

## **1 Präambel:**

1.1 Dieser AVV bildet einen Anhang zu den Allgemeinen Geschäftsbedingungen und dem Dienstleistungsvertrag, der bei einer Beauftragung der Kanzlei C5 abzuschließen ist.

1.2 Mit der Annahme der Allgemeinen Geschäftsbedingungen haben der Verantwortliche und der Auftragsverarbeiter diesen AVV als Teil der Dienstleistungsbeauftragung akzeptiert, um sicherzustellen, dass die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen in Übereinstimmung mit den geltenden Datenschutzgesetzen erfolgt.

1.3 Die folgend aufgeführten Standardvertragsklauseln erfüllen gemäß Durchführungsbeschluss der EU-Kommission vom 04.06.2021 EU die Anforderungen an Verträge zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725. Demnach werden diese Standardvertragsklauseln als Vertrag zwischen einem Verantwortlichen und einem Auftragsverarbeiter, der personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, verwendet als:

# **Vertrag zur Auftragsverarbeitung**

## **Standardvertragsklauseln**

### **ABSCHNITT I**

#### *Klausel 1*

#### **Zweck und Anwendungsbereich**

- a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sichergestellt werden.
- b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.
- c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.
- d) Die Anhänge I bis IV sind Bestandteil der Klauseln.
- e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.
- f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

#### *Klausel 2*

#### **Unabänderbarkeit der Klauseln**

- a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

- b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

#### *Klausel 3*

#### **Auslegung**

- a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.
- b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.
- c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

#### *Klausel 4*

#### **Vorrang**

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

#### *Klausel 5*

#### **Kopplungsklausel**

- a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.
- b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.
- c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

### **ABSCHNITT II**

### **PFLICHTEN DER PARTEIEN**

#### *Klausel 6*

#### **Beschreibung der Verarbeitung**

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

## Klausel 7

### **Pflichten der Parteien**

#### **7.1. Weisungen**

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

#### **7.2. Zweckbindung**

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

#### **7.3. Dauer der Verarbeitung personenbezogener Daten**

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

#### **7.4. Sicherheit der Verarbeitung**

a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

#### **7.5. Sensible Daten**

Falls die Verarbeitung personenbezogener Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

#### **7.6. Dokumentation und Einhaltung der Klauseln**

a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

- d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.
- e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

### **7.7. Einsatz von Unterauftragsverarbeitern**

- a) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste (Anhang IV) aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 14 Tage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.
- b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.
- c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.
- d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.
- e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

### **7.8. Internationale Datenübermittlungen**

- a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.
- b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

## Klausel 8

### **Unterstützung des Verantwortlichen**

- a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.
- b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.
- c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:
- 1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;
  - 2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;
  - 3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;
  - 4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.
- d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

## Klausel 9

### **Meldung von Verletzungen des Schutzes personenbezogener Daten**

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

#### **9.1. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten**

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

- a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);
- b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:
- 1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
  - 2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und so weit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679 die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

## **9.2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten**

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

- a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);
- b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;
- c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und so weit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

**ANHANG I**  
**Liste der Parteien**

**Verantwortliche(r):** **Auftraggebende/s Organisation/Unternehmen,**  
benannt gemäß Dienstleistungsvertrag dem dieser  
Vertrag zur Auftragsverarbeitung als Anlage hinzugefügt  
ist.

**Auftragsverarbeiter:** **Kanzlei C5 Unternehmensberatung**  
Tobias Wolf  
Dr. Max Str. 14  
82031 Grünwald

## ANHANG II

### **Beschreibung der Verarbeitung**

Der Auftragsverarbeiter bietet Beratungen und Schulungen im Bereich Vergütungsmodelle von Mitarbeitern an. Dabei wird analysiert, ob und welche Optimierungsmöglichkeiten für den Auftraggeber in Frage kommen. Bei erfolgreichen Optimierungen kann der Auftraggeber eingesetzt werden, im Rahmen eines zu vereinbarenden Konzeptes, diese Optimierungen an die Mitarbeiter des Unternehmens zu kommunizieren, beispielsweise per Schulung.

Wenn der Verantwortliche den Auftragsverarbeiter mit der Verarbeitung zusätzlicher personenbezogener Daten beauftragen möchte, die über die nachstehend genannten personenbezogenen Daten hinausgehen, muss er dies dem Auftragsverarbeiter mitteilen. Der Auftragsverarbeiter wird den Antrag prüfen und – wenn möglich – die Änderungen bestätigen.

#### *Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden*

- Mitarbeiter
- Kunden und voraussichtliche Kunden
- Lieferanten
- Geschäftspartner
- Sonstige:

#### *Kategorien personenbezogener Daten, die verarbeitet werden*

- Namen
- Geschäftliche Kontaktdaten (z. B. Geschäftsadresse, geschäftliche E-Mail, geschäftliche Telefonnummer)
- Persönliche Kontaktdaten (z. B. private Adresse, private E-Mail, private Telefonnummer)
- Benutzerdaten. B. Benutzername, Passwort, Benutzerhistorie, Protokolldateien, IP-Adresse)
- HR-Informationen (z. B. Gehalt, Zeiterfassungsdaten)
- Sonstige:

*Verarbeitete sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen*

- Rassistische und ethnische Herkunft
- politische Meinungen, religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Genetische Daten
- Biometrische Daten
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung
- Daten über strafrechtliche Verurteilungen und Straftaten



### **Umfang, Art und Zweck der Datenverarbeitung, Art der personenbezogenen Daten und Datensubjekte**

Der Auftragsverarbeiter bietet eine Beratung und Schulung im Bereich von Bezahlung und Vergütung von Mitarbeitern mittelständischer Unternehmen an. Schwerpunkt sind Optimierungsmöglichkeiten, steuerliche Vergünstigungen sowie Einführung und Verwaltung von Benefits.

