Vereinbarung zur Auftragsverarbeitung

für ein Servicepaket on Fabasoft PROCECO

Gültig ab 1. Januar 2024
Öffentlich

Aus Gründen der einfacheren Lesbarkeit wird auf die geschlechtsspezifische Differenzierung, z. B. Benutzer/-innen, verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für beide Geschlechter.

Vertragspartner

Diese Vereinbarung zur Auftragsverarbeitung wird abgeschlossen zwischen den Vertragsparteien gemäß Informationsblatt CSA.

1. Vorbemerkungen und Verpflichtung zur Einhaltung

1.1. Die nachfolgenden Bestimmungen finden Anwendung auf alle Leistungen der Auftragsverarbeitung iSd. Art. 28 Datenschutzgrundverordnung (EU) 2016/679 (im Folgenden „DSGVO“) bzw. den jeweiligen nationalen Vorschriften, die der Auftragnehmer gegenüber dem Auftraggeber (im Folgenden auch Kunden) erbringt. Dies umfasst alle Tätigkeiten, die mit dieser Vereinbarung in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Kunden in Berührung kommen können.

1.2. Der Kunde und der Auftragnehmer verpflichten sich bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze.

1.3. Nicht ausdrücklich definierte Begriffe in dieser Vereinbarung unterliegen der Definition gemäß DSGVO.

2. Gegenstand/Dauer des Auftrags; Umfang/Art/Zweck der Datenverarbeitung, Datenarten und der Kreis der Betroffenen

2.1. Der Auftragnehmer wird nach Maßgabe der DSGVO bzw. der nationalen Vorschriften, gemäß des zwischen den Parteien geschlossenen Cloud Service Agreement (nachfolgend „Hauptvertrag“), sowie gemäß den Bestimmungen dieser Vereinbarung personenbezogene Daten im Auftrag und nach schriftlicher dokumentierter Weisung des Kunden verarbeiten.

Die letztaktuelle Fassung des Hauptvertrags ist online abrufbar unter der im Informationsblatt CSA angegebenen Website „Link zu Vertragsgrundlagen“.

Die umfassten Tätigkeiten, sowie Umfang und Art der Auftragsverarbeitung, sind entweder in der Leistungsbeschreibung des Hauptvertrags konkretisiert oder ergeben sich aus einer nachträglich erteilten Weisung durch den Kunden.

2.2. Der Kunde ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Zulässigkeit der Datenverarbeitung und Datennutzung im Rahmen dieser Vereinbarung, sowie für die Wahrung der Rechte der Betroffenen alleinverantwortlich. Es obliegt dem Kunden eigenverantwortlich, die Betroffenen darauf hinzuweisen, dass ihre Daten erhoben, verarbeitet und genutzt werden und zu welchem Zweck dies erfolgt. Der Kunde wird dafür Sorge tragen, dass die Betroffenen auf etwaige Widerrufsmöglichkeiten hingewiesen werden.

2.3. Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Hauptvertrags. Wird der Hauptvertrag gekündigt, endet auch diese Vereinbarung zur Auftragsverarbeitung automatisch mit dessen Beendigung, ohne dass es seiner gesonderten Kündigung bedarf. Das Datengeheimnis besteht auch nach Beendigung dieser Vereinbarung, gleich aus welchem Rechtsgrund, fort.

2.4. Der Auftragnehmer verarbeitet folgende personenbezogene Daten im Auftrag des Kunden:

a) Kontaktdaten des Kunden.
b) Die Benutzerdaten des Kunden bleiben ausschließlich in der Verfügungsmacht des Kunden und sind dem Auftragnehmer weder bekannt, noch unterliegen sie seinem Zugriff.

Die Definition, sowie die Unterschiede zwischen Kontaktdaten und Benutzerdaten sind in Punkt 4 der „Leistungsmerkmale Datensicherheit“ dargestellt.

2.5. Zweck der Auftragsverarbeitung ist die Erfüllung der in der Leistungsbeschreibung des Hauptvertrages konkretisierten Tätigkeiten oder der Weisungen des Kunden durch den Auftragnehmer.

