

Auftragsverarbeitungsvertrag

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DSGVO

zwischen

...

– nachfolgend „**Auftraggeber**“ genannt –

und

CANEI.tax GmbH & Co. KG (Vormals HAUFE-CANEI GmbH & Co. KG)

Phönixseestr. 22a

44263 Dortmund

– nachfolgend „**Auftragnehmer**“ genannt –

1. Vertragsgegenstand

Im Rahmen der Nutzung der Software Lösungen **CANEI.tax** (nachfolgend „**Hauptvertrag**“ genannt) ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten umgeht, für die der Auftraggeber als Verantwortlicher im Sinne der datenschutzrechtlichen Vorschriften fungiert (nachfolgend „**Auftraggeber-Daten**“ genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung des Hauptvertrags.

2. Umfang der Beauftragung

- 2.1 Der Auftragnehmer verarbeitet die Auftraggeber-Daten im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber bleibt Verantwortlicher im datenschutzrechtlichen Sinn.
- 2.2 Die Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer erfolgt in der Art, dem Umfang und zu dem Zweck wie in **Anlage 1** zu diesem Vertrag spezifiziert; die Verarbeitung betrifft die darin bezeichneten Arten personenbezogener Daten und Kategorien betroffener Personen. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.
- 2.3 Dem Auftragnehmer bleibt es vorbehalten, die Auftraggeber-Daten zu anonymisieren oder zu aggregieren, so dass eine Identifizierung einzelner betroffener Personen nicht mehr möglich ist, und in dieser Form zum Zweck der bedarfsgerechten Gestaltung, der Weiterentwicklung und der Optimierung sowie der Erbringung des nach Maßgabe des Hauptvertrags vereinbarten Dienstes zu verwenden. Die Parteien stimmen darin überein, dass anonymisierte bzw. nach obiger Maßgabe aggregierte Auftraggeber-Daten nicht mehr als Auftraggeber-Daten im Sinne dieses Vertrags gelten.
- 2.4 Der Auftragnehmer darf die Auftraggeber-Daten im Rahmen des datenschutzrechtlich Zulässigen für eigene Zwecke auf eigene Verantwortung verarbeiten und nutzen, wenn eine gesetzliche

Erlaubnisvorschrift oder eine Einwilligungserklärung des Betroffenen das gestattet. Auf solche Datenverarbeitungen findet dieser Vertrag keine Anwendung.

