ZUSATZVEREINBARUNG DATENSCHUTZ BEI Mustermann GmbH IM RAHMEN DER AUFTRAGSVERARBEITUNG

Mustermann GmbH
Samplestr. 815
40000 Düsseldorf

- nachfolgend Auftraggeber genannt -

und

alpha EDV Systemhaus GmbH & Co. KG
Kronprinzenstraße 82-84
40217 Düsseldorf

- nachfolgend Auftragnehmer genannt -

treffen die nachfolgenden Vereinbarungen zur Wahrung des Datenschutzes bei der Auftragsverarbeitung gemäß Artikel 28 Abs. 3 Datenschutzgrundverordnung (DSGVO).

1 PRÄAMBEL

(1) Gemäß Art. 28 DSGVO werden an die Durchführung einer Auftragsverarbeitung sowie an Form und Inhalt der Vereinbarung über die Auftragsverarbeitung bestimmte gesetzliche Anforderungen gestellt.

(2) Diese Anlage konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus den Dienstleistungen des Auftragnehmers für den Auftraggeber ergeben. Sie findet Anwendung auf alle Tätigkeiten, die der Auftragnehmer für den Auftraggeber durchführt.

(1) DEFINITIONEN

(1) Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden "betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;. Dabei kommt es nicht darauf an, wer diese Zuordnung vornehmen kann, sondern nur darauf, ob eine solche überhaupt möglich ist.

(2) Im Zweifelsfall gelten alle Daten, mit denen der Auftragnehmer oder seine Mitarbeiter bzw. von ihm Beauftragte in Berührung kommen oder kommen können, als personenbezogene Daten im Rahmen dieser Vertragsdurchführung.

(2) ANWENDUNGSBEREICH UND VERANTWORTLICHKEIT

(1) Der Auftragnehmer führt alle Arbeiten im Auftrag und nach den Weisungen des Auftraggebers durch.

(2) Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich ("verantwortliche Stelle" im Sinne des Artikel 4 Nummer 7 DSGVO).

(3) Soweit eine der Vertragsparteien nicht in der Union niedergelassenen ist, benennt der Verantwortliche oder der Auftragsverarbeiter schriftlich gem. Artikel 27 einen Vertreter in der Union. Dieser vertritt den Verantwortlichen oder den Auftragsverarbeiter in allen nach der DSGVO obliegenden Pflichten. Die Vertragsparteien informieren sich gegenseitig in einem Fall der Bestellung über die Kontaktdaten des Vertreters und den Umfang seiner Beauftragung.

(4) Soweit eine Vertragspartei einen Datenschutzbeauftragten benannt hat, informiert sie die jeweils andere Vertragspartei über den Namen und die Kontaktdaten.

(5) Der Auftragnehmer (Auftragsverarbeiter) und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:

a) den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und des Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;

b) die Kategorien von Verarbeitungen, die im Auftrag des Verantwortlichen durchgeführt werden;

c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

d) eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO.

(6) Der Auftragnehmer führt das Verzeichnis schriftlich, was auch in einem elektronischen Format erfolgen kann. Der Auftraggeber übermittelt dem Auftragnehmer die zur Führung des Verzeichnisses erforderlichen Informationen mit Vertragsbeginn. Der Auftragnehmer stellt dem Auftraggeber und seinem bestellten Datenschutzbeauftragten einen Abdruck des Verzeichnisses auf Anforderung zur Verfügung.

(7) Verlangt eine Aufsichtsbehörde von einer der Vertragsparteien die Herausgabe des Verzeichnisses, informieren sich die Vertragsparteien gegenseitig unverzüglich hierüber und über den Inhalt der Auskunft.

(8) Soweit die Pflicht zum Führen eines Verzeichnisses für eine der Vertragsparteien nicht gilt, bleiben hiervon die Informationspflichten unberührt.

(3) UMFANG, ART UND ZWECK DER DATENVERWENDUNG, ART DER DATEN UND KREIS DER BETROFFENEN

(1) Der Auftragnehmer wird die Auswahl und Gestaltung seiner Datenverarbeitungssysteme an dem Ziel ausrichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Er wird sofern dies nach dem Auftrag möglich ist, personenbezogene Daten anonymisieren oder pseudonymisieren. Er wird den Auftraggeber auf technische Möglichkeiten zur Datenvermeidung und Datensparsamkeit hinweisen. Er wird Maßnahmen zur Gewährleistung des Rechts auf Datenportabilität gem. Art. 20 DSGVO treffen.

