Vertrag zur Auftragsverarbeitung personenbezogener Daten (gem. DSGVO)

zwischen

Stempel des Auftraggebers

- Auftraggeber -

und der

bizz consult gmbh
Entwicklung von Geschäftsprozessen

Braunsberger Feld 12
51429 Bergisch Gladbach

- Auftragnehmer –

1. Allgemeines

(1) 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.
(2) 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.

2. Gegenstand des Auftrags

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag festgelegt.

3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 5 das Recht zu, den

Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen können in Textform (z.B. E-Mail) erfolgen.

(4) Regelungen über eine etwaige Vergütung von Mehraufwendungen, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

(5) Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 1** benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.

(6) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(7) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

(2) Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen.

(3) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

(4) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der Auftragnehmer wird

Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Auftraggeber abstimmen.

(5) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(6) Die Verarbeitung von Daten im Auftrag des Auftraggebers außerhalb von Betriebsstätten des Auftragnehmers oder Subunternehmern ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform zulässig. Eine Verarbeitung von Daten für den Auftraggeber in Privatwohnungen ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform im Einzelfall zulässig.

(7) Der Auftragnehmer wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich.

(8) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Sofern weisungsempfangsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 1** benannt. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

5. Datenschutzbeauftragter des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Der Auftragnehmer wird dem Auftraggeber den Namen und die Kontaktdaten seines Datenschutzbeauftragten gesondert in Textform mitteilen.

(2) Die Pflicht zur Benennung eines Datenschutzbeauftragten nach Absatz 1 kann im Ermessen des Auftraggebers entfallen, wenn der Auftragnehmer nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu bestellen und der Auftragnehmer nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des Auftraggebers gewährleisten.

6. Meldepflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

(2) Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

– eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

– eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7. Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 11 dieses Vertrages.

(2) Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber mit. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(3) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

8. Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(3) Der Auftraggeber kann eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

(4) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören.

(5) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

9. Unterauftragsverhältnisse

(1) Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist nur mit Zustimmung des Auftraggebers in Textform zulässig. Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der **Anlage 2** zu diesem Vertrag angeben.

(2) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln.

(3) Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat. Für den Fall, dass kein Datenschutzbeauftragter beim Unterauftragnehmer benannt worden ist, hat der Auftragnehmer den Auftraggeber hierauf hinzuweisen und Informationen dazu beizubringen, aus denen sich ergibt, dass der Unterauftragnehmer gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragte zu benennen.

(4) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

(5) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

(6) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 8 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

(7) Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 6 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit

auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-System oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

10. Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Auftragnehmer sichert ferner zu, dass er insbesondere die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Auftraggebers informiert hat.

(3) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

11. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützten. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

12. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

13. Vergütung

Die Vergütung des Auftragnehmers wird gesondert vereinbart.

14. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 3** zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

(3) Der Auftragnehmer wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der Auftragnehmer den Auftraggeber informieren.

15. Dauer des Auftrags

(1) Der Vertrag beginnt mit Unterzeichnung und wird auf unbestimmte Zeit geschlossen.

(2) Er ist mit einer Frist von drei Monaten zum Quartalsende kündbar.

(3) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

16. Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt. Für Datenträger gilt, dass diese im Falle einer vom Auftraggeber gewünschten Löschung zu vernichten sind, wobei mindestens die Sicherheitsstufe 3 der DIN 66399 einzuhalten ist; die Vernichtung ist dem Auftraggeber unter Hinweis auf die Sicherheitsstufe gemäß DIN 66399 nachzuweisen.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

17. Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

18. Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Für Nebenabreden ist die Schriftform erforderlich.

(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Bergisch Gladbach, den _____ _____

Ort Datum

_____ _____

- Auftragnehmer - - Auftraggeber -

Anlage 1 - Gegenstand des Auftrags

1. Gegenstand und Zweck der Verarbeitung

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

- Entwicklung von Geschäftsprozessen
- Einrichtung, Pflege und Wartung von IT-Systemen
- Entwicklung, Anpassung und Installation von Software
- 1st und 2nd Level Support für Softwareprodukte
- Remotezugriff auf IT-Systeme des Auftraggebers
- Umgang mit Echtdaten in Images und Backup

Zweck der Verarbeitung ist die Begründung einer Geschäftsbeziehung zwischen dem Auftragnehmer und dem Auftraggeber.