- 2.5 Die Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer findet grundsätzlich innerhalb der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Es ist dem Auftragnehmer gleichwohl gestattet, Auftraggeber-Daten unter Einhaltung der Bestimmungen dieses Vertrags auch außerhalb des EWR zu verarbeiten, wenn er den Auftraggeber vorab über den Ort der Datenverarbeitung informiert und die Voraussetzungen der Art. 44–48 DSGVO erfüllt sind oder eine Ausnahme nach Art. 49 DSGVO vorliegt.
- 2.6 Im Rahmen dieses Auftrages werden auch Daten verarbeitet, die unter ein Berufsgeheimnis (im Sinne von § 203 StGB) fallen. Der Auftragnehmer verpflichtet sich, über Berufsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben erforderlich ist. Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, strafbar machen nach § 203 Abs. 4 S. 1 StGB. Zudem macht sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.
 - 2.6.1 Der Auftragnehmer stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Auftraggebers befassten Beschäftigten und andere für den Auftragnehmer tätigen Personen (z.B. Subunternehmer), die damit befasst sind, sich in Textform dazu verpflichtet haben, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB belehrt wurden. Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar macht, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und die mitwirkende Person nicht dafür Sorge getragen hat, dass die weitere mitwirkende Person zur Geheimhaltung verpflichtet wurde.
 - 2.6.2 Der Auftragnehmer ist berechtigt, Unterauftragnehmer zur Vertragserfüllung heranzuziehen. Im Ausland dürfen Unterauftragnehmer zur Vertragserfüllung nur dann herangezogen werden, wenn im Falle des damit verbundenen Zugangs zu fremden Geheimnissen der dort bestehende Schutz der Geheimnisse dem Schutz im Inland vergleichbar ist. Der Auftragnehmer wird etwaige Unterauftragnehmer sorgfältig auswählen und diese, soweit sie im Rahmen ihrer Tätigkeit Kenntnis von fremden Geheimnissen im Sinne dieser Vereinbarung erlangen könnten, zum Stillschweigen verpflichten. Der Auftragnehmer wird ferner etwaige Unterauftragnehmer dazu verpflichten, sämtliche von diesen eingesetzte Personen und etwaige weitere Unterauftragnehmer, die bestimmungsgemäß mit Geheimnisschutzdaten in Berührung kommen oder bei denen dies nicht auszuschließen ist, nach den zuvor genannten Grundsätzen zur Verschwiegenheit zu verpflichten und über die Folgen einer Pflichtverletzung zu belehren. Des weiteren werden Subunternehmer über das bestehende Schweigerecht gemäß § 53a StPO sowie den Beschlagnahmenschutz gemäß § 97 StPO informiert; dies beinhaltet auch den Hinweis auf das Recht des Berufsgeheimnisträgers über dieses Recht zu entscheiden und die damit verbundene Pflicht, unverzüglich den Auftraggeber bzgl. der Wahrnehmung dieser Rechte zu kontaktieren. Diese Verpflichtung gilt für sämtliche weitere Unterbeauftragungen.
 - 2.6.3 Der Auftragnehmer wird darauf hingewiesen, dass Daten, die er im Auftrag eines Berufsgeheimnisträgers verarbeitet u.U. dem Zeugnisverweigerungsrechts von sogenannten mitwirkenden Personen unterliegt (§ 53a Strafprozessordnung (StPO)). Entsprechend § 53a StPO entscheidet jedoch der Berufsgeheimnisträger über die Ausübung des Schweigerechts. Im Falle einer Befragung wird der Auftragnehmer unter Hinweis auf § 53a StPO dieser widersprechen und unverzüglich den Auftraggeber informieren, der daraufhin bzgl. der Wahrnehmung des Schweigerechts entscheidet.

- 2.6.4 Der Auftragnehmer wird darauf hingewiesen, dass die sich in seinem Gewahrsam befindenden Geheimnisschutzdaten dem Beschlagnahmeverbot gemäß § 97 Abs. 2 StPO unterliegen. Die Daten dürfen nicht ohne das Einverständnis des Auftraggebers (Berufsgeheimnisträger) herausgegeben werden. Im Falle einer Beschlagnahme wird der Auftragnehmer dieser widersprechen und unverzüglich den Auftraggeber informieren.

3. Weisungsbefugnisse des Auftraggebers

- 3.1 Der Auftragnehmer verarbeitet die Auftraggeber-Daten gemäß den Weisungen des Auftraggebers, sofern der Auftragnehmer nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
- 3.2 Die Weisungen des Auftraggebers sind grundsätzlich abschließend in den Bestimmungen dieses Vertrags festgelegt und dokumentiert. Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers und erfolgen nach Maßgabe des im Hauptvertrag festgelegten Änderungsverfahrens, in dem die Weisung zu dokumentieren und die Übernahme etwa dadurch bedingter Mehrkosten des Auftragnehmers durch den Auftraggeber zu regeln ist.
- 3.3 Der Auftragnehmer gewährleistet, dass er die Auftraggeber-Daten im Einklang mit den Weisungen des Auftraggebers verarbeitet. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, ist er nach einer entsprechenden Mitteilung an den Auftraggeber berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen. Die Parteien stimmen darin überein, dass die alleinige Verantwortung für die weisungsgemäße Verarbeitung der Auftraggeber-Daten beim Auftraggeber liegt.