Aus Sicht des Kunden sind Kategorien betroffener Personen dessen Kunden, Interessenten, Mitarbeiter, Bewerber, Lieferanten, Vertragspartner, sowie alle darüber hinaus vom Kunden zur Cloud berechtigte Personen, deren Kontaktdaten verarbeitet werden.

2.6. Die Auftragsverarbeitung der Daten findet ausschließlich in Deutschland, Österreich und der Schweiz statt.

Die letztaktuelle Fassung der Leistungsmerkmale Rechenzentrumsbetrieb ist online abrufbar unter der im Informationsblatt CSA angegebenen Website „Link zu Vertragsgrundlagen“.

2.7. Aufgrund dieser Verantwortlichkeit ermöglicht es der Auftragnehmer dem Kunden, während der Laufzeit der Vereinbarung die Berichtigung, Einschränkung, Löschung und Herausgabe von Daten selbst durchzuführen. Betroffenenrechte sind vom Kunden wahrzunehmen. Soweit eine Mitwirkung vom Auftragnehmer für die Wahrung von Betroffenenrechten (insbesondere auf Auskunft, Berichtigung oder Löschung) durch den Kunden erforderlich ist, verpflichtet sich der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Kunden unverzüglich zu treffen.

3. Technischen und organisatorischen Maßnahmen

3.1. Der Auftragnehmer muss geeignete technische und organisatorische Maßnahmen iSd. Art 32 DSGVO zur Gewährleistung eines angemessenen Datenschutzniveaus setzen. Der Auftragnehmer wird die innerbetriebliche Organisation derart gestalten, dass die Umsetzung und Einhaltung der besonderen Anforderungen des Kunden und der DSGVO bzw. der nationalen Vorschriften gegeben ist. Die letztaktuelle Fassung der Leistungsmerkmale Datensicherheit ist online abrufbar unter der im Informationsblatt CSA angegebenen Website „Link zu Vertragsgrundlagen“ .

3.2. Der Auftragnehmer verpflichtet sich keinem Dritten

a) direkten, indirekten, umfassenden oder uneingeschränkten Zugriff auf Daten oder
b) zur Sicherung von Daten verwendete Verschlüsselungsschlüssel oder die Möglichkeit, eine solche Verschlüsselung zu umgehen,

zu geben.

3.3. Die letztaktuelle Fassung der „Technischen und organisatorischen Maßnahmen“ ist online abrufbar unter der im Informationsblatt CSA angegebenen Website „Link zu Vertragsgrundlagen“. Darin sind alle technischen und organisatorischen Maßnahmen, die der Auftragnehmer zu erfüllen hat, dem Grunde nach dargestellt. Mit Erteilung des Auftrags

gelten die technischen und organisatorischen Maßnahmen als vom Kunden geprüft und genehmigt.

3.4. Die Dokumente „Leistungsmerkmale Datensicherheit“, „Leistungsmerkmale Rechenzentrumsbetrieb“ und „Technische und organisatorische Maßnahmen“ bilden das Datenschutz- und Datensicherheitskonzept dem Grunde nach ab. Der Auftragnehmer ist verpflichtet, dieses Datenschutz- und Datensicherheitskonzept zu evaluieren, sowie zu aktualisieren, wobei Änderungen in sinngemäßer Anwendung der Bestimmungen des Hauptvertrags mit dem Kunden vorgenommen werden.

3.5. Nachweise können auch durch Vorlage von Testaten oder Berichten unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, akkreditierte Prüfstellen, Datenschutzbeauftragte, IT-Sicherheitsexperten) oder eine geeignete Zertifizierung erbracht werden.

4. Weisungen des Kunden

4.1. Der Kunde hat das Recht, in Textform oder mündlich Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Mündliche Weisungen wird der Kunde unverzüglich in Textform bestätigen. Ausschließlich schriftliche Weisungen sind für den Auftragnehmer verbindlich.

