Allgemeine Bestimmungen über Datenverarbeitung im Auftrag

1 Geltungsbereich, Vertragsgegenstand

1.1 Die nachfolgenden Bestimmungen gelten für alle Vertragsbeziehungen, vertragsähnlichen Beziehungen und vorvertraglichen Verhandlungen der Microdat GmbH, Feldstraße 8, 91080 Uttenreuth (im Folgenden insgesamt: „Auftragnehmer“) mit ihren Kunden (im Folgenden: „Kunde“ oder „Auftraggeber“), wenn und soweit der Auftragnehmer personenbezogene Daten gemäß Art. 28 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 (DSGVO) im Auftrag verarbeitet.

1.2 Die Vorschriften der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 (DSGVO), des Bundesdatenschutzgesetzes (BDSG), insbesondere jeweils der Vorschriften über die Datenverarbeitung im Auftrag, finden Anwendung.

2 Datenverarbeitung im Auftrag

2.1 Der Auftragnehmer gewährleistet den Schutz der Rechte der betroffenen Person durch geeignete technische und organisatorische Maßnahmen, so dass die Datenverarbeitung im Einklang mit den gesetzlichen Anforderungen der DSGVO und des BDSG erfolgt.

2.2 Die nachfolgenden Bestimmungen regeln die datenschutzrechtlichen Maßnahmen sowie die Rechte und Pflichten des Auftraggebers und des Auftragnehmers zur Erfüllung der vorstehend genannten Regelungen.

2.3 Der Auftragnehmer verarbeitet die vom Auftraggeber überlassenen Daten ausschließlich für den Auftraggeber und nur im Rahmen des zugrundeliegenden Auftrags sowie gemäß den Weisungen des Auftraggebers, soweit sich nicht aus zwingenden gesetzlichen Vorgaben oder Anordnungen der zuständigen Aufsichtsbehörde etwas anderes ergibt. 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.

3 Datenarten

3.1 Die Datenverarbeitung können folgende Personenkreise betreffen:

3.1.1 Mitarbeiter

3.1.2 Kunden

3.1.3 Auftragnehmer

3.2 Gegenstand der Verarbeitung können folgende Datenarten sein:

3.2.1 Personenstammdaten

3.2.2 Kommunikationsdaten (z. B. Email, Telefon)

3.2.3 Vertragsstammdaten (z. B. Vertragsbeziehung)

3.2.4 Kommunikationsdaten

3.2.5 Kundenhistorie

3.2.6 Planungs- und Steuerungsdaten

4 Technische und organisatorische Maßnahmen

4.1 Der Auftragnehmer sichert ein dem Risiko für die Rechte und Freiheiten der Betroffenen adäquates Schutzniveau der personenbezogenen Daten zu. Zu diesem Zweck verpflichtet sich der Auftragnehmer, seine innerbetriebliche Organisation und die erforderlichen technischen und organisatorischen Maßnahmen unter Berücksichtigung des jeweiligen Stands der Technik, der Implementierungskosten und der Art, des Umfangs sowie der Umstände und Zwecke der Verarbeitung und der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen so zu gestalten und laufend zu aktualisieren, dass diese den besonderen Anforderungen des Datenschutzes nach der DSGVO entsprechen und den Schutz der Rechte der betroffenen Personen gewährleisten.

4.2 Die technischen und organisatorischen Maßnahmen umfassen insbesondere

- die dauerhafte Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung der Daten,
- die rasche Wiederherstellung der Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen im Fall eines physischen oder technischen Zwischenfalls und
- die Einführung und das Vorhalten von Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

4.3 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4.4 Der Auftragnehmer kann die Eignung der nach Art. 32 DSGVO zu treffenden technisch-organisatorischen Maßnahmen durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO oder ein Datenschutzsiegel oder Prüfzeichen nach Art. 42 DSGVO nachweisen, das für die vertragsgegenständlichen Verarbeitungsverfahren und Orte erteilt und für die unter diese Vereinbarung fallenden Verarbeitungsverfahren relevant ist. Der Auftragnehmer hat Veränderungen am

Zertifikat oder dessen Ablauf dem Auftraggeber unverzüglich mitzuteilen. Die Kontroll- und Auditrechte des Auftraggebers bleiben unberührt.

