

Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 DS-GVO

zwischen

Firma

Vertreten durch (Vorname, Name)

Straße, Hausnummer

PLZ, Sitz

- Verantwortlicher - nachstehend **Auftraggeber** genannt -

und

**e.Consult AG, vertreten durch den Vorstand, Dominik Bach-Michaelis,
Neugrabenweg 1, 66123 Saarbrücken**

- Auftragsverarbeiter - nachstehend **Auftragnehmer** genannt

Präambel

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten. Er basiert auf einem Muster des Bayerischen Landesamts für Datenschutzaufsicht.

Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

1. Gegenstand und Dauer des Auftrags

Der Auftrag umfasst Folgendes:

Der Auftragnehmer verarbeitet beim Betreiben der WebAkte personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages. Der Gegenstand des Auftrags ergibt sich aus dem zwischen den Parteien bestehenden Servicevertrag, auf den hier verwiesen wird (im Folgenden Hauptvertrag genannt) sowie aus etwaigen Einzelweisungen.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu 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).

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrages. Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

Der Auftragnehmer stellt dem Auftraggeber nach Maßgabe des Hauptvertrages und der Nutzungsbedingungen eine Plattform für den Dokumentenaustausch über das Internet zur Verfügung. Dabei verarbeitet der Auftragnehmer ausschließlich Daten, die der Auftraggeber oder sonstige autorisierte Nutzer in die WebAkte einbringen. Sämtliche in die WebAkte eingebrachten Daten werden entweder vom Auftraggeber oder nach dessen Weisung erhoben.

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Der Auftragnehmer verwendet die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

Art der Verarbeitung (Art. 4 Nr. 2 DS-GVO)

Die regelmäßige Verarbeitung besteht im Erheben, Erfassen, Organisieren, Ordnen, Speichern, Bereitstellen sowie dem Einschränken und Löschen von Daten

Art der personenbezogenen Daten (Art. 4 Nr. 1, 13, 14 und 15 DSGVO)

Verarbeitete Daten sind Kommunikationsinhalte und Metadaten, wie Namen und E-Mail-Adressen von Nutzern, soweit dies für das Funktionieren der Anwendung unumgänglich ist.

Kategorien betroffener Personen (Art. 4 Nr. 1 DS-GVO)

Kunden (z. B. Anwälte, Steuerberater, Wirtschaftsprüfer) und deren Beschäftigte, Kommunikationspartner (z. B. Mandanten, Beschäftigte von Versicherungen), sonstige Personen, auf die sich die Kommunikation beziehen kann (z. B. Gegner)

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

Weisungen des Auftraggebers sind nur beachtlich, wenn sie von einem Weisungsberechtigten an einen empfangsberechtigten Adressaten beim Auftragnehmer gerichtet werden.

<p>Weisungsberechtigte Personen (Vorname, Name, Organisationseinheit, Telefon) des Auftraggebers sind (mangels konkreter Angabe nur der im Rubrum dieser Vereinbarung aufgeführte Auftraggeber persönlich (ggf. gesetzlicher Vertreter)</p>
<p>Weisungsempfänger beim Auftragnehmer sind (Vorname, Name, Organisationseinheit, Telefon):</p> <p>Mitarbeiter des e.Consult AG – Support (verantwortlich: Leiter des Supports)</p>
<p>Für Weisung zu nutzende Kommunikationskanäle (postalische Adresse/ E-Mail/ Telefonnummer):</p> <ul style="list-style-type: none"> • unter der im Rubrum genannten Postadresse mit dem Zusatz „Support“ • telefonisch unter 0681 9508280 • per E-Mail unter support@e-consult.de

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen.

Mündliche Weisungen bestätigt der Auftraggeber unverzüglich zumindest in Textform.

Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5. Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind.

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Falls dem Auftragnehmer Datenträger überlassen werden, werden diese, sofern sie vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber insbesondere folgende Überprüfungen in seinem Bereich durchzuführen:

Jährliche Prüfung durch den betrieblichen Datenschutzbeauftragten hinsichtlich aller ergriffenen technischen und organisatorischen Maßnahmen. Externe Auditierung. Umsetzung einer regelmäßigen Evaluierung, Bewertung und Verbesserung, regelmäßige Kontrolle der Subunternehmer. Das Ergebnis der Kontrollen ist zu dokumentieren. Der Auditbericht des Datenschutzbeauftragten und Zertifizierungsergebnisse werden dem Auftraggeber auf Verlangen vorgelegt.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an folgende Stelle des Auftraggebers weiterzuleiten:

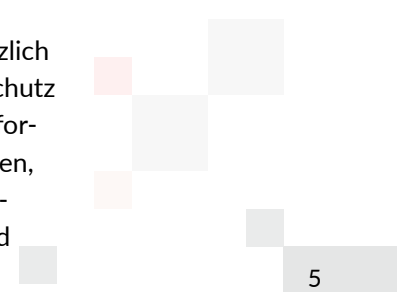
<i>Mangels konkreter Angabe nur der im Rubrum dieser Vereinbarung aufgeführte Auftraggeber persönlich (ggf. gesetzlicher Vertreter)</i>

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber – grundsätzlich nach Terminvereinbarung – berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO).



Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DS-GVO sind auch in diesem Fall sicherzustellen.

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind. Er verpflichtet sich, auch folgende für diesen Auftrag relevanten **Geheimnisschutzregeln** zu beachten, die dem Auftraggeber obliegen:

Der Auftragnehmer wirkt ggf. an der beruflichen Tätigkeit des Auftraggebers, der **einer beruflichen Verschwiegenheitsverpflichtung** unterliegt, mit. Der Auftragnehmer wahrt in Kenntnis der strafrechtlichen Folgen einer Verletzung der Verschwiegenheitspflicht gemäß § 203 StGB (Freiheitsstrafe bis zu einem Jahr oder Geldstrafe) und den sonst anwendbaren rechtlichen Vorschriften fremde Geheimnisse, die ihr vom Auftraggeber als Berufsträger zugänglich gemacht werden.

Der Auftragnehmer verpflichtet sich, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist.

Der Auftragnehmer ist berechtigt, Dritte zur Vertragserfüllung heranzuziehen. Beim Einsatz von Dritten verpflichtet sich der Auftragnehmer, diese unter Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung zur Verschwiegenheit zu verpflichten, soweit diese im Rahmen ihrer Tätigkeit Kenntnis von fremden Geheimnissen erlangen könnten. Mitarbeiter des Auftragnehmers, die Kenntnis von fremden Geheimnissen erlangen könnten, wurden schriftlich oder in Textform zur Verschwiegenheit verpflichtet.

Bei der Inanspruchnahme von Dienstleistungen, die unmittelbar einem einzelnen Mandat dienen, ist der Auftraggeber verpflichtet, die Einwilligung des Mandanten in die Zugänglichmachung von fremden Geheimnissen im Sinne dieser Zusatzvereinbarung einzuholen.

Die Pflicht zur Verschwiegenheit gemäß den vorstehenden Absätzen besteht nicht, soweit der Auftragnehmer aufgrund einer behördlichen oder gerichtlichen Entscheidung zur Offenlegung von vertraulichen Informationen des Auftraggebers verpflichtet ist. Soweit dies im Einzelfall zulässig und möglich ist, wird der Auftragnehmer den Auftraggeber über die Pflicht zu Offenlegung vorab in Kenntnis setzen.

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Beim Auftragnehmer ist als Beauftragter für den Datenschutz bestellt:

RA Stefan Wiesen, externer bDSB, 0681 – 685 704 01, datenschutz@ra-wiesen.de

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

Der Auftragnehmer verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DS-GVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DS-GVO unverzüglich zu informieren.

6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DS-GVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) wie folgt zu überprüfen:

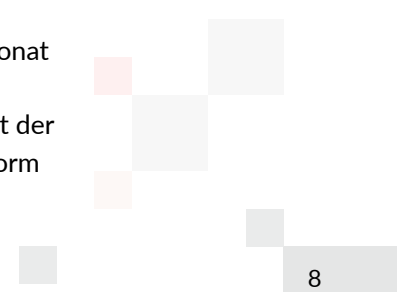
Nach Vertragsschluss erfolgen regelmäßig Folgekontrollen, und zwar grundsätzlich jährlich. Ausgenommen davon sind umfassend zertifizierte Subunternehmer, deren Kontrolle im Wesentlichen auf der Grundlage eines externen Gutachtens durchgeführt werden kann. Die Kontrolle durch den Auftragnehmer erfolgt in diesem Fall synchron zur Laufzeit der Zertifizierung. Kontrollen werden im Übrigen durch (vom Subunternehmen zu belegenden) Selbstauskünfte des Subunternehmens auf der Grundlage von Fragebögen des Auftragnehmers durchgeführt, darüber hinaus auch durch Vor-Ort-Kontrollen.

Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Zurzeit sind für den Auftragnehmer die in **Anlage Unterauftragnehmer** mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden. Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO).

Die Information hinsichtlich einer beabsichtigten Änderung erfolgt spätestens einen Monat vor dem Zeitpunkt der geplanten Übergabe der Daten schriftlich oder in Textform. Die Änderung ist zulässig, wenn der Auftraggeber nicht bis zwei Wochen vor dem Zeitpunkt der geplanten Übergabe der Daten dem Auftragnehmer gegenüber schriftlich oder in Textform Einspruch erhebt.



Im Falle des Einspruchs steht dem Auftragnehmer ein außerordentliches Kündigungsrecht sowohl hinsichtlich dieser Vereinbarung als auch bezüglich des Hauptvertrages zu. Ansprüche des Auftraggebers auf Schadenersatz sind ausgeschlossen.

8. Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

Für die auftragsgemäße Verarbeitung personenbezogener Daten wird folgende Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt:

Anhand der „Richtlinie der e.Consult AG für Datenschutz-Risikobewertung“ identifiziert der Auftragnehmer aus den generellen Risikoquellen die relevanten Bedrohungen (Möglichkeit, dass ein Schaden entsteht) für Vertraulichkeit, Integrität und Verfügbarkeit (Belastbarkeit). Die Einschätzung der Schwere der Auswirkung erfolgt anhand einer (vierstufigen) Einstufungstabelle. Besonders wegen der Möglichkeit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten, wird ein hoher Schutzbedarf angenommen. Die Eintrittswahrscheinlichkeit wird im Hinblick auf nichtmenschliche Risikoquellen als vernachlässigbar eingestuft, im Hinblick auf menschliche Risikoquellen (insbesondere Hackerangriff, Fehlbedienungen, nicht ordnungsgemäß angelegte Zugänge und Zugriffsrechte, Manipulation, Sabotage) als vernachlässigbar bis eingeschränkt.

Das in der **Anlage TOM** beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

Das in der Anlage beschriebene Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung wird als verbindlich festgelegt.

Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber auf Anforderung mitzuteilen.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.

Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

9. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzgerecht zu löschen. Die Löschung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

10. Vergütung

Für das Ermöglichen von aufwendigen, insbesondere Vor-Ort-Kontrollen durch den Auftraggeber, kann der Auftragnehmer eine angemessene Vergütung beanspruchen. Vorgehaltene Dokumentationen, wie Datenschutz- und Informationssicherheitskonzepte, Zertifizierungsurkunden, werden vom Auftragnehmer kostenfrei zur Verfügung gestellt.

11. Haftung

Die Haftung des Auftragnehmers ist beschränkt auf Fälle, in denen er, seine Mitarbeiter, Erfüllungsgehilfen oder ein weiterer Auftragsverarbeiter schuldhaft seinen speziell auferlegten Pflichten aus der DS-GVO nicht nachgekommen ist oder er erteilte Weisungen des Auftraggebers nicht beachtet hat oder Weisungen des Auftraggebers zuwidergehandelt hat.

Der Auftragnehmer ist von der Haftung befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

Sind sowohl Auftraggeber als auch Auftragnehmer für einen Schaden verantwortlich, der bei gemeinsamer Beteiligung an einer Verarbeitung entstanden ist, so haften beide der betroffenen Person gegenüber als Gesamtschuldner; sie haften im Innenverhältnis entsprechend ihrem Anteil an der Verantwortung für den Schaden.

12. Sonstige Regelungen


Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

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

	 <p>e.Consult® Aktiengesellschaft Neugrabenweg 1 66123 Saarbrücken Tel.: 06 81 / 950 82 80 Fax: 06 81 / 950 82 81 service@e-consult.de www.e-consult.de (e.Consult AG)</p>
Auftraggeber	e.Consult AG
durch	durch Dominik Bach-Michaelis

Anlage Unterauftragnehmer

Der Auftraggeber stimmt folgenden Unterauftragnehmern zu:

Name	Anschrift/Land	Leistung
DATEV eG	Paumgartnerstr. 6 – 14, 90429 Nürnberg / Deutschland	Rechenzentrum
Schuster & Walther IT-Business GmbH	Schwabacher Straße 3 90439 Nürnberg	Hosting Unterstützung
Schuster & Walther IT-Kanzlei GmbH	Schwabacher Straße 3 90439 Nürnberg	Hosting Unterstützung