(2) Der Auftragnehmer führt im Auftrag des Auftraggebers Service- und/oder Supportarbeiten an den IT-Systemen des Auftraggebers durch.

Monitoring

Die Arbeiten umfassen das Monitoring der IT-Systeme des Auftraggebers auf Basis des Monitoringsystems Paessler PRTG.

Tätigkeiten des Auftragnehmers:

- Automatisierte Erfassung von Zustandsdaten der IT-Systeme des Auftraggebers

- Übermittlung von Fehlerzuständen an die Überwachungskonsolen
- Darstellung des zeitlichen Ablaufs von Parametern
- Implementierung / Optimierung von Monitoring-Sensoren auf der Probe des Auftraggebers

Erhobene Daten:

- Zustandsparameter der überwachten Systeme
- zeitlicher Ablauf der Zustandsparameter

Kreis der Betroffenen:

- Auftraggeber

Service / Support

Die Arbeiten umfassen Service- und Supportarbeiten an den IT-Systemen des Auftraggebers. Dem Auftragnehmer sind hierfür administrative Rechte auf die Zielsysteme eingeräumt. In diesem Zusammenhang ist nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf personenbezogene Daten bekommt bzw. Kenntnis erlangt oder personenbezogene Daten verarbeitet, um die Service- und/oder Supportarbeiten an den IT-Systemen durchführen zu können.

Tätigkeiten des Auftragnehmers:

- ggf. Monitoring
- Sämtliche Tätigkeiten zur Sicherstellung der Betriebsbereitschaft der IT-Systeme des Auftraggebers
- Installation, Einrichtung, Konfiguration und Wartung der eingesetzten Systemsoftware
- Support, Wartung und Pflege der Datensicherungseinrichtungen
- Support, Wartung und Pflege der Sicherheitssysteme
- Unterstützung der Endanwender bei der Lösung von systemtechnischen und anwendungsspezifischen Fragestellungen

Die Tätigkeiten werden per Fernwartung oder vor Ort beim Auftraggeber durchgeführt.

Erhobene Daten:

- Benutzer-Informationen
- Protokolldaten (Active Directory)
- Protokolldaten (Security Systeme: Firewall, Mail Perimeter)
- Personenbezogene Daten von Mitarbeitern des Auftraggebers
- Personenbezogene Daten von Geschäftspartnern, Kunden und Interessenten des Auftraggebers sowie dessen Erfüllungsgehilfen

Kreis der Betroffenen:

- Auftraggeber, Kunden, Interessenten, Dritte, Aufsichtsbehörden

Bereitstellung Infrastructure-as-a-Service (IaaS)

Der Auftragnehmer stellt dem Auftraggeber Hard- und Software-Ressourcen in Form virtueller Server, Switches und Sicherheitssystemen zur Verfügung.

Tätigkeiten des Auftragnehmers:

- Bereitstellung der Ressourcen
- Management der Ressourcen (Anpassung Hardware)
- Monitoring der Ressourcen
- Sicherung der Systeme
- Bereitstellung der Netzwerkanbindung des Auftraggebers (verschlüsselt)

Die Ressourcen werden automatisiert über die entsprechende Verwaltungs-Software (VMware vSphere oder Hyper-V) zur Verfügung gestellt.

Erhobene Daten:

- Protokolldaten (Laufzeit, Hardware, Kapazitätsauslastung)
- Zugriff auf Server über Management-Console
- Zugriff auf Backupdaten, sofern seitens des Auftraggebers keine Verschlüsselung/Kennwortschutz eingerichtet wurde

Kreis der Betroffenen:

- Auftraggeber, Kunden, Interessenten, Dritte, Aufsichtsbehörden

Bereitstellung cloud-basierter Backup-Kapazitäten (BaaS)

Der Auftragnehmer stellt dem Auftraggeber Backup-Kapazitäten als externes Backup-Repository zur Verfügung.

Tätigkeiten des Auftragnehmers:

- Bereitstellung der Speicherkapazitäten als Repository
- Bereitstellung der Netzwerkanbindung des Auftraggebers (verschlüsselt)

Die Ressourcen werden automatisiert über die entsprechende Backup-Software (Veaam oder Altaro) zur Verfügung gestellt.