Sofern eine Weisung nicht in der erforderlichen Form vom Kunden erteilt wird, wird der Auftragnehmer den Kunden darüber informieren

4.2. Der Kunde teilt dem Auftragnehmer unter Angabe von Name, Organisationseinheit, Funktion und Telefonnummer die Personen mit, die gegenüber dem Auftragnehmer weisungsberechtigt sind oder als Ansprechpartner fungieren. Änderungen werden dem Auftragnehmer unverzüglich in Textform mitgeteilt.

4.3. Der Kunde wird sich vor Beginn der Auftragsverarbeitung von der Einhaltung der technischen und organisatorischen Maßnahmen vom Auftragnehmer zur Datensicherheit überzeugen. Der Kunde informiert den Auftragnehmer, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Anforderungen des Kunden und/oder datenschutzrechtlichen Vorschriften feststellt.

4.4. Erteilt der Kunde Weisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die damit verbundenen Kosten und Aufwendungen vom Kunden zu tragen.

5. Pflichten des Auftragnehmers; Datengeheimnis

5.1. Der Auftragnehmer verpflichtet sich, ausschließlich aufgrund der Leistungsbeschreibung im Hauptvertrag, der schriftlich dokumentierten Weisungen des Kunden und der gegenständlichen Vereinbarung personenbezogene Daten des Kunden zu verarbeiten oder zu nutzen.

5.2. Die Vertragsparteien verpflichten sich, über nicht allgemein bekannte, geschäftlich relevante und bedeutsame Angelegenheiten des jeweiligen Vertragspartners (Geschäftsgeheimnisse) Verschwiegenheit zu wahren. Der Auftragnehmer hat bei der Speicherung der Daten des Kunden das Datengeheimnis gemäß den nationalen Vorschriften bzw. der DSGVO zu wahren.

5.3. Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der personenbezogenen Daten des Kunden befassten Mitarbeiter bei der Aufnahme ihrer Tätigkeit gemäß den nationalen Vorschriften bzw. der DSGVO auf das Datengeheimnis – auch für die Zeit nach Beendigung dieser Vereinbarung – verpflichtet wurden und in die geltenden Datenschutzbestimmungen eingewiesen wurden.

5.4. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Kunden in Textform erteilen.

5.5. Die Pflicht zur Führung eines Verzeichnisses über Verarbeitungstätigkeiten nach Art. 30 Abs 1 DSGVO bzw. der nationalen Vorschriften liegt beim Kunden. Der Auftragnehmer wird ihn hierbei unterstützen. Der Auftragnehmer hat ein eigenes Verzeichnis über Verarbeitungstätigkeiten nach Art. 30 Abs 2 DSGVO zu führen und dieses auf Anfrage dem Kunden auszuhändigen. Der Auftragnehmer wird den Kunden bei seiner Verantwortung in Hinblick auf eine allenfalls durchzuführende Datenschutzfolgenabschätzung und Konsultation mit den Aufsichtsbehörden, unterstützen.

5.6. Der Auftragnehmer informiert den Kunden unverzüglich über Kontrollhandlungen; Ermittlungen und Maßnahmen der datenschutzrechtlichen Aufsichtsbehörde.

Insoweit der Auftragnehmer aufgrund einer gesetzlichen Verpflichtung oder im Zuge eines rechtlichen Verfahrens vor Gericht oder einer sonstigen staatlichen Autorität verpflichtet wird, beim Auftragnehmer vom Kunden gespeicherte Daten dem Gericht oder der sonstigen staatlichen Autorität zugänglich zu machen, geht der Auftragnehmer folgendermaßen vor:

I. Staatliche Auskunftsersuchen, werden vor Entsprechung, auf deren Legalität hin durch dafür qualifizierte Personen juristisch eingehend geprüft.
- Sofern der Auftragnehmer dadurch keine Gesetze verletzt, wird der Auftragnehmer den Kunden hievon so rasch als möglich (elektronisch) verständigen, um dem Kunden dadurch die Möglichkeit zu verschaffen, gegen die Zugänglichmachung der Daten insbesondere rechtliche Schutzmaßnahmen auf eigene Kosten zu versuchen.
- Der Auftragnehmer wird den Zugriff nur nach positiv abgeschlossener Prüfung (vgl. Punkt i.) zulassen und mit dem Kunden, soweit rechtlich möglich, kooperieren, um dessen Datenschutzinteresse zu unterstützen.