Anlage TOM

Kurzdarstellung der technischen und organisatorischen Maßnahmen (WebAkte 02/18)

Vertraulichkeit

Zutrittskontrolle (kein unbefugter Zutritt zu Datenverarbeitungsanlagen)

Die Verarbeitung der beim Betrieb der Anwendung WebAkte erhobenen Daten erfolgt ausschließlich in einem Hochsicherheits-Rechenzentrum, welches über eine lückenlose Außenüberwachung und eine Sicherheitszentrale sowie einen Betriebsschutz verfügt. Der Zutritt ist nur über Schleusen mit SmartCard-Buchungsstellen möglich.

Der Unternehmensstandort verfügt über ein elektronisches Zutrittskontrollsystem und Alarmanlage.

Zugangskontrolle (Keine unbefugte Systembenutzung)

Die zur Administrierung der Server verwendeten Clientsysteme sind nur bei passwortgestützter Authentifizierung nutzbar; der Transfer erfolgt über verschlüsselte VPN-Verbindung.

Zugriffskontrolle (Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems)

Die Anzahl der Administratoren ist auf das Notwendigste beschränkt. Zugriffe sind nur nach Authentisierung auf Betriebssystemebene und separat auf Anwendungsebene möglich. Eine Firewall gegen unberechtigte Zugriffe ist eingerichtet. Zugriffe bzw. Zugriffsversuche werden überwacht und protokolliert.

Trennungsgebot (Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden)

Die verwendeten Berechtigungsmechanismen ermöglichen die exakte Umsetzung der Vorgaben des Berechtigungskonzepts. Trennung von Produktiv- und Testsystemen ist gewährleistet.

Pseudonymisierung

Übertragung von Daten an und von WebAkte erfolgt stets ohne erkennbaren Personenbezug durch 256 Bit ssl- bzw. tls-Verschlüsselung (Symantec).

Integrität

Weitergabekontrolle (Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport)

Übertragung und Abruf von Daten durch Kunden und berechnigte Nutzer in die bzw. aus der Anwendung erfolgt über mindestens tls-verschlüsselte Verbindungen.

Eingabekontrolle (Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind)

Eingaben sind durch individuelle Benutzernamen nachvollziehbar. Eingabe-, Änderungs- und Löschbefugnisse erfolgen auf der Grundlage des Berechnigungskonzepts. Administrati-onstätigkeiten werden protokolliert (mit einer Aufbewahrungsfrist von 18 Monaten).

Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle (Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust)

Ausweichrechenzentren mit einsatzbereiten Zwillingsystemen sind ständig verfügbar. Über ein vollständiges Backup- und Recovery-Konzept werden Daten täglich gesichert und Datenträger katastrophensicher aufbewahrt. Es werden Schutzprogramme (Virens Scanner, Firewalls, Verschlüsselungsprogramme, Spam-Filter) sachkundig und effizient eingesetzt.

Rasche Wiederherstellbarkeit

Infrastruktur und Daten sowie Datensicherung werden mehrfach vorgehalten.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutzmanagement

Es ist ein Datenschutzbeauftragter bestellt. Alle Mitarbeiter sind auf Datengeheimnis und Vertraulichkeit verpflichtet. Verantwortlichkeiten und Zuständigkeiten sind verbindlich geregelt. Die Umsetzung wird über eine Leitlinie zu Informationssicherheit und Datenschutz, Sicherheits- und Datenschutzrichtlinien und -verfahren gesteuert. Ein Prozess zur kontinuierlichen Verbesserung ist etabliert.

Zertifizierung

Es erfolgt eine jährliche Kontrolle und Überprüfung hinsichtlich der getroffenen Sicherheitsmaßnahmen durch TÜV Süd basierend auf ISO/IEC 25051:2014 / PPP 13011:2008.

Auftragskontrolle

Daten werden nur aufgrund dokumentierter Weisungen durch autorisierte Mitarbeiter an autorisierte Weisungsempfänger verarbeitet.

Das Rechenzentrum als Subunternehmer ist gemäß DQS Gütesiegel Datenschutz sowie ISO/IEC 27001:2013 zertifiziert und wird regelmäßig kontrolliert hinsichtlich der getroffenen Sicherheitsmaßnahmen.

*Wegen weiterer Informationen zum Thema fordern Sie gerne das ausführliche **Datenschutz- und Informationssicherheitskonzept** der e.Consult AG unter support@e-consult.de an.*