mandatsbearbeitung notwendige Kunden- und Lieferantendaten, z.B. • Name • Vorname • Anschrift • Branche • Steuernummer • USt ID • Anrede • Bankverbindungen • ggf. USt 1TG - Bescheinigung • Telefon • Telefax • Mobiltelefon • E-Mail • Webadresse • E-Mail-Adresse • Spracheinstellung • Lokation • Belegdaten, inklusive archivierungspflichtige Originalbelege • Vertragsstammdaten • Kommunikationsdaten • Vertragsabrechnungs- und Zahlungsdaten
Personaldaten	Personaldaten von abgerechneten Arbeitnehmern und/oder Mitarbeitern Unter anderem: • Benutzername • Anrede • Namenszusatz • Vorsatzwort • Titel • Name • Vorname • Straße / Hausnummer • Anschriftenzusatz • Postleitzahl (Wohn)-ort • Geburtsland, Geburtsdatum • Eintrittsdatum (Erst-Eintrittsdatum) • Austrittsdatum • Geschlecht • Familienstand • Beschäftigungsart • Beschäftigungsort • Telefonnummer • Mobilfunknummer • E-Mail-Adresse • SteuerID • eTIN • Steuerklasse • Konfession Arbeitnehmer • Konfession Ehegatte • Kinder Anzahl Freibeträge • Monatsfreibetrag

	• Jahresfreibetrag • Staatsangehörigkeit • Mitarbeiterstatus • Tätigkeitsschlüssel • Krankenkassen • Zahlungsart • Arbeitnehmerbank Bezeichnung • Swift-BIC Arbeitnehmerbank • IBAN Arbeitnehmerbank • Sonstige steuerlich, SV, KV abrechnungsrelevante Daten • Daten zu ausgestellten Bescheinigungen (z.B. Arbeitsamt …)
Steuerpflichtige	Im Rahmen der Steuererklärung erhobene steuerrelevante Daten, z.B. • Persönliche Daten • Einkünfte • Besondere steuerrelevante Eigenschaften (Behinderung, Renten …) • Daten über Kinder, Ehegatten • Pflegebedürftigkeit • Originalbelege

Anlage 5 – Kreis der Betroffenen

Kreis der Betroffenen	
	Insbesondere: • Kunden/deren Mandanten • Interessenten/deren Mandanten • Beschäftigte • Lieferanten • Handelsvertreter

Anlage 6 - Umfang, Art und Zweck der Auftragsverarbeitung

a. Bei **Nutzung von Addison OneClick**: WOLTERS KLUWER stellt dem Kunden Portalleistungen entsprechend den Tätigkeiten wie sie im Nutzungsvertrag und deren Anlagen definiert sind zur Verfügung.

   Bei **Nutzung des ASP-Angebotes:** WOLTERS KLUWER wird entsprechend der Tätigkeiten, wie sie im Nutzungsvertrag und deren Anlagen definiert sind, für den Kunden als Subunternehmer im Bereich Hosting und Providing für Endkunden tätig.

   Bei Nutzung der Docuware-Cloud-Lösung: WOLTERS KLUWER stellt dem Kunden über Subunternehmer ein cloudbasiertes Dokumentenmanagement-System nebst Applikationen entsprechend der Tätigkeiten, wie sie im Nutzungsvertrag und deren Anlagen definiert sind, zur Verfügung.

b. WOLTERS KLUWER übernimmt den Support bzw. Professional Services für Kunden und Interessenten. Dieser umfasst je nach Umfang des Nutzungsvertrages insbesondere:
   - Einstellen und Einrichten der Softwareprodukte, Schnittstellen etc.
   - Online-Schulungen
   - Remotezugriff auf das Benutzerkonto des Kunden in den dem Service zugrundeliegenden IT-Systemen
   - Umgang mit einem Echtdaten enthaltenen Dump / Snapshot / Backup
   - Fehlerbehebung, Prüfung von Datenbeständen
   - Datentransfer auf das IT-System von WOLTERS KLUWER bzw. ihrer eingesetzten Dienstleister z.B. zur Analyse des Datenbestandes nach technischen Gesichtspunkten, im Rahmen von Serverumzügen
   - Migration von Datenbeständen insbesondere von und in die WOLTERS KLUWER Softwareumgebung

   Die Verarbeitung erfolgt in der Regel durch Remote-Zugriff von WOLTERS KLUWER auf die Daten bzw. IT-Systeme des Kunden und/oder per Telefon, Fax oder E-Mail oder durch Präsenz vor Ort beim Kunden.

c. Des Weiteren stellt WOLTERS KLUWER dem Kunden ggf. Rechnerkapazitäten 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 Backendsysteme inklusive der Datenbanksysteme und Portalsysteme/Apps, sowie die Pflege der Hardwaresysteme, auf denen die Dienste basieren.