II. Der Auftragnehmer wird, soweit mit verhältnismäßigen Mitteln möglich, nur Zugriff auf vom Auskunftsersuchen umfasste Daten erlauben. Hierbei ist der Auftragnehmer auf die Unterstützung des Kunden zwingend angewiesen, um erheben zu können, welche Daten vom Auskunftsersuchen umfasst sind und welche nicht, da dem Auftragnehmer die im Servicepaket gespeicherten Daten nicht bekannt sind.

5.7. Der Auftragnehmer verpflichtet sich die Einhaltung der datenschutzrechtlichen Bestimmungen in ihrem Verantwortungsbereich regelmäßig zu kontrollieren und gegebenenfalls erforderliche Anpassungen von Regelungen und/oder Maßnahmen zur ordnungsgemäßen Auftragsverarbeitung vorzunehmen. Sofern der Auftragnehmer eine Weisung des Kunden als rechtswidrig erachtet, hat sie den Kunden unverzüglich zu informieren.

5.8. Der Auftragnehmer verfügt über ein mit datenschutz-rechtlichen Themen betrautes Datensicherheits-Team („Privacy Team“). Die Kontaktdaten dieses Privacy Teams sind unter der im Informationsblatt CSA angegebenen Website „Weitere hilfreiche Links“, „Privacy Website“ aktuell gehalten. Das Privacy-Team kann unter der im Informationsblatt CSA unter „Kontaktmöglichkeiten“, „Datenschutz“ angegebenen E-Mail-Adresse kontaktiert werden.

Soweit von der DSGVO bzw. den nationalen Vorschriften vorgeschrieben, wird der Auftragnehmer einen Datenschutzbeauftragten bestellen. Die Kontaktdaten dieses Datenschutzbeauftragen sind unter der im Informationsblatt CSA angegebenen Website „Weitere hilfreiche Links“, „Privacy Website“ aktuell gehalten.

5.9. Der Auftragnehmer verpflichtet sich, dem Kunden auf Anfrage innerhalb eines angemessenen Zeitraums die Informationen bereitzustellen, die der Kunde zur Ausübung der umfassenden Kontrolle des Auftrags als erforderlich erachtet.

5.10. Sämtliche Beschwerden oder Unklarheiten im Zusammenhang mit dem Service Paket können über folgende Kanäle geltend gemacht werden:

- Per E-Mail: „Kontaktmöglichkeiten“, „Datenschutz“ gemäß Informationsblatt CSA
- Per Post: Sitz des Auftragnehmers gemäß Informationsblatt CSA

Sämtliche Beschwerde sind gegenüber dem Auftragnehmer schriftlich anzubringen. Um einen Missbrauch durch Unberechtigte zu verhindern, muss gegenüber dem Auftragnehmer die Identität des Beschwerdeführers in geeigneter Form nachgewiesen werden.

Fabasoft AG ist Gründungsmitglied der Generalversammlung des europäischen Cloud Code of Conduct („CoC“) und gestaltet daher seine Vertragswerke entsprechend den hohen Standards des CoC. Fabasoft AG gibt diesbezüglich regelmäßig eine Unterwerfungserklärung zu der jeweiligen letztaktuellen und gültigen Fassung des CoC ab. Diesbezüglich können Beschwerden ebenfalls beim Monitoring Body des CoC unter dem Link https://eucoc.cloud/en/public-register/complaints/ erhoben werden.

6. Sub-Auftragsverarbeiter

6.1. Der Auftragnehmer ist nach den nachfolgenden Bestimmungen berechtigt, Sub-Auftragsverarbeiter zu beauftragen oder bereits beauftragte zu ersetzen.

