

# Vereinbarung

zwischen

- Verantwortlicher - nachstehend Auftraggeber genannt –

und

Bi Smart Tu GmbH, Wallstraße 43, 21335 Lüneburg, vertreten durch den Geschäftsführer Herrn Claas Beckmann

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

## § 1

### Gegenstand und Dauer des Auftrags

#### (1) Gegenstand

Der Gegenstand des Auftrags zum Datenumgang ergibt sich aus dem Hauptvertrag der Parteien, auf den hier verwiesen wird (im Folgenden als „Leistungsvereinbarung“ bezeichnet). Gegenstand der Leistungsvereinbarung sind Leistungen des Auftragnehmers zur Verarbeitung und Abwicklung von Verfahrensdokumentationen, die Abwicklung von Kassenmeldungen der Mandanten/Kunden des Auftraggebers sowie die Bereitstellung eines Tools zur Stammdatenbearbeitung.

#### (2) Dauer

Die Laufzeit dieses Auftrags entspricht der Laufzeit der Leistungsvereinbarung.

## § 2

### Konkretisierung des Auftragsinhalts

#### (1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Die Verarbeitung personenbezogener Daten durch den Auftragnehmer dient der Verarbeitung und Abwicklung von Verfahrensdokumentationen und der Bereitstellung von verschie-

denen EDV-Produkten. Dies umfasst das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Weitergabe durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung und das Löschen von personenbezogenen Daten (insbesondere von Verfahrensdokumentationen).

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber ergeben sich zudem aus der Leistungsvereinbarung.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

## (2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Anrede
- Vor- und Nachname,
- Nutzer-IDs, Benutzernamen,
- Kontaktdaten/Kommunikationsdaten (z.B. Anschrift, Telefon, E-Mail,)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie, sonstige kundenbezogene Daten
- Vertragsabrechnungs- und Zahlungsdaten
- Buchhaltungsdaten
- Sonstige personenbezogene Daten, die vom Auftraggeber aktiv hinterlegt werden, bspw. im Rahmen von der Erstellung der Verfahrensdokumentationen (ggf. inkl. Daten zur Verfahrensdokumentation, der Kassenmeldung und der Stammdatenpflege der Kunden/Mandanten des Auftraggebers, sofern diese der Auftraggeber über die EDV-Produkte des Auftragnehmers verarbeitet).

## (3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden/Mandanten und sonstige Vertragspartner, Dienstleister und sonstige Ansprechpartner des Auftraggebers
- Beschäftigte der Kunden/Mandanten des Auftraggebers
- Beschäftigte des Auftraggebers
- Sonstige Personen, die Gegenstand der Verfahrensdokumentationen, der Kassenmeldung und der Stammdatenpflege des Auftraggebers bzw. von dessen Kunden/Mandanten sind (z.B. weitere Vertragsparteien, Kontaktpersonen/Ansprechpartnern) bzw. die der Auftraggeber über die EDV-Produkte des Auftragnehmers verarbeitet.

### § 3

#### **Technisch-organisatorische Maßnahmen**

- (1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
- (2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in der **Anlage**].
- (3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

### § 4

#### **Berichtigung, Einschränkung und Löschung von Daten**

- (1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder de-

ren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

- (2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

## **§ 5**

### **Qualitätssicherung und sonstige Pflichten des Auftragnehmers**

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- a) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr Claas Beckmann, [info@einfach-edocu.de](mailto:info@einfach-edocu.de), Bi Smart Tu GmbH, Wallstraße 43, 21335 Lüneburg
- b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
- c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in der **Anlage**].
- d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Be-

zug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

- f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- h) Die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 7 dieses Vertrages.

## **§ 6**

### **Unterauftragsverhältnisse**

- (1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
- (2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.
  - a) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

|                        |                |          |
|------------------------|----------------|----------|
| Firma Unterauftragneh- | Anschrift/Land | Leistung |
|------------------------|----------------|----------|

|                                                                               |                                     |                           |
|-------------------------------------------------------------------------------|-------------------------------------|---------------------------|
| mer                                                                           |                                     |                           |
| Wolters Kluwer Tax & Accounting GmbH                                          | Kammerer Str. 39, 71636 Ludwigsburg | Anbieter IT-Infrastruktur |
| StBVS Steuerberater<br>Verrechnungsstelle<br>VS Rechtsanwaltsgesellschaft mbH | Schanzenstraße 30,<br>51063 Köln    | Factoring                 |

b) Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

## **§ 7**

### **Kontrollrechte des Auftraggebers**

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

- (2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
- (3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch
- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
  - die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
  - aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
  - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).
- (4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