4.5 Die in der Anlage 1 aufgeführten technisch-organisatorischen Maßnahmen werden verbindlich festgelegt.

5 Berichtigung, Löschung und Sperrung von Daten

Die zu verarbeitenden Daten dürfen nur nach Anweisung bzw. nach vorheriger Zustimmung des Auftraggebers berichtigt, gelöscht oder gesperrt werden. Soweit sich ein Betroffener wegen einer Berichtigung, Löschung oder Sperrung von Daten unmittelbar an den Auftragnehmer wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

6 Pflichten des Auftragnehmers

6.1 Verarbeitungspflichten

Der Auftragnehmer führt den Auftrag ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers durch. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben.

Auszüge, Kopien oder Duplikate von Daten oder Datenträgern dürfen ohne Wissen des Auftraggebers nur hergestellt und verwendet werden, soweit dies für die Ausführung des Auftrages oder zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich ist oder eine gesetzliche oder sonstige Aufbewahrungspflicht besteht. Eventuell hergestellte Auszüge, Kopien oder Duplikate sind nach Abschluss der Verarbeitung oder Nutzung vom Auftragnehmer unverzüglich sicher zu löschen bzw. datenschutzgerecht zu vernichten oder dem Auftraggeber auszuhändigen.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nicht oder nur nach Weisung des Auftraggebers erteilen. Auskünfte an Mitarbeiter des Auftraggebers darf der Auftragnehmer nur gegenüber den autorisierten Personen erteilen.

Der Auftragnehmer verpflichtet sich, nur solche Software, Daten oder Datenträger einzusetzen, die zuverlässig auf Freiheit von schädlicher Software geprüft sind, um ein Einschleusen von Viren etc. zu vermeiden.

Der Auftragnehmer verpflichtet sich, bei Wartungs- und Servicetätigkeiten den Datenzugriff auf das unverzichtbare Mindestmaß zu beschränken und personenbezogene Daten ausschließlich für Zwecke der Leistungserbringung zur Kenntnis zu nehmen und keinesfalls anderweitig zu verarbeiten oder zu nutzen. Ein Zugriff auf personenbezogene Daten oder eine Kenntnisnahme von personenbezogenen Daten über das zur Erfüllung des Auftrages hinausgehende Maß ist streng untersagt. Beim Zugriff auf personenbezogene Daten dürfen keine Veränderungen vorgenommen werden. Versehentlich vorgenommene Veränderungen sind dem Auftraggeber bekannt zu geben. Auf Verlangen des Auftraggebers sind solche Veränderungen nach Abschluss der Arbeiten rückgängig zu machen.

Nach Erfüllung des Auftrages sind ggf. vom Auftragnehmer auf seinem System

gespeicherte Daten aller Art des Auftraggebers sicher zu löschen.

6.2 Duldungspflichten bei Kontrollen

Der Auftragnehmer verpflichtet sich, in Prüfungen durch den Auftraggeber die Einhaltung der getroffenen technischen und organisatorischen Maßnahmen nachzuweisen, Auskünfte zu erteilen und die entsprechenden Unterlagen vorzulegen bzw. Einsicht in die erforderlichen Unterlagen und Systeme zu gewähren und nach vorheriger Abstimmung entsprechende Prüfungen des Auftraggebers vor Ort zu dulden und zu unterstützen. Er verpflichtet sich, bei datenschutz- und datensicherheitsrelevanten Vorfällen alle erforderlichen Auskünfte zu erteilen und die Aufklärung derartiger Vorfälle nach Möglichkeit zu unterstützen.