Der Auftragnehmer beauftragt nur jene Sub-Auftragsverarbeiter, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den anwendbaren Datenschutzbestimmungen erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Der Auftragnehmer kann sich über die Einhaltung der Datenschutzbestimmungen vor Ort unter rechtzeitiger Ankündigung überzeugen.

Als Sub-Auftragsverhältnisse 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 oder die Entsorgung von Datenträgern in Anspruch nimmt sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Kunden auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

Der Auftragnehmer wird eine beabsichtigte Subbeauftragung oder den Wechsel eines Sub-Auftragsverarbeiters dem Kunden unverzüglich bekanntgeben. Dem Kunden wird sodann eine 14-tägige Frist zum Widerspruch eingeräumt. Erfolgt innerhalb von 14 Tagen kein

Widerspruch aus sachlich gerechtfertigtem Grund gegen die Subbeauftragung bzw. den Wechsel des Sub-Auftragsverarbeiters, so gilt sie als genehmigt.

Ein sachlich gerechtfertigter Grund liegt insbesondere vor, wenn Anhaltspunkte dafür vorliegen, dass durch die Beauftragung die Erbringung der vertragsgegenständlichen Leistungen gefährdet oder beeinträchtigt wird, die Zusammenarbeit mit dem Sub-Auftragsverarbeiter die Erfüllung von gesetzlichen oder vertraglichen Verpflichtungen einer Vertragspartei, insbesondere von aufsichtsbehördlichen Vorschriften, gefährdet.

Im Falle, dass der Kunde der Subbeauftragung aus sachlich gerechtfertigtem Grund widerspricht, so ändert dieser Widerspruch nichts an der Rechtmäßigkeit der Subbeauftragung. Im Falle eines erfolgten Widerspruchs, sind der Kunde und der Auftragnehmer – mangels einvernehmlicher Lösung – je zur außerordentlichen Kündigung des Hauptvertrages berechtigt.

Dieses außerordentliche Kündigungsrecht steht dem Kunden auch dann zu, wenn der Auftragnehmer ohne vorherige Einholung der schriftlichen Genehmigung des Kunden oder entgegen einem sachlich gerechtfertigten Einspruch des Kunden eigenmächtig einen Sub-Auftragsverarbeiter heranzieht und eine einvernehmliche Lösung nicht möglich ist.

Im Falle der Beauftragung von Sub-Auftragsverarbeitern, sind diese hinsichtlich der Anforderungen zu Vertraulichkeit, Datenschutz und Datensicherheit gemäß dieser Vereinbarung vertraglich zu verpflichten. Der Auftragnehmer wird dem Sub-Auftragsverarbeiter vertraglich sinngemäß dieselben Pflichten auferlegen, die in dieser Vereinbarung oder in sonstigen Vereinbarungen zwischen dem Kunden und dem Auftragnehmer festgelegt sind. Der Auftragnehmer ist verpflichtet, dem Kunden auf eine entsprechende Aufforderung hin, Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen durch die Sub-Auftragsverarbeiter zu erteilen.

Der Auftragnehmer ist gegenüber dem Kunden für sämtliche Handlungen und Unterlassungen der von ihm eingesetzten Sub-Auftragsverarbeiter verantwortlich.

Die Inanspruchnahme von mit dem Auftragnehmer konzernverbundene Unternehmen innerhalb der Europäischen Union als Sub-Auftragsverarbeiter gilt mit dem Abschluss dieser Vereinbarung jedenfalls als vom Kunden genehmigt. Konzernverbundene Unternehmen sind Unternehmen, an welchen die Fabasoft AG direkt oder indirekt derzeit oder zukünftig

a) über mehr als die Hälfte der Stimmrechte verfügt; oder

b) mehr als die Hälfte der Mitglieder des Leitungs- oder Verwaltungsorgans oder der zu gesetzlichen Vertretung berufenen Organe bestellen kann; oder

c) das Recht hat, die Geschäfte des Unternehmens zu führen.