4. Verantwortlichkeit des Auftraggebers

- 4.1 Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen im Verhältnis der Parteien zueinander allein verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund der Verarbeitung von Auftraggeber-Daten nach Maßgabe dieses Vertrages Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.
- 4.2 Dem Auftraggeber obliegt es, dem Auftragnehmer die Auftraggeber-Daten rechtzeitig zur Leistungserbringung nach dem Hauptvertrag zur Verfügung zu stellen und er ist verantwortlich für die Qualität der Auftraggeber-Daten. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.
- 4.3 Der Auftraggeber hat dem Auftragnehmer auf Anforderung die in Art. 30 Abs. 2 DSGVO genannten Angaben zur Verfügung zu stellen, soweit sie dem Auftragnehmer nicht selbst vorliegen.
- 4.4 Ist der Auftragnehmer gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von Auftraggeber-Daten zu erteilen oder mit diesen Stellen anderweitig zusammenzuarbeiten, so ist der Auftraggeber verpflichtet, den Auftragnehmer auf erstes Anfordern bei der Erteilung solcher Auskünfte bzw. der Erfüllung anderweitiger Verpflichtungen zur Zusammenarbeit zu unterstützen.

5. Anforderungen an Personal

Der Auftragnehmer hat alle Personen, die Auftraggeber-Daten verarbeiten, bezüglich der Verarbeitung von Auftraggeber-Daten zur Vertraulichkeit zu verpflichten.

6. Sicherheit der Verarbeitung

- 6.1 Der Auftragnehmer wird gemäß Art. 32 DSGVO erforderliche, geeignete technische und organisatorische Maßnahmen ergreifen, die unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Auftraggeber-Daten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeber-Daten zu gewährleisten.
- 6.2 Dem Auftragnehmer ist es gestattet, technische und organisatorische Maßnahmen während der Laufzeit des Vertrages zu ändern oder anzupassen, solange sie weiterhin den gesetzlichen Anforderungen genügen.

7. Inanspruchnahme weiterer Auftragsverarbeiter

- 7.1 Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung, weitere Auftragsverarbeiter hinsichtlich der Verarbeitung von Auftraggeber-Daten hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses hinzugezogenen und hiermit genehmigten weiteren Auftragsverarbeiter ergeben sich aus **Anlage 2**. Generell nicht genehmigungspflichtig sind Vertragsverhältnisse mit Dienstleistern, die die Prüfung oder Wartung von Datenverarbeitungsverfahren oder -anlagen durch andere Stellen oder andere Nebenleistungen zum Gegenstand haben, auch wenn dabei ein Zugriff auf Auftraggeber-Daten nicht ausgeschlossen werden kann, solange der Auftragnehmer angemessene Regelungen zum Schutz der Vertraulichkeit der Auftraggeber-Daten trifft.
- 7.2 Der Auftragnehmer wird den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter informieren. Dem Auftraggeber steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines potenziellen weiteren Auftragsverarbeiters zu erheben. Ein Einspruch darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erhoben werden. Soweit der Auftraggeber nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Auftraggeber Einspruch, ist der Auftragnehmer berechtigt, den Hauptvertrag und diesen Vertrag mit einer Frist von 3 Monaten zu kündigen.
- 7.3 Der Vertrag zwischen dem Auftragnehmer und dem weiteren Auftragsverarbeiter muss letzterem dieselben Pflichten auferlegen, wie sie dem Auftragnehmer kraft dieses Vertrages obliegen. Die Parteien stimmen überein, dass diese Anforderung erfüllt ist, wenn der Vertrag ein diesem Vertrag entsprechendes Schutzniveau aufweist bzw. dem weiteren Auftragsverarbeiter die in Art. 28 Abs. 3 DSGVO festgelegten Pflichten auferlegt sind.
- 7.4 Unter Einhaltung der Anforderungen der Ziffer 2.5 dieses Vertrags gelten die Regelungen in dieser Ziffer 7 auch, wenn ein weiterer Auftragsverarbeiter in einem Drittstaat eingeschaltet wird. Der Auftraggeber bevollmächtigt den Auftragnehmer hiermit, in Vertretung des Auftraggebers mit einem weiteren Auftragsverarbeiter einen Vertrag unter Einbeziehung der EU-Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern zu schließen. Der Auftraggeber erklärt sich bereit, an der Erfüllung der Voraussetzungen nach Art. 49 DSGVO im erforderlichen Maße mitzuwirken.