Der Nachweis angemessener technischer und organisatorischer Maßnahmen kann auch durch Vorlage von Testaten oder Zertifikaten oder durch eine Zertifizierung bzw. ein Datenschutzaudit einer unabhängigen Einrichtung bzw. eines autorisierten Sachverständigen geführt werden. Unabhängig von diesen Nachweisen ist der Auftragnehmer verpflichtet, Kontrollen durch den Auftraggeber nach dieser Vereinbarung zu dulden.

6.3 Informationspflichten

Der Auftragnehmer ist verpflichtet, wesentliche Änderungen in den technischen und organisatorischen Verhältnissen, die die Sicherheit und Ordnungsmäßigkeit der Durchführung der Auftragsleistungen herabsetzen, unaufgefordert dem Auftraggeber zu melden.

Der Auftragnehmer unterrichtet den Auftraggeber über Kontrollen der Aufsichtsbehörde für den Datenschutz, insbesondere gem. Art. 58 DSGVO, und über eventuelle Maßnahmen und Auflagen zum Schutz der personenbezogenen Daten.

Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen. Er informiert den Auftraggeber unverzüglich über das Erlöschen oder den Widerruf von Zertifikaten oder von Maßnahmen gem. Art. 41 Abs. 4 DSGVO.

Der Auftragnehmer teilt dem Auftraggeber Name und Kontaktdaten und Änderungen in der Person des betrieblichen Datenschutzbeauftragten oder, wenn keine Bestellpflicht besteht, den Namen und die Kontaktdaten der sonstigen zuständigen Stelle mit.

6.4 Mitwirkungs- und Unterstützungspflichten

Der Auftragnehmer verpflichtet sich, im Rahmen des Art. 28 Abs. 3 lit. e und f DSGVO, die für das Verzeichnis von Verarbeitungstätigkeiten sowie für die Risikoermittlung und eventuelle Datenschutzfolgenabschätzung erforderlichen Informationen unverzüglich zur Verfügung zu stellen und, soweit es seinen Verantwortungsbereich betrifft, im erforderlichen Umfang bei der Ermittlung der Risiken und einer eventuellen Datenschutzfolgenabschätzung mitzuwirken sowie den Auftraggeber bei der Erfüllung der Rechte der Betroffenen zu unterstützen.

6.5 Organisationspflichten

Der Auftragnehmer verpflichtet sich zur Einrichtung von Maßnahmen und Dokumentationen, die eine Kontrolle und Nachvollziehbarkeit aller mit der Auftragsverarbeitung zusammenhängenden Tätigkeiten und Verarbeitungsprozesse im Sinne

einer Auftragskontrolle und der Ordnungsmäßigkeit der Datenverarbeitung ermöglichen. Datenschutzvorfälle und sonstige sicherheitsrelevante Störungen bei der Verarbeitung der Daten des Auftraggebers sind einschließlich ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen zu dokumentieren und dem Auftraggeber zu melden.

Wird die Verarbeitung von Privatwohnungen oder von einem dritten Ort aus durchgeführt, ist der Auftraggeber darüber zu informieren. Der Auftragnehmer verpflichtet sich, durch geeignete Regelungen und Sicherheitsvorkehrungen die Wahrung der Vertraulichkeit der Daten sowie die Sicherheit und Kontrollierbarkeit der Verarbeitung im gleichen Maße zu gewährleisten, wie dies bei einer Durchführung der Serviceleistung vom Ort des Auftragnehmers aus der Fall ist. Soll davon abgewichen werden, bedarf dies einer gesonderten schriftlichen Zustimmung des Auftraggebers.

7 Durchführung der Fernwartung

Werden Auftragsleistungen im Wege der Fernwartung durchgeführt, gelten zusätzlich folgende Vereinbarungen:

7.1 Der Auftragnehmer führt die Fernwartung ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers durch. Die Fernwartung erfolgt, soweit möglich, ohne gleichzeitige Speicherung von Daten.