Der Kunde anerkennt das berechtigte Interesse des Auftragnehmers, für interne Verwaltungszwecke personenbezogene Daten innerhalb der Unternehmensgruppe, welcher der Auftragnehmer angehört, einschließlich der Verarbeitung personenbezogener Daten, zu übermitteln.

6.2. Im Falle eines erfolgten Widerspruchs, sind der Kunde und der Auftragnehmer – mangels einvernehmlicher Lösung – je zur außerordentlichen Kündigung dieses Vertrags berechtigt.

Dieses außerordentliche Kündigungsrecht berechtigt den Kunden und den Auftragnehmer jeweils das gegenständliche Vertragsverhältnis unter Berücksichtigung der Formalitäten gemäß Ziffer 4.5 des CSA aufzukündigen. Hat der Kunde eine Zahlperiode gewählt, die

länger ist als das Vertragsverhältnis bis zur außerordentlichen Kündigung gedauert hat, erhält der Kunde das zu viel bezahlte Entgelt, aliquotiert auf Monatsbasis, rückerstattet.

Dieses außerordentliche Kündigungsrecht steht dem Kunden auch dann zu, wenn der Auftragnehmer ohne vorherige Einholung der schriftlichen Genehmigung des Kunden oder entgegen einem sachlich gerechtfertigten Einspruch des Kunden eigenmächtig einen Sub-Auftragsverarbeiter heranzieht und eine einvernehmliche Lösung nicht möglich ist.

6.3. Die aktuelle Liste von Sub-Auftragsverarbeitern ist online abrufbar unter der im Informationsblatt CSA angegebenen Website „Link zu Vertragsgrundlagen“.

7. Kontrollrechte des Kunden

7.1. Der Kunde überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers und dokumentiert das Ergebnis.

Hierfür kann der Kunde vom Auftragnehmer entsprechende Auskünfte verlangen oder sich nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich überzeugen.

7.2. Der Auftragnehmer verpflichtet sich, dem Kunden auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die für die Durchführung einer Kontrolle erforderlich sind.

7.3. Eine Zusammenfassung der Zertifizierungen und Audits finden Sie im CSA-Informationsblatt unter "Zusätzliche hilfreiche Links", "Zusammenfassung der Zertifizierungen und Audits" auf der dort angegebenen Website.

Der Kunde kann zum Nachweis von Maßnahmen zur Datensicherheit bzw. zur Einhaltung der Datensicherheitsmaßnahmen, ein Audit durch unabhängige Instanzen schriftlich verlangen bzw. auch selbst ein Audit durchführen, sofern der Kunde selbst nachweislich über die notwendige Expertise zur Durchführung eines solchen Audits verfügt.

Der Kunde wird gegenüber dem Auftragnehmer die Notwendigkeit des Audits spätestens binnen 14 Tagen ab seinem Verlangen, schriftlich darlegen und begründen. Ein Audit ist möglichst ohne Störung des Betriebsablaufs des Auftragnehmers durchzuführen. Der Ablauf, die Auswahl der Prüfinstanz, die Terminfindung, sowie die Beauftragung ist sodann im Einvernehmen zwischen Kunde und dem Auftragnehmer zu treffen.

Der Kunde, der ein Audit verlangt, hat die angemessenen Aufwendungen (= Kosten des Audits, sowie die Aufwendungen des Auftragnehmers) selbst zu tragen. Sofern darüber hinaus ein zusätzlicher Personalaufwand beim Auftragnehmer entsteht, sind diese zusätzlichen Aufwendungen nach üblichen Stundensätzen (vom Auftragnehmer) durch den Kunden abzugelten.

Der Auftragnehmer kann darüber hinaus dem Kunden, der ein Audit verlangt, die internen Vorschriften über die Durchführung eines Audits vorlegen. Der Kunde hat diese internen Vorschriften einzuhalten.

Der Kunde wird dem Auftragnehmer die Dokumentation des Audits in Form des gesamten Prüfberichts zur Verfügung stellen.

Der Auftragnehmer kann dem Ersuchen des Kunden vorrangig auch in der Form nachkommen, dass eine Auflistung der aktuellen Prüfberichte von bereits durchgeführten Audits dem Kunden bereitgestellt wird.