8. Rechte der betroffenen Personen

- 8.1 Der Auftragnehmer wird den Auftraggeber mit technischen und organisatorischen Maßnahmen im Rahmen des Zumutbaren dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.

- 8.2 Soweit eine betroffene Person einen Antrag auf Wahrnehmung der ihr zustehenden Rechte unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen zeitnah an den Auftraggeber weiterleiten.
- 8.3 Der Auftragnehmer wird dem Auftraggeber Informationen über die gespeicherten Auftraggeber-Daten, die Empfänger von Auftraggeber-Daten, an die der Auftragnehmer sie auftragsgemäß weitergibt, und den Zweck der Speicherung mitteilen, sofern dem Auftraggeber diese Informationen nicht selbst vorliegen oder er sie sich selbst beschaffen kann.
- 8.4 Der Auftragnehmer wird es dem Auftraggeber ermöglichen, im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten, Auftraggeber-Daten zu berichtigen, zu löschen oder ihre weitere Verarbeitung einzuschränken oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Einschränkung der weiteren Verarbeitung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.
- 8.5 Soweit die betroffene Person gegenüber dem Auftraggeber ein Recht auf Datenübertragbarkeit bezüglich der Auftraggeber-Daten nach Art. 20 DSGVO besitzt, wird der Auftragnehmer den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei der Bereitstellung der Auftraggeber-Daten in einem gängigen und maschinenlesbaren Format unterstützen, wenn der Auftraggeber sich die Daten nicht anderweitig beschaffen kann.

9. Mitteilungs- und Unterstützungspflichten des Auftragnehmers

- 9.1 Soweit den Auftraggeber eine gesetzliche Melde- oder Benachrichtigungspflicht wegen einer Verletzung des Schutzes von Auftraggeber-Daten (insbesondere nach Art. 33, 34 DSGVO) trifft, wird der Auftragnehmer den Auftraggeber zeitnah über etwaige meldepflichtige Ereignisse in seinem Verantwortungsbereich informieren. Der Auftragnehmer wird den Auftraggeber bei der Erfüllung der Melde- und Benachrichtigungspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten unterstützen.
- 9.2 Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei etwa vom Auftraggeber durchzuführenden Datenschutz-Folgenabschätzungen und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO unterstützen.

10. Datenlöschung

- 10.1 Der Auftragnehmer wird die Auftraggeber-Daten nach Beendigung dieses Vertrages löschen, sofern nicht gesetzlich eine Verpflichtung des Auftragnehmers zur weiteren Speicherung der Auftraggeber-Daten besteht.
- 10.2 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung von Auftraggeber-Daten dienen, dürfen durch den Auftragnehmer auch nach Vertragsende aufbewahrt werden.

11. Nachweise und Überprüfungen

- 11.1 Der Auftragnehmer wird dem Auftraggeber auf dessen Anforderung alle erforderlichen und beim Auftragnehmer vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem Vertrag zur Verfügung stellen.
- 11.2 Der Auftraggeber ist berechtigt, den Auftragnehmer bezüglich der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, zu überprüfen; einschließlich durch Inspektionen.