2. Art(en) der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

- Kontaktdaten und -historie (Kunden, Lieferanten, Ansprechpartnern von Firmen, Interessenten und Vertretern)
- Daten zur Geschäftshistorie von Kunden, Lieferanten und Vertretern
- Kunden- und Mitarbeiterdaten des Auftraggebers
- Mandantendaten des Auftraggebers
- Personenstammdaten
- Kommunikationsdaten
- Daten zur Vermögens- und Ertragssituation von Kunden und Lieferanten
- Vertragsstammdaten
- Abrechnungs- und Zahlungsdaten
- Buchhaltungsdaten
- Lohnabrechnungsdaten
- Sonstige unstrukturierte personenbezogene Daten von Kunden, Lieferanten, Ansprechpartner von Firmen, Interessenten, Vertretern, Mitarbeitern und Anwendern des Systems

3. Kategorien betroffener Person

Kreis der von der Datenverarbeitung betroffenen Personen:

- Ansprechpartner und Handelnde des Auftraggebers
- Interessenten, Kunden und Lieferanten des Auftraggebers
- Mitarbeiter des Auftraggebers

4. Weisungsberechtigte Personen des Auftraggebers

Vom Auftraggeber auszufüllen

5. Weisungsempfangsberechtigte Personen des Auftragnehmers

- Geschäftsleitung
- Projektleitung

Anlage 2 - Unterauftragnehmer

Der *Auftragnehmer* nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende(s) Unternehmen:

Unterauftragnehmer	Verarbeitungsstandort	Art der Dienstleistung
Sage GmbH Franklinstraße 61-63 60486 Frankfurt am Main Telefon: +49 69 50007-0 E-Mail: info@sage.de	Deutschland	Prüfung von Mandantendaten
Infor (Deutschland) GmbH Hauerstrasse 12 66299 Friedrichsthal Telefon +49 511 93 68 92 00 E-Mail: contact@infor.com	Deutschland	Prüfung von Mandantendaten
s&t Deutschland GmbH Am Flugplatz 35 56743 Mendig Telefon: +49 2652 93509-0 E-Mail: info@sntde.de	Deutschland	Pflege und Wartung von IT-Systemen
brainbits GmbH Alpenerstraße 16 50825 Köln Telefon: +49 221 589808-0 E-Mail: info@brainbits.net	Deutschland	Pflege und Wartung von IT-Systemen

Anlage 3 - Technische und organisatorische Maßnahmen der bizz consult gmbh

Die bizz consult gmbh ist autorisierter Fachhandels- und Entwicklungspartner von Sage, dem führenden Hersteller kaufmännischer Software für kleine und mittlere Unternehmen. Die von der bizz consult gmbh getroffenen technischen und organisatorischen Maßnahmen sind nachfolgend beschrieben:

1. Zutrittskontrolle

Dieser Absatz behandelt Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Die Büroräume der bizz consult gmbh befinden sich in einem Bürokomplex in Bergisch Gladbach. In den Bürogebäudekomplex befinden sich Büros für 4 Unternehmen. Der Eingang des Gebäudekomplexes ist über eine Zutrittstür gesichert. Das Schlüsselmanagement für die Zutrittstür zum Gebäudekomplex liegt beim Vermieter. Die vom Vermieter ausgegebenen elektronischen Schlüssel sind dem jeweiligen Mieter zugeordnet. Die Verwaltung der einzelnen elektronischen Schlüssel der bizz consult gmbh für die Zutrittstür obliegt der bizz consult gmbh selbst.

Diesbezüglich gibt es einen Prozess für die Ausgabe von Schlüsseln auf Basis eines 4-Augen-Prinzips. Die Ausgabe von Schlüsseln wird protokolliert. Mitarbeiter sind verpflichtet, einen Schlüsselverlust unverzüglich zu melden. Im Falle eines Verlusts erfolgt eine sofortige elektronische Sperrung des jeweiligen Schlüssels.

Ferner gibt es einen Prozess bei einem Ausscheiden eines Mitarbeiters, der insbesondere auch die Rückgabe von Schlüsseln und sonstigem Eigentum der bizz consult gmbh durch den ausscheidenden Mitarbeiter beinhaltet.

Der Bürogebäudekomplex insgesamt und insbesondere auch die Büroräume der bizz consult gmbh sind durch eine Alarmanlage gesichert. Die Alarmanlage in den Büroräumen der bizz consult gmbh wird durch den jeweils letzten Mitarbeiter bei Verlassen der Büroräume aktiviert. Aktivierung und Deaktivierung der Alarmanlage erfolgen durch einen Token, den Mitarbeiter erhalten. Auch hierfür gilt der Schlüsselausgabe-Prozess. Die Token sind mit einer Nummer versehen. In der Alarmanlage werden Aktivierungen und Deaktivierungen auf Basis der Token-Nummer protokolliert.

Die Büroräume der bizz consult gmbh befinden sich im 1. Stockwerk des Bürogebäudes. Die Büroräume der bizz consult gmbh sind mit Bewegungssensoren für die Alarmanlage versehen.