Jedenfalls ist vorab zwischen dem Kunden und dem Auftragnehmer, sowie mit der unabhängigen Prüfinstanz, eine entsprechende Verschwiegenheitsvereinbarung (kurz „NDA“) zu unterfertigen.

Bei der Zusammenfassung der Prüfberichte, sowie bei den Prüfberichten selbst, handelt es sich um streng vertrauliche Unterlagen. Grundsätzlich ist jede Form der Weitergabe, Verbreitung oder Offenlegung, die vom Auftragnehmer nicht ausdrücklich schriftlich genehmigt wurde, untersagt.

Sofern die Vorlage von Prüfberichten von durchgeführten Audits beim Auftragnehmer für Kontrollhandlungen; Ermittlungen oder Maßnahmen der datenschutzrechtlichen Aufsichtsbehörde gegenüber dem Kunden erforderlich wird, so wird der Auftragnehmer den Kunden – auf dessen Anfrage – bei der Erfüllung seiner Verpflichtungen gegenüber der Aufsichtsbehörde unterstützen und die erforderlichen Prüfberichte direkt an die Aufsichtsbehörde übermitteln.

7.4. Für die Datensicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind vorab mit dem Kunden abzustimmen.

7.5. Der Auftragnehmer ist verpflichtet, dem Kunden jeden Verstoß gegen datenschutzrechtliche Vorschriften oder die vertraglichen Vereinbarungen unverzüglich derart in Textform mitzuteilen, sodass der Kunde seine gesetzlichen Pflichten erfüllen kann. Entsprechendes gilt für Störungen, sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten.

8. Data-Breach-Vorfall

8.1. Dem Auftragnehmer sind die geltenden datenschutzrechtlichen Melde- und Benachrichtigungspflichten gegenüber der Aufsichtsbehörde und Betroffenen, insbesondere deren zeitliche und inhaltliche Vorgaben, bekannt.

8.2. Der Auftragnehmer erstattet in allen Fällen dem Kunden unverzüglich eine Meldung, wenn durch sie oder durch die bei ihr beschäftigten Personen Verstöße gegen Vorschriften zum Schutz der Daten des Kunden oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind. Dies umfasst insbesondere auch, wenn es zu schwerwiegenden Betriebsstörungen kommt, wenn eine Verletzung der Datenschutzregeln vermutet wird bzw. sofern sonstige Unregelmäßigkeiten bei der Verarbeitung der Daten des Kunden auftreten.

8.3. Der Auftragnehmer hat im Einvernehmen mit dem Kunden angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für den Betroffenen zu ergreifen und diese Maßnahmen zu dokumentieren. Die Dokumentation ist unverzüglich nach Aufforderung des Kunden an diesen herauszugeben. Soweit den Kunden Melde- bzw. Benachrichtigungspflichten treffen, hat der Auftragnehmer ihn hierbei zu unterstützen.

9. Rechte des Betroffenen

9.1. Der Auftragnehmer wird den Kunden dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der Betroffenen nachzukommen. Zu den Betroffenenrechten können insbesondere gehören:

a) Informationspflicht und Recht auf Auskunft zu Daten;
b) Recht auf Berichtigung, Löschung und Datenübertragbarkeit;

c) Widerspruchsrecht und Recht auf nicht ausschließlich automatisierte Entscheidungsfindung im Einzelfall.

9.2. Soweit sich Betroffene unmittelbar an den Auftragnehmer zwecks Ausübung ihrer Betroffenenrechte wenden, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Kunden weiterleiten.

9.3. Ebenso ist ein allfälliger beim Auftragnehmer einlangender Widerruf einer Einwilligung eines Betroffenen iSd. Art 7 Abs 3 DSGVO unverzüglich an den Kunden weiterzuleiten.