- 11.3 Zur Durchführung von Inspektionen nach Ziffer 11.2 ist der Auftraggeber berechtigt, im Rahmen der üblichen Geschäftszeiten (montags bis freitags von 9 bis 17 Uhr) nach rechtzeitiger Vorankündigung gemäß Ziffer 11.5 auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers die Geschäftsräume des Auftragnehmers zu betreten, in denen Auftraggeber-Daten verarbeitet werden.
- 11.4 Der Auftragnehmer ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Überprüfungszwecke sind, zu erhalten.
- 11.5 Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Überprüfung zusammenhängenden Umstände zu informieren. Der Auftraggeber darf eine Überprüfung pro Kalenderjahr durchführen. Weitere Überprüfungen erfolgen gegen Kostenerstattung und nach Abstimmung mit dem Auftragnehmer.
- 11.6 Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Überprüfung, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund von dieser Ziffer 11 dieses Vertrags gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber ihm die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Wettbewerber des Auftragnehmers mit der Kontrolle beauftragen.
- 11.7 Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der Pflichten nach diesem Verträge anstatt durch eine Inspektion auch durch die Vorlage eines geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit – z.B. nach BSI-Grundschutz – („Prüfungsbericht“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

12. Vertragsdauer und Kündigung

- 12.1 Die Laufzeit und Kündigung dieses Vertrags richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

13. Haftung

- 13.1 Für die Haftung des Auftragnehmers nach diesem Vertrag gelten die Haftungsausschlüsse und -begrenzungen gemäß dem Hauptvertrag. Soweit Dritte Ansprüche gegen den Auftragnehmer geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftraggebers gegen diesen Vertrag oder gegen eine seiner Pflichten als datenschutzrechtlich Verantwortlicher haben, stellt der Auftraggeber den Auftragnehmer von diesen Ansprüchen auf erstes Anfordern frei.
- 13.2 Der Auftraggeber verpflichtet sich, den Auftragnehmer auch von allen etwaigen Geldbußen, die gegen den Auftragnehmer verhängt werden, in dem Umfang auf erstes Anfordern freizustellen, in dem der Auftraggeber Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

14. Schlussbestimmungen

- 14.1 Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich,

anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und dabei den Anforderungen des Art. 28 DSGVO genügt.

14.2 Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrags vor.

Ort, Datum	Ort, Datum
Auftraggeber	CANEI.tax GmbH & Co. KG (Vormals HAUFE-CANEI GmbH & Co. KG)

Anlagen:

Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

Anlage 2: Weitere Auftragsverarbeiter

Anlage 3: Technische und organisatorische Maßnahmen

Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

Zweck der Datenverarbeitung:	Die Verarbeitung von Daten auf der Basis von insbesondere Summen- und Saldenlisten in der Software Lösung CANEI.tax
Art und Umfang der Datenverarbeitung:	Die Software analysiert auf der Basis dieser Listen die Ertrags-, Vermögens- und Liquiditätslage von Unternehmen und identifiziert steuerliche, betriebswirtschaftliche und Risiko relevante Auffälligkeiten.
Art der Daten:	<ul style="list-style-type: none"> ▪ Name der Systemnutzer ▪ Email-Adresse der Systemnutzer ▪ Telefonnummer der Systemnutzer ▪ Firmierungen der Steuerkanzlei ▪ Eventuell in Summen- und Saldenlisten enthaltene personenbezogene Daten (Namen, Kennzeichen, Kontonummern etc.) ▪ Firmierung der vom Nutzer für die Analyse ausgewählten Mandanten
Kategorien betroffener Personen:	<ul style="list-style-type: none"> ▪ Mitarbeiter/Kunden/Mandanten des Verantwortlichen ▪ Dritte (sofern in den in das System geladenen Summen- und Saldenlisten enthalten)

Anlage 2: Weitere Auftragsverarbeiter

Firma, Anschrift	Anschrift	Leistung
CANEI AG	Phönixseestr. 22a, 44263 Dortmund	Software-Entwicklung und Software-Betrieb
Amazon Web Services, Inc.	410 Terry Avenue North, Seattle WA 98109, United States	Rechenzentrums- und Hosting-Dienstleistungen
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855, Luxemburg	Rechenzentrums- und Hosting-Dienstleistungen

Anlage 3: Technische und organisatorische Maßnahmen (TOM)

1) Zutrittskontrolle

Wie wird das Unternehmensgebäude, in dem die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?