Die Dienstleistung erstreckt sich hauptsächlich auf Beratung und Schulung. Ein Zugriff auf elektronische Systeme und Softwaresysteme des Kunden erfolgt zu keinem Zeitpunkt.

Im Rahmen der Zusammenarbeit werden dazu geschäftliche Kontaktdaten von Ansprechpartnern/Mitarbeitern und teilweise von Geschäftspartnern des beratenen Unternehmens verarbeitet.

Im Zuge der Beratung können allgemeine Steuermerkmale (wie Steuerklassen, Krankenversicherungszusatzbeiträge, Konfessionszugehörigkeiten, Kinderfreibeträge o.ä.) zur Berechnung allgemeiner Zuschüsse erfragt werden und bei Kanzlei C5 verarbeitet werden. Diese Strukturdaten werden ohne Nennung von Namen, Geburtsdaten, Adressen oder anderer Daten, die eine eindeutige Zuordnung zu einer Person ermöglichen, zur Verfügung gestellt.

Diese allgemeinen Steuermerkmale werden zum Zwecke von Auswertungen und Berechnungen während des Projektzeitraumes von maximal 36 Monaten verwendet.

Die Löschung geschäftlicher Kontaktdaten und personenbezogener Daten, die innerhalb der Auftragsabwicklung erhoben und verarbeitet werden, erfolgt nach Wegfall gesetzlicher Aufbewahrungsfristen.

## ANHANG III

### Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Daten

#### **Vertraulichkeit**

- **Zutritt**

Kein unbefugter Zutritt für Dritte: Empfangssituation. Besucher werden in Empfang genommen und begleitet. Büro-Räume/-Gebäude Schließsystem, zu Ruhezeiten Kontrollen durch Sicherheitsdienst.

- **Zugang**

Systembenutzung nur durch sichere Identifikation über Passwörter bzw. biometrische Zugangsschlüssel, Einrichtung automatischer Kontroll- und Sperrmechanismen.

- **Zugriff**

Striktes Need to Know-Prinzip bei Rechte-/Rollenkonzepten zur Verhinderung von unbefugtem Lesen, Kopieren, Verändern oder Entfernen von personenbezogenen Daten innerhalb der Systeme.

Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte sowie Rechtebeschränkung, Protokollierung und Überwachung von Zugriffen, im Incident-Fall nachvollziehbar.

- **Trennung**

Logische Mandantentrennung in verwendeten Systemen.

- **Pseudonymisierung/Anonymisierung**

Für Berechnungsmodelle der Lohn/Gehaltsdaten werden, abhängig von den Vorgaben des Verantwortlichen, vollständig pseudonymisierte oder anonymisierte Datensätze verwendet.

#### **Integrität, Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit**

- **Integrität**

Systeme laufen auf gesicherten Servern in Deutschland und/oder EWR, Redundanz sichert Wiederherstellbarkeit

- **Weitergabekontrolle**

Verschlüsselung, verschlossene Transportbehälter, Überwachung und Protokollierung von Datenübertragungen und Datenübergaben, Virtual Private Networks (VPN) zur Verhinderung von unbefugtem Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport.

- **Eingabekontrolle**

Protokollierung und Dokumentenmanagement der verwendeten Systeme

- **Verfügbarkeit**

Brandschutz, Virenschutz, Firewall, Ausfallschutz, Sicherungs- und Backup-Strategien gewährleisten Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste

## **Datenschutz-Management**

**Evaluierung**, regelmäßiger Einsatz Datenschutzauditor

**Datenschutztraining** Mitarbeiter; regelmäßige Schulung

**Prozesse/Verarbeitungen** und TOM, anlassbezogene und Regelprüfungen/Anpassungen. Protokollierungen, Überwachung von Wartungstätigkeiten, vertragliche Regelungen, Prozessbeschreibungen

**Auftragskontrolle**, mit Dienstleistern, die zur Durchführung und Aufrechterhaltung des Geschäftsbetriebes beitragen sind Verträge zur Auftragsverarbeitung geschlossen.

**Löschkonzept**, Löschung nach Zweckentfall. Einsatz automatisierter Löschroutinen nach Entfall von Aufbewahrungspflichten.

**Privacy by Default**, datenschutzfreundliche Voreinstellungen in den Systemen werden regelmäßig überprüft, bei Neuinstallationen wird sichergestellt, dass die Einstellungen datenschutzfreundlich ausgewählt werden.

**Privacy by Design**, Datenschutzaspekte und Anforderungen werden in Planungsphase neuer Prozesse einbezogen.

**Betroffenenrechte**, Prozesse zur Sicherstellung eingerichtet.

**Datenschutzvorfälle**, Bewertungs- und Meldeprozesse eingerichtet

## **ANHANG IV**

### **Liste der Unterauftragsverarbeiter**

Kein direkter Einsatz von Unterauftragnehmern in Verbindung mit der beschriebenen Verarbeitung.