7.2 Der Auftragnehmer muss personenbezogene Daten, die er bei der Fernwartung erhalten oder gewonnen hat, unverzüglich sicher löschen oder dem Auftraggeber zurückgeben, wenn sie für die Durchführung der Fernwartungsarbeiten nicht mehr erforderlich sind. Etwaige dem Auftragnehmer übergebene Daten oder Datenträger mit personenbezogenen oder sonstigen vertraulichen Daten sind dem Auftragnehmer nach Abschluss der Fernwartungsarbeiten unverzüglich zurückzugeben oder sicher zu vernichten.

7.3 Notwendige Datenübertragungen zu Zwecken der Fernwartung müssen in hinreichend verschlüsselter Form erfolgen.

7.4 Der Beginn der Fernwartung ist vom Auftragnehmer anzukündigen, um dem Auftraggeber die Möglichkeit zu geben, die Maßnahmen der Fernwartung zu verfolgen. Die Mitarbeiter des Auftragnehmers verwenden nach dem Stand der Technik hinreichend sichere Identifizierungs- und Einwahlverfahren. Die Fernwartung darf nur über nach dem Stand der Technik sichere Leitungen abgewickelt werden.

7.5 Der Auftragnehmer verpflichtet sich, nur aufgrund von Störungsmeldungen des Auftraggebers per Fernwartung oder aufgrund sonstiger ausdrücklicher Anforderungen des Auftraggebers mittels Remote-Zugriff auf Software und Daten zuzugreifen und nach Beseitigung der Störung per Fernwartung oder bei Beendigung des Remote-Zugriffs dem Auftraggeber Serviceberichte zu erstellen.

7.6 Der Auftraggeber ist berechtigt, die Fernwartungsarbeiten von einem Kontrollbildschirm aus zu verfolgen. Soweit der Auftragnehmer daran mitwirken muss, gewährleistet er, dass dies möglich ist. Der Auftraggeber ist ferner berechtigt, die Fernwartungsaktivitäten des Auftragnehmers zu protokollieren, die Protokolle zu überprüfen und eine angemessene Zeit aufzubewahren.

7.7 Wird die Fernwartung von Privatwohnungen oder von einem dritten Ort aus durchgeführt, verpflichtet sich der Auftragnehmer, durch geeignete Regelungen und Sicherheitsvorkehrungen die Wahrung der Vertraulichkeit der Daten sowie die Sicherheit und Kontrollierbarkeit der Serviceleistung im gleichen Maße zu gewährleisten, wie dies bei einer Durchführung der Serviceleistung von der Wartungszentrale aus der Fall ist. Soll davon abgewichen werden, bedarf dies einer gesonderten schriftlichen Zustimmung des Auftraggebers.

7.8 Der Auftraggeber hat das Recht, die Fernwartung zu unterbrechen, wenn der Auftragnehmer von den vereinbarten Sicherheitsmaßnahmen abweicht oder die Fernwartung mit nicht vereinbarten Hard- und Softwarekomponenten durchgeführt wird.

8 Unterauftragnehmer

Die Einschaltung von Unterauftragnehmern ist nur zulässig, wenn der Auftraggeber vor der Vergabe der Auftragsleistung schriftlich zugestimmt hat. Der Auftraggeber kann bei Vorliegen eines wichtigen Grundes, insbesondere bei einer Gesetzes- oder Vertragsverletzung, seine Zustimmung zur Unterbeauftragung widerrufen. Die Unterbeauftragung ist dann unverzüglich einzustellen. Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem Unterauftragnehmer so zu gestalten, dass sie den Datenschutzbestimmungen dieses Vertrages entsprechen. Er hat die Einhaltung dieser Pflichten regelmäßig zu überprüfen. Die Weiterleitung von Daten an den Unterauftragnehmer ist erst zulässig, wenn ein Vertrag nach diesen Auflagen abgeschlossen worden ist und der Unterauftragnehmer alle Anforderungen dieses Vertrages erfüllt hat.