Erhobene Daten:

- Protokolldaten (Backup-Software)
- Zugriff auf Backupdaten, sofern seitens des Auftraggebers keine Verschlüsselung/Kennwortschutz eingerichtet wurde

Kreis der Betroffenen:

- Auftraggeber, Kunden, Interessenten, Dritte, Aufsichtsbehörden

(3) UMFANG DER WEISUNGSBEFUGNIS

(1) Der Auftraggeber behält sich umfassende Weisungsbefugnis für die Durchführung des Auftrages gegenüber dem Auftragnehmer und alle durch ihn zur Verarbeitung von personenbezogenen Daten befugten Personen vor. Sollten über den Hauptvertrag oder diese Zusatzvereinbarung hinaus konkrete Weisungen erforderlich sein, wird der Auftraggeber dem Auftragnehmer Einzelweisungen erteilen. Alle Weisungen werden durch den Auftragnehmer dokumentiert.

Weisungsberechtigte Personen des Auftraggebers sind:

- Geschäftsleitung

(2) Der Auftraggeber ist verpflichtet, die Einzelweisung auf Verlangen des Auftragnehmers schriftlich zu bestätigen. Der Auftraggeber dokumentiert alle Weisungen.

(4) PFLICHTEN DES AUFTRAGNEHMERS

(1) Der Auftragnehmer darf Daten nur gemäß und im Umfang der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Der Auftragnehmer informiert den Auftraggeber unverzüglich wenn er der Meinung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder eines Mitgliedstaates verstößt und soweit eine mitgliedstaatliche Bestimmung auf den Auftragnehmer anwendbar ist.

(2) Wenn personenbezogene Daten verarbeitet oder genutzt werden, so ist die Organisation auf der Seite des Auftragnehmers so zu gestalten, dass die besonderen Anforderungen des Datenschutzes umgesetzt werden. Der Auftragnehmer garantiert daher, die notwendigen technischen und organisatorischen Maßnahmen zu ergreifen, um die Verarbeitung der personenbezogenen Daten des Auftraggebers zu schützen. Dies beinhaltet insbesondere folgende Maßnahmen:

a) Zutrittskontrolle

Unbefugten wird der Zutritt zu Räumlichkeiten, in denen personenbezogene Daten lagern oder verarbeitet werden verwehrt. Während der Dienstzeit wird dieses durch die Mitarbeiter des Auftragnehmers gewährleistet. Außerhalb der Dienstzeiten sind diese Räumlichkeiten verschlossen zu halten. Ausschließlich autorisierte Personen, welche zutrittsberechtigt sind, haben einen Schlüssel zu diesen Räumlichkeiten.

b) Zugangskontrolle

Im Rahmen der Zugangskontrolle wird verhindert, dass Unbefugte die Verarbeitungssysteme nutzen. Die logische Zugangskontrolle wird durch ein umfassendes Rechte- und Rollenkonzept erreicht.

c) Zugriffskontrolle

Im Rahmen der Zugriffskontrolle stellt der Auftragnehmer sicher, dass ausschließlich die Berechtigten auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

Die Rollen der Benutzer, die auf die personenbezogenen Daten des Auftraggebers zugreifen können, sind fest definiert.

d) Weitergabekontrolle

Eine Weitergabe der Daten an Dritte erfolgt nicht. Datentransfer zwischen Auftraggeber und Auftragnehmer erfolgt über eine dem aktuellen Stand der Technik entsprechende verschlüsselte Verbindung.

Der Auftragnehmer verpflichtet sich ferner ausdrücklich, dafür Sorge zu tragen, dass Daten des Auftraggebers während ihrer Speicherung und Verarbeitung beim Auftragnehmer nicht unbefugt kopiert werden können.

e) Eingabekontrolle

Im Rahmen der Eingabekontrolle stellt der Auftragnehmer sicher, dass für alle Eingaben überprüft werden kann, ob und von wem personenbezogene Daten eingegeben, gelöscht oder verändert worden sind. Die Eingabekontrolle erfolgt über die systeminterne Protokollierung. Auf Verlangen des Auftraggebers ist diesem der aktuelle Stand der Protokollierungsdaten zugänglich zu machen.

f) Auftragskontrolle

Der Auftragnehmer stellt sicher, dass personenbezogene Daten des Auftraggebers ausschließlich nach dessen Weisungen verarbeitet werden können. Der Auftragnehmer ist daher verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit diese Auskünfte Daten und Unterlagen des Auftraggebers betreffen. Ferner verpflichtet sich der Auftragnehmer, die Kontrolle der Datenverarbeitung durch den Auftraggeber jederzeit zu dulden und zu unterstützen.