- Das Gebäude verfügt über eine Schließanlage
- Die Schlüsselvergabe an Mitarbeiter wird dokumentiert
- Besucher werden vom Ansprechpartner (oder anderem Personal) in Empfang genommen und beaufsichtigt
- Das Gebäude ist mit einer Alarmanlage ausgestattet

Wie werden in Ihrem Unternehmen die Büroräume, in denen die personenbezogenen Daten verarbeitet werden, vor unbefugtem Zutritt gesichert?

- Türen sind bei Abwesenheit der Mitarbeiter verschlossen
- Fenster sind bei Abwesenheit der Mitarbeiter verschlossen

2) Zugangskontrolle

Welche Vorkehrungen werden bei Ihnen im Unternehmen getroffen, um unberechtigten Zugang zu personenbezogene Daten zu verhindern?

- Die IT-Systeme sind passwortgeschützt
- Jeder meiner Mitarbeiter verfügt über ein eigenes nur ihm bekanntes und von ihm selbst gewähltes Passwort
- Die Nutzung der IT-Systeme wird protokolliert
- Es wird ein Monitoring-System eingesetzt
- Zugriffsberechtigungen und Rollen werden dokumentiert
- Rollen und Zugriffsberechtigungen werden anforderungsgerecht und zeitlich beschränkt vergeben
- Mobile Systeme (Notebook etc.) werden außerhalb der Bürozeiten unter Verschluss gehalten
- Bei Arbeitsunterbrechungen wird ein passwortgeschützter Bildschirmschoner aktiviert
- Es ist ein angemessener Virenschutz vorhanden
- Die IT-System/Nutzer Passwörter werden gesichert aufbewahrt
- Netzwerke werden ihrer Schutzbedürftigkeit nach eingeteilt
- Es wird eine sichere Übertragungstechnik verwendet (VPN)
- Es gilt das Prinzip der Minimalberechtigung. Jeder Benutzer erhält nur die Zugriffsrechte, die erforderlich sind, um seine vertraglichen Tätigkeiten durchzuführen.

Welche Anforderungen werden an die Komplexität von Passwörtern gestellt?

- Die Passwörter sind aus Zahlen, Buchstaben und Zeichen zusammengesetzt
- Die Passwörter müssen eine Mindestlänge aufweisen
- Trivialpasswörter werden nicht akzeptiert

Wie wird gewährleistet, dass der Benutzer sein Passwort regelmäßig ändert und es zu keiner Wiederholung der Passwörter kommt?

- Der Nutzer kann sein Passwort jederzeit selbst ändern

Welche Maßnahmen werden bei gescheiterten Anmeldeversuchen ergriffen?

- Bei 3-maliger Falscheingabe des Passworts erfolgt eine automatische Sperrung des IT-Systems

3) Zugriffskontrolle

Wie stellen Sie eine differenzierte Zugriffsberechtigung bei den verschiedenen Mitarbeitern des Unternehmens sicher?

- Es gibt ein Berechtigungskonzept
- Alle Mitarbeiter besitzen verschiedene Passwörter
- Bestimmte Berechtigungen werden durch eine Genehmigung erteilt

Wie wird sichergestellt, dass der Zugriff auf Datenträger wie USB-Sticks, Festplatten oder auch einfache Papierblätter ausschließlich durch berechtigte Personen erfolgt?

- Ausdrucke mit personenbezogenen Daten werden unmittelbar nach dem Ausdruck aus dem Drucker entnommen
- Datenträger werden in verschließbaren Schränken aufbewahrt
- Einzelne Dateien/Daten sind auf den IT-Systemen verschlüsselt
- Es ist ein angemessener Virenschutz vorhanden

Wie erfolgt die Kontrolle der Zugriffsberechtigungen?