Bei der Unterbeauftragung sind dem Unterauftragnehmer die gleichen vertraglichen Regelungen aufzuerlegen, wie sie für den Auftragnehmer gelten. Dem Auftraggeber sind gegenüber dem Unterauftragnehmer die gleichen Weisungs-, Kontroll- und Überprüfungsrechte entsprechend diesen Regelungen und dem Art. 28 DSGVO einzuräumen, wie sie gegenüber dem Auftragnehmer gelten. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z. B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremdvergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

Eine Beauftragung von Unterauftragnehmern außerhalb des Gebiets der Bundesrepublik Deutschland oder der Europäischen Union bzw. der Staaten des Europäischen Wirtschaftsraumes ist nur mit vorheriger Zustimmung des Auftraggebers zulässig und nur soweit ein Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 Abs. 3 DSGVO vorliegt oder durch andere geeignete Garantien i. S. v. Art. 46 Abs. 2 DSGVO ein angemessenes Datenschutzniveau sichergestellt ist.

9 Weisungsbefugnisse des Auftraggebers

9.1 Die Verarbeitung der Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der getroffenen Auftragsbeschreibung ein Weisungsrecht in Form von Einzelanweisungen über Art, Umfang und Verfahren der Datenverarbeitung sowie über Änderungen der Verarbeitung vor. Die Weisungen betreffen insbesondere, aber nicht ausschließlich, die datenschutzkonforme Auftragsabwicklung und sonstige Handlungen zur Sicherstellung einer gesetzmäßigen Auftragsabwicklung. Weisungen werden schriftlich oder in einem geeigneten elektronischen Format erteilt. Mündliche Weisungen sind unverzüglich schriftlich oder in einem elektronischen Format zu bestätigen.

9.2 Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzvorschriften verstößt. Der Auftragnehmer kann die Ausführung der Anweisung bis zu einer Bestätigung durch den Auftraggeber aussetzen. Der Auftraggeber haftet für rechtswidrige Weisungen und stellt den Auftragnehmer insoweit von Schadensersatzansprüchen und sonstigen Forderungen frei.

9.3 Auf erstes Anfordern benennt der Auftraggeber dem Auftragnehmer weisungsberechtigte Personen des Auftraggebers und teilt danach dem Auftragnehmer Änderungen der weisungsberechtigten Person unaufgefordert unverzüglich mit.

9.4 Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

10 Kontroll- und Auditrechte des Auftraggebers

10.1 Der Auftraggeber ist befugt, vor Beginn der Datenverarbeitung und nach seinem Ermessen auch wiederholt nach vorheriger Abstimmung während der üblichen Geschäftszeiten im erforderlichen Umfang die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen, insbesondere der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen, zu kontrollieren. Hierzu ist der Auftraggeber befugt, schriftliche Auskünfte und die Vorlage von Nachweisen über die eingerichteten Datenschutzmaßnahmen sowie über die Art und Weise ihrer technischen und organisatorischen Umsetzung zu verlangen, das Grundstück und die Betriebsstätten des Auftragnehmers zu betreten, nach seinem Ermessen Prüfungen und Besichtigungen vorzunehmen und im erforderlichen Umfang in verarbeitungsrelevante Unterlagen, Verarbeitungs- und Ablaufprotokolle, Systeme und gespeicherte Daten und in Regelungen, Richtlinien und Handbücher zur Regelung der beauftragten Datenverarbeitung einzusehen.

10.2 Dazu gehören auch Nachweise über die Bestellung eines Datenschutzbeauftragten, die Verpflichtung der Mitarbeiter auf die Wahrung der Vertraulichkeit und technische und organisatorische Konzepte, z. B. Datenschutzhandbuch, einschlägige Verfahrensanweisungen und auch Verträge mit Unterauftragnehmern. Die gleichen Rechte besitzen auch Beauftragte des Auftraggebers, z. B. Gutachter oder Sachverständige, soweit sie besonders zur Verschwiegenheit verpflichtet sind oder strafbewehrten berufsständischen Schweigepflichten unterliegen.

10.3 Die Prüfung erfolgt nach vorheriger Anmeldung. In besonderen Fällen, insbesondere wenn Verarbeitungsprobleme bestehen, meldepflichtige Vorfälle aufgetreten sind oder aufsichtsrechtliche Maßnahmen anstehen oder eingeleitet worden sind, kann die Prüfung auch ohne vorherige Anmeldung erfolgen.