g) Verfügbarkeitskontrolle

Der Auftragnehmer schützt die personenbezogenen Daten im Umfang und gemäß den Vereinbarungen des zwischen Auftragnehmer und Auftraggeber geschlossenen Hauptvertrags vor zufälliger Zerstörung oder Verlust. Er gewährleistet die rasche Wiederherstellung der Verfügbarkeit personenbezogener Daten und des Zugangs zu diesen auch bei einem technischen Zwischenfall oder einer ungewöhnlichen Belastung der Systeme.

h) Trennungskontrolle

Der Auftragnehmer hat durch Organisation seiner Arbeitsprozesse sicherzustellen, dass die Daten des Auftraggebers nicht mit den Daten anderer Kunden vermischt werden oder anderen Kunden bekannt werden können. Innerhalb von Datenverarbeitungsanlagen kann dieses durch Zugriffsberechtigungen sichergestellt werden.

i) Wirksamkeitskontrolle

Der Auftragnehmer hat ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzuführen und die Ergebnisse zu dokumentieren. Dazu gehört die Sicherstellung der Benachrichtigungspflichten gegenüber Aufsichtsbehörden und Betroffenen bei Verletzungen des Schutzes personenbezogener Daten durch die Einführung von Überwachungsmaßnahmen, die geeignet sind, Schutzverletzungen und deren Auswirkungen rechtzeitigt festzustellen und deren mögliche Auswirkungen zu bestimmen. Die Dokumentation ist dem Auftraggeber auf Verlangen zur Verfügung zu stellen.

(3) Der Auftragnehmer stellt dem Auftraggeber die für das Verzeichnis nach Art. 30 Abs. 1 DSGVO notwendigen Angaben zur Verfügung.

(4) Der Auftragnehmer stellt sicher, dass die zur Verarbeitung der Daten des Auftraggebers befugten Personen gemäß Art. 28 Abs. 3 Satz 2 lit. b DSGVO oder aufgrund einer gesetzlichen Regelung zur Verschwiegenheit verpflichtet sind und in die Schutzbestimmungen des Datenschutzrechtes eingewiesen worden sind. Der Auftragnehmer weist dem Auftraggeber die wirksame Verpflichtung seiner Mitarbeiter auf das Datengeheimnis auf Verlangen nach. Der Auftragnehmer gibt dem Datenschutzbeauftragten des Auftraggebers zu diesem Zweck die Verpflichtungserklärungen zur Kenntnis.

(5) Der Auftragnehmer teilt dem Auftraggeber die Kontaktdaten des bestellten betrieblichen Datenschutzbeauftragten wie folgt mit:

Paul Köhler
BITsic -Datenschutz und Informationssicherheit-
Untere Kampstraße 12
33181 Fürstenberg
Tel.: 02953 99244
Fax: 02953 99245
Mob: 0175 2206923

Mail: paul.koehler@bitsic.de
http: www.bitsic.de

und informiert den Auftraggeber bei einer Änderung.

(6) Stellt der Auftraggeber fest, dass eine der in der Anlage 1 beschriebenen und festgelegten Schutzmaßnahmen nicht oder nicht mehr wirksam ist und hierdurch, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führen kann, teilt er dies dem Auftraggeber unverzüglich mit. Die Mitteilung muss folgende Informationen enthalten:

a) 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;

b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

d) 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.

Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Auftragnehmer diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

(7) Er unterstützt den Auftraggeber bei der Erfüllung seiner Benachrichtigungs- und Auskunftspflichten gegenüber Aufsichtsbehörden und Betroffenen. Er trägt hierfür durch die Einführung von Überwachungsmaßnahmen Sorge, die geeignet sind, Schutzverletzungen und deren Auswirkungen rechtzeitig festzustellen und deren mögliche Auswirkungen zu bestimmen. Er trägt durch geeignete technische und organisatorische Maßnahmen dafür Sorge, dass der Auftraggeber seine Pflicht zur Benachrichtigung aller Empfänger von Daten über eine Berichtigung oder Löschung der personenbezogenen Daten oder der Einschränkung der Verarbeitung sowie seine Pflicht zur Übermittlung von bereitgestellten personenbezogenen Daten an den Betroffenen oder an einen anderen Verantwortlichen in einem strukturierten, gängigen und maschinenlesbaren Format (Recht auf Datenübertragbarkeit) erfüllen kann..

(8) Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Der Auftragnehmer wird bei Beendigung des Vertragsverhältnisses alle vom Auftraggeber überlassenen Datenträger sowie gefertigte Kopien vollständig an den Auftraggeber zurückgeben, es sei denn, der Auftraggeber verlangt eine Löschung der Daten. Der Auftragnehmer weist dem Auftraggeber in diesem Fall die ordnungsgemäße Löschung der Daten durch ein Löschprotokoll oder einen anderes zum Nachweis geeignetem Dokument nach. Der Auftragnehmer wird in diesem Dokument die Art der Löschung konkret beschreiben.