10. Rückgabe der Daten nach Auftragsende

10.1. Der Auftragnehmer hat keinen Zugriff auf die Benutzerdaten des Kunden. Diese personenbezogenen Daten liegen in der ausschließlichen Verfügungsmacht des Kunden. Der Kunde hat daher mit Auftragsende die von ihm gespeicherten Daten selbst direkt zu löschen. Der Kunde kann alternative die Löschung auch vom Auftragnehmer durchführen lassen. Für diesen Fall ist eine schriftliche Weisung an den Auftragnehmer sowie ein Datenzugang zu erteilen und sind die Kosten und Aufwendungen, die im Zusammenhang mit der Löschung beim Auftragnehmer entstehen, vom Kunden zu tragen.

10.2. Der Kunde legt die Maßnahmen zur Rückgabe und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest. Der Kunde hat zudem eine Zeitschiene, in der die Rückgabe und/oder Löschung zu erfolgen hat, festzulegen. Andernfalls erfolgen die Löschung der Daten bzw. die unwiederbringliche Rückgabe der Daten durch den Auftragnehmer spätestens 6 Monate nach Beendigung der Vertragsbeziehung. Sämtliche Kosten in Zusammenhang mit Beendigung und/oder Herausgabe der Daten, hat der Kunde zu tragen.

10.3. Die Daten des Kunden, die etwa dem Nachweis der auftrags- und ordnungsgemäßen Auftragsverarbeitung dienlich sein können, können vom Auftragnehmer über das Vertragsende soweit gerechtfertigt datenschutzgerecht aufbewahrt werden.

11. Sonstiges

11.1. Sollten die Daten des Kunden beim Auftragnehmer aufgrund einer Pfändung, Vollstreckung oder Beschlagnahme bzw. wegen eines Insolvenz- oder Vergleichsverfahrens oder aufgrund eines sonstigen Ereignisses bzw. einer sonstigen Handlung eines Dritten nicht mehr sicher bzw. gefährdet sein, hat der Auftragnehmer den Kunden unverzüglich zu benachrichtigen. Der Auftragnehmer informiert alle in diesem Zusammenhang verantwortlichen Parteien unverzüglich darüber, dass die Macht über die Daten beim Kunden liegt.

11.2. Der Auftragnehmer und der Kunde vereinbaren, dass Änderungen, Ergänzungen und diese Vereinbarung betreffende Erklärungen der Schriftform bedürfen. Auch das Aufheben dieses Schriftformerfordernisses bedarf der Schriftform. Sind Änderungen dieser Vereinbarung aufgrund geänderter rechtlicher Grundlagen, zB Gesetzesänderungen oder höchstgerichtlicher Rechtsprechung erforderlich, wird die Änderung mit dem jeweiligen Datum des Inkrafttretens (siehe Deckblatt, Datumsangabe) wirksam.

11.3. Diese Vereinbarung unterliegt dem Recht am Sitz des Auftragnehmers unter Ausschluss von Verweisnormen und von UN-Kaufrecht. Gerichtsstand ist das örtlich und sachlich zuständige Gericht am Sitz des Auftragnehmers.

11.4. Sollte eine Bestimmung dieser Vereinbarung unwirksam oder undurchführbar sein oder werden, berührt dies die Wirksamkeit ihrer übrigen Bestimmungen nicht. Die Vertragsparteien verpflichten sich, anstelle der unwirksamen Regelung eine neue, wirksame Regelung zu vereinbaren, die dem Sinn und Zweck der unwirksamen Regelung am nächsten kommt. Dasselbe gilt für etwaige Lücken in dieser Vereinbarung.

11.5. Der Kunde ist verpflichtet, für die Zwecke dieser Vereinbarung und der Kontaktaufnahme durch den Auftragnehmer einen Kontakt im dafür vorgesehenen Pflichtfeld im Servicepaket zu benennen und aktuell zu halten. Der Kunde nimmt zur Kenntnis, dass der Auftragnehmer sämtliche Nachrichten aus und/oder im Zusammenhang mit Datensicherheits- und Datenschutzangelegenheiten, insbesondere gemäß Punkt 8., ausschließlich an diesen vom Kunden eingerichteten Kontakt richtet.