10.4 Der Auftraggeber hat das Recht, die Auftragsausführung zu unterbrechen, wenn er den Eindruck gewinnt, dass der Auftrag nicht weisungsgemäß ausgeführt oder unbefugt auf Dateien zugegriffen wird oder Daten unbefugt oder nicht weisungsgemäß übertragen oder verarbeitet oder genutzt werden.

10.5 Die Rechte des Auftraggebers bestehen während der Laufzeit dieser Vereinbarung und darüber hinaus bis zum Eintritt der Verjährung von Ansprüchen aus diesem Vertrag, mindestens jedoch solange der Auftraggeber personenbezogene Daten aus den beauftragten Verarbeitungen speichert.

10.6 Die vorstehenden Überprüfungsrechte unterliegen folgenden Regelungen:

10.6.1 Prüfungen dürfen nur zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt werden. Der Auftragnehmer darf die Prüfung von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen.

10.6.2 Keine der vorstehenden Regelungen gibt dem Auftraggeber oder einem mit der Prüfung beauftragten Dritten das Recht, Materialien, Informationen oder Tätigkeiten in Augenschein zu nehmen, die keinen Bezug zur Verarbeitung der Daten des Auftraggebers haben oder wenn dies zu einem Gesetzesverstoß durch den Auftragnehmer führen würde.

10.6.3 Der Auftraggeber und von diesem mit der Prüfung beauftragte Dritte ist verpflichtet, alle Informationen und Materialien, die ihnen im Rahmen der Prüfung bekannt werden, als vertrauliche Informationen des Auftragnehmers zu behandeln. Der Auftraggeber ist verpflichtet, mit den bei der Prüfung eingesetzten Dritten vor deren Einsatz eine entsprechende Vertraulichkeitsvereinbarung abzuschließen.

10.6.4 Der Auftragnehmer kann der Prüfung durch einen vom Auftraggeber mit der Vornahme der Prüfung beauftragten Mitarbeiter oder Dritten widersprechen, wenn der mit der Prüfung beauftragte Dritte in einem Wettbewerbsverhältnis zum Auftragnehmer steht oder gegen die Person sachlich begründete Einwände bestehen. Das Kontrollrecht des Auftraggebers wird hierdurch nicht berührt.

11 Pflichten des Auftraggebers

11.1 Soweit die Verarbeitungstätigkeiten im Auftrag des Auftraggebers erfolgen, obliegt diesem die Führung des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO.

11.2 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.

11.3 Im Falle einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO verpflichtet sich der Auftraggeber den Auftragnehmer bei der Abwehr des Anspruches zu unterstützen.

12 Meldung von Datenschutzverstößen

12.1 Bei einer Störung der Verarbeitung oder einer Datenschutzverletzung leitet der Auftragnehmer umgehend alle geeigneten und erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung eines eventuellen Schadens für die Betroffenen und für den Auftraggeber ein.

12.2 Der Auftragnehmer verpflichtet sich, den Auftraggeber unverzüglich über Verstöße gegen Vorschriften zum Schutz der personenbezogenen Daten oder gegen die in dieser Vereinbarung getroffenen Festlegungen zu unterrichten. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen von Vorschriften zum Schutz personenbezogener Daten oder andere Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers, die Auswirkungen auf die betroffenen Personen oder den Auftraggeber nach sich ziehen oder Schaden verursachen können. Zu den Datenschutzverstößen gehören insbesondere der Verlust der Vertraulichkeit und der Verlust oder die Zerstörung oder Verfälschung von Daten des Auftraggebers oder sonstiger vertraulicher Informationen im Sinne dieses Vertrages.