(9) Die vom Auftragnehmer konkret getroffenen technischen und organisatorischen Maßnahmen sind in der **Anlage 1** mit dem Titel „Technische und organisatorische Maßnahmen“ verbindlich festgelegt. Änderungen dieser Maßnahmen sind nach Mitteilung an den Auftraggeber und dessen Genehmigung oder bei Maßnahmen, die ausschließlich zu einer Erhöhung des Sicherheitsniveaus führen nach Mitteilung an den Auftraggeber zulässig.

(10) Jedwede Übermittlung personenbezogener Daten in ein Drittland, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der Auftragsverarbeiter die in der DSGVO niedergelegten Bedingungen einhält; dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation. Soweit sich die Übermittlung auf geeignete Garantien i.S.d. Art. 46 DSGVO stützt, sind diese gegenüber dem Auftraggeber nachzuweisen. Stützt sich die Übermittlung auf eine Ausnahmeregel des Art. 49 DSGVO so hat der Auftragnehmer die Garantien und die von ihm vorgenommene Beurteilung schriftlich ausführlich dokumentiert nach Genehmigung durch den Auftraggeber im Verzeichnis gem. Art. 30 DSGVO aufzunehmen.

(5) PFLICHTEN DES AUFTRAGGEBERS

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Über die Herausgabe oder Löschung der Daten nach Vertragsende muss der Auftraggeber bis zum Vertragsende entschieden haben. Trifft der Auftraggeber bis zu diesem Zeitpunkt keine Entscheidung, werden die Daten ordnungsgemäß nach Stand der Technik gelöscht.

(6) ANFRAGEN UND AUSKUNFTS-, SPERRUNGS- ODER LÖSCHVERLANGEN BETROFFENER

(1) Ist der Auftraggeber aufgrund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer ihn dabei unterstützen, diese Informationen bereit zu stellen, wenn der Auftraggeber den Auftragnehmer hierzu schriftlich auffordert.

(2) Der Auftraggeber ist auch für die Berichtigung, Sperrung und Löschung der Daten Betroffener verantwortlich. Der Auftragnehmer unterstützt ihn bei den dabei anfallenden Arbeiten und wird die Weisungen des Auftraggebers unverzüglich durchführen und den Auftraggeber über die erfolgte Berichtigung, Sperrung und Löschung informieren.

(3) Stellt ein Betroffener eine Anfrage oder einen Antrag an den Auftragnehmer, wird dieser die Anfrage bzw. den Antrag unverzüglich unter Angabe des Zeitpunkts des Zugangs der Anfrage beim Auftragnehmer an den Auftraggeber weiterleiten.

2 Kontrollpflicht des Auftraggebers

(1) Der Auftraggeber kann sich vor Vertragsbeginn und danach in regelmäßigen Abständen nach rechtzeitiger Anmeldung zu Prüfzwecken in den Betriebsstätten des Auftragnehmers zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsverarbeitung einschlägigen Datenschutzgesetze überzeugen oder einen Dritten damit beauftragen.

(2) Der Auftragnehmer unterstützt den Auftraggeber bei der Prüfung in den Betriebsstätten des Auftragnehmers im erforderlichen Umfang und wird die Kontrollen des Auftraggebers dulden.

(7) SUBUNTERNEHMER

(1) Es ist dem Auftragnehmer grundsätzlich nicht gestattet, die Vertragserfüllung insgesamt oder hinsichtlich einzelner Teilleistungen an Subunternehmer ohne vorherige ausdrückliche Zustimmung des Auftraggebers zu übertragen. Hierzu muss der Auftragnehmer dem Auftraggeber den Namen und die genaue Anschrift des in Betracht kommenden Subunternehmers mitteilen (**siehe Anlage 2 Unterauftragnehmer**) sowie Auskunft über die getroffenen Maßnahmen und Ergebnisse zur Feststellung der hinreichenden Garantien für eine Verarbeitung im Einklang mit den Anforderungen der DSGVO und den Schutz der Rechte der betroffenen Person geben. Den Auftraggeber trifft keine Pflicht, die gewünschte Genehmigung zu erteilen.