## **§ 8**

### **Mitteilung bei Verstößen des Auftragnehmers**

- (1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.
- a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;
  - b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden;

- c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;
  - d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung;
  - e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.
- (2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

## **§ 9**

### **Weisungsbefugnis des Auftraggebers**

- (1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).
- (2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

## **§ 10**

### **Löschung und Rückgabe von personenbezogenen Daten**

- (1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
- (2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

- (3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

, den

, den

---

Auftraggeber



---

Auftragnehmer

## **Anlage : Technisch-organisatorische Maßnahmen**

Da die Verarbeitung personenbezogener Daten, die Gegenstand der AVV sind, ausschließlich über unseren Dienstleister Wolters Kluwer erfolgt, verweisen wir auf die nachstehenden Darstellungen von Wolters Kluwer.

## **ANLAGE 2 – 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 personenbezogenen 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 Frankfurt

#### **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 Virtualisierungs-umgebung, sowie der Netzwerk- und Internet-Infrastruktur. Die unbefugte Nutzung von DV-Systemen des Rechenzentrumsbetreibers 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 Rechenzentrumsbetreibers 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 Stagingssysteme 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 WLAN 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 kreuzangeordneten doppelten Kopf auf RAID-gespiegelten Diskshelms. Das gilt sowohl für Netzlaufwerkspeicher als auch für virtuelle Server.

Darüber hinaus sind zentrale Netzwerkkomponenten (Switches, 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 KLUWER 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 einem 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 3 – UNTERAUFTRAGSVERARBEITER**

| Firma                                                                                                                                                         | Anschrift                                                                                | Auftragsinhalt                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Produkt / Leistung                                                                                                                 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Wolters Kluwer Tax and Accounting Tech. B.V.<br><br>(einschließlich Hosting über Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, L-1855, Luxemburg) | De Beek 9, 3871 MS, Hoevelaken                                                           | Betrieb und Web-Hosting, Infrastruktur, Fehlersammlung und -überwachung, Analyse, Support<br><br>Art der verarbeiteten Daten:<br><ul style="list-style-type: none"><li>• produktspezifische Daten</li><li>• E-Mail Adresse</li><li>• Vor- und Nachname</li><li>• IP-Adresse</li><li>• Telefonnummer</li><li>• TaskFlow-Benutzer-ID (TUID)</li></ul><br>Die Datenverarbeitung bei AWS erfolgt grundsätzlich innerhalb von Deutschland.                                                                                                                                                                                                                                                                                                                      | Bereitstellung Komponente „Taskflow“                                                                                               |
| Microsoft Azure Services (in Deutschland gehostet)<br><br>Workplace Infrastruktur für Mitarbeiter                                                             | Wolters Kluwer Deutschland GmbH<br><br>Wolters-Kluwer-Straße 1, 50354 Hürth, Deutschland | <ul style="list-style-type: none"><li>• Bereitstellung von Rechenzentrumsleistungen (Betrieb/Hosting)</li><li>• Unterstützung bei Betriebsmaßnahmen des Rechenzentrums, z. B. Securityreviews, Audits und andere Sicherheitsmaßnahmen</li></ul><br>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. | Betrieb/Hosting nur bei Verwendung von ADDISON Online Funktionen oder ADDISON Online Diensten und Applikationen (ADDISON OneClick) |
| Flowmailer                                                                                                                                                    | Flowmailer N.V.<br>Van Nelleweg 1<br>3044 BC Rotterdam Niederlande                       | Versand der Benachrichtigungs- und Passwortwiederherstellungs-E-Mails aus dem ADDISON OneClick-Portal heraus<br><br>Flowmailer bekommt die Daten aus dem ADDISON OneClick-Portal und stellt den Versand an Kunden und Mandanten sicher                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | ADDISON OneClick                                                                                                                   |
| TeamViewer                                                                                                                                                    | TeamViewer GmbH<br>Jahnstr. 30<br>73037 Göppingen Deutschland                            | Remote Support<br><br>Support-Mitarbeiter können sich mit dem expliziten Einverständnis des Kunden auf deren Systeme verbinden, um dort bei der Problemanalyse und Fehlerbehebung zu unterstützen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | ADDISON OneClick                                                                                                                   |