Daten der bizz consult gmbh , die im Auftrag verarbeitet werden, werden ausschließlich auf eigenen Servern innerhalb der Räume der bizz consult gmbh gespeichert.

Nachts von 22:00 bis 7:00 Uhr und am Wochenende werden die Räumlichkeiten der bizz consult gmbh durch einen Wachdienst überwacht.

2. Zugangskontrolle

Dieser Absatz behandelt Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Die Büroräume der bizz consult gmbh befinden sich im ersten Stock. Die Bildschirme der Mitarbeiter sind stets so ausgerichtet, dass eine Einsichtnahme von außen nicht erfolgen kann.

An jedem IT-System, das bei der bizz consult gmbh im Einsatz ist, muss eine vorherige Domänen-Authentifizierung erfolgen. Dies erfolgt auf Basis eines Benutzernamens und eines Passworts. Das Passwort ist nur dem jeweiligen Mitarbeiter bekannt und darf nicht weitergegeben werden.

Eine Berechtigung zur Nutzung eines IT-Systems oder einer Applikation wird bei der bizz consult gmbh nach dem 4-Augen-Prinzip erteilt. Eine Berechtigung muss daher zwingend vom jeweiligen Vorgesetzten für einen Mitarbeiter bei der IT-Administration beantragt werden. Der Vorgesetzte ist verpflichtet, hierbei nur die Berechtigungen zu beantragen, die für den jeweiligen Mitarbeiter unbedingt erforderlich sind, damit dieser die ihm zugewiesenen Aufgaben erfüllen kann. Berechtigungen sind dabei auf das Minimale zu beschränken.

Im Falle des Ausscheidens von Mitarbeiter informieren die Personalverantwortlichen die IT-Administration unverzüglich über anstehende Veränderungen, damit die IT-Administration entsprechende Berechtigungen entziehen kann. Der Entzug von Berechtigungen muss binnen 24 Stunden nach Ausscheiden eines Mitarbeiters durchgeführt worden sein.

Werden Initialpasswörter vergeben, ist bei der bizz consult gmbh stets vorgesehen, dass das Initialpasswort bei der ersten Anmeldung geändert wird. Dies wird technisch erzwungen.

Bei der bizz consult gmbh gibt es Richtlinien zur Passwortverwendung, die ebenfalls grundsätzlich technisch erzwungen werden. Die Mindestpasswortlänge beträgt 12 Zeichen. Passwörter sind komplex zu wählen. Dies beinhaltet die Verwendung von Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern.

Ein Passwortwechsel ist spätestens nach 180 Tagen zwingend. Es ist sichergestellt, dass die letzten 16 verwendeten Passwörter eines Nutzers nicht von diesem wiederverwendet werden können. Sollte sich der Stand der Technik bei der Verwendung von Passwörtern ändern, wird die bizz consult gmbh die Passwortrichtlinien entsprechend anpassen.

Ein Zugriff auf die externen IT-Systeme findet ausschließlich über verschlüsselte Verbindungen statt. Die dabei verwendeten Verschlüsselungsalgorithmen und Schlüssellängen entsprechen dem Stand der Technik. Für den Fall einer zertifikatsbasierten Zugriffstechnologie ist gewährleistet, dass die Zertifikate durch Mitarbeiter der IT-Administration verwaltet werden.

Alle IT-Systeme, mit denen Daten im Auftrag verarbeitet werden, sind mit Antivirus-Software ausgestattet.

Die jeweilige, persönliche Domänen-Authentifizierung wird mit dem Ausscheiden eines Mitarbeiters gesperrt und Zugänge zu Servern der bizz consult gmbh gelöscht.

3. Zugriffskontrolle

Dieser Absatz behandelt Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Für die Erteilung von Benutzerrechten gilt bei der bizz consult gmbh ein Berechtigungskonzept. Dies sieht vor, dass Berechtigungen ausschließlich auf Basis des 4-Augenprinzips und nach dem Minimalprinzip vergeben werden. Dies beinhaltet, dass jeder Mitarbeiter nur die Berechtigungen erhält, die er unmittelbar benötigt, um seine Aufgaben im Unternehmen erfüllen zu können.

Das Berechtigungskonzept ist rollenbasiert. Jedem Mitarbeiter wird grundsätzlich eine bestimmte Rolle zugewiesen. Von dieser Rolle abweichende Berechtigungen müssen begründet sein.

Die Vergabe und der Entzug von Berechtigungen wird protokolliert.