(2) Wenn Subunternehmer durch den Auftragnehmer eingeschaltet werden sollen, so werden die vertraglichen Vereinbarungen so gestaltet, dass sie allen Anforderungen zwischen den Vertragspartnern aus diesem Vertrag entsprechen. Dem Auftraggeber sind Kontroll- und Überprüfungsrechte entsprechend Ziffer 10 dieser Zusatzvereinbarung auch durch den Subauftragnehmer einzuräumen. Ebenso ist der Auftraggeber berechtigt, auf schriftliche Anforderung von dem Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

3 Haftung, Sonstiges

(1) Jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat. Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Der Auftragnehmer unterstützt den Auftraggeber bei den erforderlichen Nachweisen. Ist mehr als ein Verantwortlicher oder mehr als ein Auftragsverarbeiter bzw. sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie gemäß Art. 82 Abs. 2 und 3 DSGVO für einen durch die Verarbeitung verursachten Schaden verantwortlich, so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist. Hat ein Verantwortlicher oder Auftragsverarbeiter gemäß Art. 82 Abs. 4 DSGVO vollständigen Schadenersatz für den erlittenen Schaden gezahlt, so ist dieser Verantwortliche oder Auftragsverarbeiter berechtigt, von den übrigen an derselben Verarbeitung beteiligten für die Datenverarbeitung Verantwortlichen oder Auftragsverarbeitern den Teil des Schadenersatzes zurückzufordern, der unter den in Art. 82 Abs. 2 DSGVO festgelegten Bedingungen ihrem Anteil an der Verantwortung für den Schaden entspricht.

(2) Liegen die hinreichenden Garantien i.S.d. Art. 28 Abs. 1 DSGVO nicht mehr vor oder zeigt sich ein Mangel erst nach Begründung des Auftragsverhältnisses und wird dieser nicht innerhalb einer vom Auftraggeber gesetzten Frist abgestellt, haftet der Auftragnehmer für den hierdurch entstehenden Schaden.

(3) Stellt der Auftraggeber im Rahmen seiner regelmäßigen Kontrolle einen Verstoß gegen die gesetzlichen oder vertraglichen Regelungen fest, hat der Auftragnehmer diese innerhalb einer angemessenen Frist zu beseitigen.

(4) Im Fall eines vom Auftragnehmer zu verantwortenden Verstoßes gegen eine Verpflichtung aus diesem Vertrag kann der Auftraggeber vom Auftragnehmer für jeden Einzelfall eine angemessene Vertragsstrafe verlangen. Ein Einzelfall liegt dann vor, wenn eine einzige Handlung kausal ist für einen oder zeitgleich auch mehrere Verstöße gegen die o.g. Verpflichtungen oder wenn mehrere selbständige Handlungen vorliegen, diese aber immer dieselbe(n) Verpflichtung(en) verletzen und darüber hinaus in

einem engen, räumlichen und zeitlichen Zusammenhang stehen. Der Auftraggeber kann die Höhe der Vertragsstrafe unter Berücksichtigung der Schwere des Verstoßes nach billigem Ermessen festsetzen, wobei die Vertragsstrafe mindestens 5.000€ pro Einzelfall, maximal jedoch 300.000 € pro Vertragsjahr bei einem Dauerschuldverhältnis oder mindestens 15% und maximal 90% der vereinbarten Gesamtvergütung betragen wird. Die Verpflichtung zur Zahlung einer Vertragsstrafe besteht nicht, wenn der Auftragnehmer nachweist, dass er oder ein von ihm beauftragter Subunternehmer den Verstoß nicht zu vertreten hat. Hierbei gilt der gesetzliche Haftungsmaßstab des § 276 BGB, wobei eine Verletzung der zugesicherten technisch-organisatorischen Maßnahmen als eine übernommene Garantie gewertet wird. Im Falle der Geltendmachung der Vertragsstrafe wird die Vertragsstrafe auf einen Schadensersatzanspruch angerechnet. Der Anspruch auf Erstattung eines die Vertragsstrafe übersteigenden Schadens bleibt unberührt.

(5) Der Auftragnehmer haftet für ein Verschulden seines Subunternehmers sowie dessen weitere Subunternehmer wie für eigenes Verschulden.

(6) Sollte die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter, auch soweit es sich um staatliche Maßnahmen handelt, gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftraggeber wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den Daten beim Auftraggeber liegt. Die Einrede des Zurückbehaltungsrechts § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(7) Die Unwirksamkeit einer Bestimmung dieser Vereinbarung berührt die Gültigkeit der übrigen Bestimmungen nicht. Sollte sich eine Bestimmung als unwirksam erweisen, werden die Parteien diese durch eine neue ersetzen, die dem von den Parteien Gewollten am nächsten kommt.