- Unser Unternehmen besitzt ein Berechtigungskonzept

4) Weitergabekontrolle

Wie gewährleisten Sie die Integrität und Vertraulichkeit bei der Weitergabe von personenbezogenen Daten?

- Daten werden nur weitergegeben nach einer Prüfung der Rechtslage
- Nur ein bestimmter Personenkreis ist zur Weitergabe berechtigt
- Beim Verschicken personenbezogener Daten per Briefpost werden Sichtgeschützte Umschläge verwendet
- Die interne E-Mail-Kommunikation erfolgt über eine unternehmenseigene Domain
- Datenträger sind verschlüsselt
- Daten auf dem Datenträger sind verschlüsselt

Wie wird die Weitergabe von personenbezogenen Daten kontrolliert?

- Die Weitergabe personenbezogener Daten wird protokolliert

5) Verfügbarkeitskontrolle

Welche Maßnahmen werden getroffen, um auch im Schadensfall die Verfügbarkeit von Daten und Systemen schnellstmöglich zu gewährleisten?

- In regelmäßigen Zeitabständen werden Datensicherungen durchgeführt
- Es werden Protokolle geführt wann welche Daten gesichert wurden
- In unserem Unternehmen wird eine unterbrechungsfreie Stromversorgung sichergestellt
- Wir nutzen AWS (Amazon Web Services) als Hosting Partner. AWS ist nach DIN ISO 27001 zertifiziert.

Wie wird gewährleistet, dass die Datenträger vor Umwelteinflüssen (Feuer, Wasser etc.) geschützt sind?

- Das Gebäude und die Arbeitsräume sind mit Rauch- und Feuermeldern ausgestattet
- Serverräume sind Feuchtigkeitssensoren installiert
- Wichtige Räumlichkeiten sind mit Brandschutztüren ausgestattet
- Wir nutzen AWS (Amazon Web Services) und deren Rechenzentren in Frankfurt am Main als Hosting Partner. AWS ist nach DIN ISO 27001 zertifiziert.

Welche Schutzmaßnahmen werden zur Bekämpfung von Schadprogrammen eingesetzt und wie wird deren Aktualität gewährleistet?

- Virens Scanner
- Spam-Filter
- Anti-Spy-Programme - Firewalls

Wie wird gewährleistet, dass nicht mehr benötigte bzw. defekte Datenträger ordnungsgemäß entsorgt werden?

- Datenträger werden zur Entsorgung immer an die IT-Abteilung abgegeben

6) Auftragskontrolle in Zusammenhang mit der Auftragsverarbeitung

Welche Maßnahmen werden ergriffen, damit die Verarbeitung der personenbezogenen Daten durch die damit betrauten Mitarbeiter nur gemäß den Weisungen des Auftraggebers erfolgen kann?

- Es erfolgt eine Angebots- und Auftragsbestätigung
- Die Mitarbeiter werden auf die Verpflichtung zum Datengeheimnis hingewiesen

Welche Maßnahmen werden getroffen, damit auch ggf. Unterauftragnehmer keine unbefugten Aktivitäten mit den zur Verfügung gestellten Daten durchführt?

- Unterauftragnehmer werden sorgfältig ausgewählt
- Unterauftragnehmer werden vertraglich zur Einhaltung der DS-GVO verpflichtet
- Mit Unterauftragnehmern sind entsprechende vertragliche Vereinbarungen (z.B. Verträge zur Auftragsverarbeitung) geschlossen.

Werden Maßnahmen getroffen, die am Ende des Aufbewahrungszwecks der personenbezogenen Daten deren Löschung/Sperrung sicherstellen?

- Unterauftragnehmer werden sorgfältig ausgewählt
- Unterauftragnehmer werden vertraglich zur Löschung/Sperrung verpflichtet