4. Weitergabekontrolle

Dieser Absatz behandelt Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Dadurch, dass Berechtigungen nach dem Minimalprinzip vergeben werden, ist gewährleistet, dass der Kreis der Personen, die Zugang zu Daten haben, die im Auftrag verarbeitet werden, beschränkt ist.

Sofern Daten im Einzelfall auf Anfrage des Auftraggebers an diesen durch die bizz consult gmbh übergeben werden soll, werden die Parteien im Vorwege eine Verschlüsselungsmethode bzw. einen Weg der sicheren Übertragung vereinbaren.

5. Eingabekontrolle

Dieser Absatz behandelt Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Mitarbeiter sind angewiesen, in Datenverarbeitungssystemen des Auftraggebers keine personenbezogenen Daten zu erfassen oder zu bearbeiten, es sei denn, der Auftraggeber fordert sie ausdrücklich dazu auf. Fernwartungssitzungen werden aufgezeichnet und archiviert. Der Auftraggeber wird über diese Aufzeichnungen informiert.

6. Auftragskontrolle

Dieser Absatz behandelt Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Der Schutz personenbezogener Daten und auch der Schutz von Betriebs- und Geschäftsgeheimnissen hat bei der bizz consult gmbh eine hohe Priorität. Alle Mitarbeiter sind auf das Datengeheimnis verpflichtet.

Es gibt einen betrieblichen Datenschutzbeauftragten, der auch die regelmäßige Schulung der Mitarbeiter plant und durchführt.

Mitarbeiter, die an der Erbringung von Leistungen für den Auftraggeber beteiligt sind, sind im Hinblick auf die Verarbeitung der Daten instruiert. Sofern der Auftraggeber ergänzende Weisungen erteilt, wird die bizz consult gmbh alle betroffenen Mitarbeiter unverzüglich über die jeweilige Weisung informieren und Handlungsanweisungen zur Umsetzung geben.

Die Datenschutzvorkehrungen der bizz consult gmbh beinhalten auch eine regelmäßige Überprüfung und Bewertung der getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit. Hierzu gehört auch ein Verbesserungs- und Vorschlagswesen, an dem sich Mitarbeiter beteiligen können. Die bizz consult gmbh gewährleistet so eine kontinuierliche Verbesserung der Prozesse im Umgang mit personenbezogenen Daten.

7. Verfügbarkeitskontrolle

Dieser Absatz behandelt Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Alle Daten, die für den Auftraggeber verarbeitet werden, befinden sich nur auf Servern und Arbeitsstationen der bizz consult gmbh. Die bizz consult gmbh hat Maßnahmen getroffen, die eine Sicherung der Daten und Wiederherstellung von Daten gewährleistet. Die Datenhaltung erfolgt zudem redundant. Es gibt ein Datensicherungs- und Wiederherstellungskonzept, dessen Wirksamkeit regelmäßig getestet wird.

Das Netzwerk der bizz consult gmbh ist durch zwei redundante Firewalls abgesichert. Alle Mitarbeiter sind verpflichtet, Sicherheits-Patches schnellstmöglich einzuspielen und Antivirensoftware regelmäßig zu aktualisieren.

8. Trennungsgebot

Produktivdaten werden täglich verschlüsselt auf Band gesichert und in regelmäßigen Abständen in einem Bandschließfach außerhalb der Räumlichkeiten der bizz consult gmbh aufbewahrt. Der Zugriff auf das Bankschließfach ist nur zwei Mitarbeitern möglich. Zugriffe werden protokolliert.

Dieser Absatz behandelt Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Die IT-Systeme, auf denen Daten im Auftrag verarbeitet werden, sind mandantenfähig. Es ist sichergestellt, dass Daten getrennt voneinander verarbeitet werden. Die Verarbeitung erfolgt für

jeden Auftraggeber in einer eigenen virtuellen Umgebung (VMWare). Der Zugriff auf virtuelle Umgebungen ist durch das Domänenkennwort geschützt. Der Speicherort der virtuellen Maschinen ist vom Produktivsystem der bizz consult gmbh abgekoppelt.

9. Pseudonymisierung & Verschlüsselung

Daten des Auftraggebers dürfen nur verschlüsselt übertragen werden. Unverschlüsselter Cloudspeicher darf nicht genutzt werden.

Anlage 4 - Datenschutzbeauftragte

1. Datenschutzbeauftragter des Auftraggebers
(sofern vorhanden)

Vom Auftraggeber auszufüllen (falls vorhanden)

2. Datenschutzbeauftragter des Auftragnehmers

Martin Höh-Coolen
c/o bizz consult gmbh

Braunsberger Feld 12
51429 Bergisch Gladbach

Telefon +49 2204 48 240-0
Telefax +49 2204 48 240-12
Email: dsb@bizz-consult.de