(8) Sämtliche Vereinbarungen, die eine Änderung, Ergänzung oder Konkretisierung dieser Anlage beinhalten, sowie besondere Zusicherungen und Abmachungen oder eine Änderung dieser Regel selbst sind schriftlich oder elektronisch niederzulegen.

(9) Es besteht zwischen den Parteien Einigkeit darüber, dass eventuelle "Allgemeine Geschäftsbedingungen" des Auftragnehmers auf diese Vereinbarung keine Anwendung finden.

(10) Es gilt deutsches Recht.

(11) Im Fall von Widersprüchen von Regelungen dieser Vereinbarung und Regelungen aus sonstigen Vereinbarungen gehen die Regelungen dieser Vereinbarung vor.

(12) Die Anlagen sind verbindlicher Bestandteil dieser Vereinbarung.

Düsseldorf,

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift Auftragnehmer	Unterschrift Auftraggeber

Anlage 1

Technische und organisatorische Maßnahmen

der

alpha EDV Systemhaus GmbH & Co. KG
Kronprinzenstraße 82-84
40217 Düsseldorf

(Auftragnehmer)

Als nicht-öffentliche Stelle, die im Auftrag personenbezogene Daten erhebt, verarbeitet oder nutzt, müssen Auftragnehmer technische und organisatorische Maßnahmen treffen, die erforderlich sind, um die Ausführung der Datenschutzvorschriften zu gewährleisten. Insbesondere sind Vertraulichkeit, Integrität, Verfügbarkeit und Systembelastbarkeit im Zusammenhang mit der Datenverarbeitung sicherzustellen. Die folgenden technischen und organisatorischen Maßnahmen sind dazu beim Auftragnehmer umgesetzt:

1. Zutrittskontrolle

Der Auftragnehmer hat angemessene Vorkehrungen zu treffen, um Unbefugte am Zutritt zu den Datenverarbeitungssystemen zu hindern:

Dies soll gewährleistet werden durch:

Bürogebäude (keine Serversysteme / Datenspeicherung)

- Zutrittsberechtigungen für Mitarbeiter und Dritte sowie entsprechende Dokumentation
- Manuelles Schließsystem
- Sicherung dezentraler Datenverarbeitungsanlagen und PCs (Verschlüsselung, tägliches Backup, BIOS-Kennwörter)

Rechenzentrum (Serversysteme / Datenspeicherung)

- Zutrittsberechtigungen für Mitarbeiter und Dritte sowie entsprechende Dokumentation
- Alarmanlage
- mehrstufiges Schließsystem (Chipkarte, PIN, Biometrie)
- Bewegungsmelder
- Videoüberwachung
- Schlüsselbuch
- Gebäudesicherung (angriffshemmende Verglasung, Alarmanlage, Wachleute, Kontrolle von Rinnen und Schächten)

2. Zugangskontrolle

Der Auftragnehmer versichert, dass die zur Nutzung des Datenverarbeitungssystems befugten Personen nur im Umfang der erteilten Berechtigung auf die Daten zugreifen können.

Dies soll gewährleistet werden durch:

- Zugang zu Rechnern / Systemen (Authentifikation mit Benutzer + Passwort)
- Einsatz von Anti-Viren-Software
- Einsatz von Firewalls
- Einsatz von VPN-Technologie

- Verschlüsselung von Datenträgern
- Festlegung der nutzungsberechtigten Personen
- Identifikation und Authentifizierung der Benutzer
- Sicherung der Datenstationen, Netze und Übertragungsleitungen
- Verschlüsselung der zu übertragenden Daten
- Protokollierung der Benutzer und deren Aktivitäten
- Verwaltung der Benutzerberechtigungen
- Passwortvergabe / Passwortregeln
- Sperrung von Terminals nach Inaktivität

3. Zugriffskontrolle

Der Auftragnehmer trifft angemessene Maßnahmen, um zu verhindern, dass seine Datenverarbeitungssysteme von Unbefugten zu Datenübertragungszwecken genutzt werden. Außerdem hat der Auftragnehmer unbefugtes Lesen, Kopieren, Verändern oder Löschen der Datenträgermedien oder der gespeicherten Daten sowie unbefugte Eingaben in den Arbeitsspeicher zu verhindern.

Dies soll gewährleistet werden durch:

- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Verschlüsselung von Datenträgern,
- Anlegen von revisionsfähigen Benutzerprofilen
- Identifikation und Authentifizierung der Benutzer
- Maschinelle Überprüfung der Berechtigungen
- Berechtigungskonzept
- Datenträgerverwaltung
- Anzahl der Administratoren auf das "Notwendigste" reduziert
- Passwortrichtlinie inkl. Länge und Wechsel
- Sichere Aufbewahrung von Datenträgern
- Verwaltung der Benutzerrechte durch Systemadministratoren
- Richtlinie zur Kontrolle von Sicherungskopien

4. Weitergabekontrolle

Der Auftragnehmer ist verpflichtet, durch den Einsatz von Datenübertragungseinrichtungen das Verifizieren und Rückverfolgen der Standorte, in die die Daten der Betroffenen übertragen werden, zu ermöglichen.

Dies soll gewährleistet werden durch:

- Einrichtungen von VPN-Tunneln
- Festlegung der für die Übermittlung oder den Transport Berechtigten
- Regelungen für die Versandart und Festlegung des Transportweges
- Sicherung des Übertragungs- und Transportweges
- Verschlüsselung der Daten
- Überprüfung aller Daten und Datenträger hinsichtlich Virenbefall
- Firewall
- Protokollierungsmaßnahmen
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- Sorgfältige Auswahl von Transportpersonal und -fahrzeugen
- Löschung von Datenresten vor Datenträgeraustausch

5. Eingabekontrolle

Der Auftragnehmer stellt sicher, dass der Zeitpunkt und Ort der Dateneingabe des Betroffenen in das Datenverarbeitungssystem rückwirkend überprüft und festgehalten werden kann.

Dies soll gewährleistet werden durch:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Benutzeridentifikation
- Protokollauswertungssysteme
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten

6. Organisationskontrolle

Der Auftragnehmer verwaltet seine interne Organisation entsprechend der Anforderungen des Datenschutzrechts.

Dies soll gewährleistet werden durch:

- Interne Datenverarbeitungsrichtlinien und -verfahren, Leitfaden, Arbeitsanweisungen, Vorgangsbeschreibungen und Programmier-, Test- und Freigabebestimmungen (im Entstehen)
- Formulierung eines Datensicherheitskonzepts (im Entstehen)
- Formulierung eines Notfallplans (Sicherheitskontingent-Plan).

7. Auftragskontrolle

Der Auftragnehmer wird die vom Auftraggeber übermittelten Daten nur nach dessen Weisung verarbeiten.

Dies soll gewährleistet werden durch:

- Einsatz von Aktenvernichtern
- Ordnungsgemäße Vernichtung von Datenträgern
- Physische Löschung von Datenträgern vor deren Wiederverwendung
- Protokollierung der Vernichtung von Daten
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Verpflichtung der Mitarbeiter auf das Datengeheimnis (§ 5 BDSG)
- Klare Vertragsgestaltung und -ausführung
- Abgrenzung der Kompetenzen und Pflichten zwischen Auftragnehmer und Auftraggeber

8. Kontrolle der Trennung der Daten

Der Auftragnehmer ermöglicht die Trennung von Daten, die zu unterschiedlichen Zwecken erhoben wurden.

Dies soll gewährleistet werden durch:

- Speicherung der Daten in unterschiedlichen Datenpools (physische Trennung)
- Berechtigungsrichtlinie (logische Trennung)

- Berechtigungskonzept;
- Festlegung von Datenbankrechten

9. Angaben zur Personenzahl

Anzahl der Beschäftigten (regelmäßig): 6 Mitarbeiter

Anzahl der Personen, die personenbezogene Daten verarbeiten (regelmäßig): 6 Mitarbeiter

Anzahl der Personen mit Zugriff auf Daten des Verantwortlichen / des Auftraggebers: 4 Mitarbeiter

10. Zusätzliche Bemerkungen

_____

Düsseldorf,

Anlage 2 Unterauftragnehmer

Rechenzentrumsleistungen

dogado GmbH
Saarlandstraße 25
44139 Dortmund
T: +49 (231) 286620-0
F: +49 (231) 286620-20
M: info@dogado.de
W: http://www.dogado.de

Colocation Full Rack
Full Rack 42HE

- 2 x GigE Uplink / RJ45
- Stromzuführung 2 x 16 Ampere (Zwei separat abgesicherte Phasen A + B Feed)
- max. Leistungsaufnahme 2,5 KW
- Kundeneigener IP Adressbereich (Vergabe nach RIPE - Richtlinien)
- 20Mbit/s CDR (Committed Data Rate) gem. 95/5 je Monat gem. 95/5 percentile Abrechnung.
- Zutrittskontrolle