12.3 Die Meldung an den Auftraggeber umfasst alle Informationen, die für den Auftraggeber erforderlich sind, um den Vorfall und seine Meldepflicht an die Aufsichtsbehörde und die Informationspflicht der Betroffenen gem. Art. 33 und 34 DSGVO beurteilen und ggf. fristgerecht die Meldung an die Aufsichtsbehörde und ggf. die Information der Betroffenen vornehmen zu können. Die Meldung an den Auftraggeber umfasst insbesondere Angaben zur Art des Vorfalls und der Verletzung des Schutzes von personenbezogenen Daten, eine Beschreibung der wahrscheinlichen Risiken für die Interessen, Grundrechte und Grundfreiheiten der betroffenen Personen und eine Beschreibung der bereits eingeleiteten Maßnahmen zur Behebung bzw. Reduzierung eines möglichen Schadens oder sonstiger Risiken für die Betroffenen und den Auftraggeber.

12.4 Der Auftragnehmer dokumentiert den Vorfall und unterstützt den Auftraggeber bei der Erfüllung seiner Melde- und Informationspflicht gem. Art. 33 und 34 DSGVO.

13 Haftung

Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung fahrlässig oder schuldhaft verursachen.

14 Verfahren nach Beendigung des Auftrages

14.1 Nach Abschluss der Verarbeitung, spätestens nach Beendigung dieses Vertrages, hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse oder zur Leistungserfüllung hergestellten oder kopierten personenbezogenen oder sonstige vertrauliche Daten,

die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder in Abstimmung mit dem Auftraggeber datenschutzgerecht zu vernichten oder sicher zu löschen. Test- und Ausschussmaterial ist unverzüglich datenschutzgerecht zu vernichten oder dem Auftraggeber auszuhändigen. Diese Verpflichtung gilt in gleichem Maße auch für eventuell beauftragte Unterauftragnehmer. Unberührt bleiben Daten, deren Löschung aus technischen Gründen nicht möglich ist oder einen unverhältnismäßig hohen Aufwand verursachen würde, sowie Kopien, die zum Nachweis der Ordnungsmäßigkeit der Datenverarbeitung oder zur Erfüllung von Haftungs- und Gewährleistungsansprüchen erforderlich sind.

14.2 Für diese Daten ist die Verarbeitung gem. Art. 18 DSGVO einzuschränken. Die Daten dürfen durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahrt werden und sind nach Ablauf der Aufbewahrungsfrist unverzüglich sicher zu löschen. Der Auftraggeber ist über Art und Umfang dieser gespeicherten Daten zu unterrichten. Der Auftragnehmer kann diese Daten zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

14.3 Der Auftraggeber kann verlangen, dass der Auftragnehmer die sichere Löschung bzw. die sichere Vernichtung aller in seinem Besitz befindlichen Unterlagen schriftlich bestätigt.

15 Geheimhaltung

15.1 Die Parteien versichern, dass sie vertrauliche Informationen der anderen Partei nicht verwenden oder veröffentlichen und stets sorgsam behandeln werden.

15.2 Als vertrauliche Informationen gelten seitens des Auftragnehmers alle Informationen einschließlich Abbildungen, Systemspezifikationen, Zeichnungen, Muster, Kalkulationen und sonstige Unterlagen, sowohl in schriftlicher als auch in jeder anderen Form, die als vertraulich gekennzeichnet sind oder nach ihrer Art als vertraulich zu bewerten sind.

15.3 Als vertrauliche Informationen gelten seitens Auftraggebers alle mit einer Software des Auftragnehmers erstellten oder verwalteten Daten. Vor diesem Hintergrund verpflichtet sich der Auftragnehmer über die nach diesen Bestimmungen getroffenen Regelungen hinaus keinerlei Gebrauch von diesen Daten zu machen und auch die mit der Erbringung der vertragsgegenständlichen Leistungen betrauten Personen entsprechend zu verpflichten.

15.4 Die Parteien werden alle angemessenen vorsorglichen Maßnahmen ergreifen, um ihre Geheimhaltungspflicht zu erfüllen. Die Parteien werden dabei die Sorgfalt walten lassen, die sie auch in eigenen Angelegenheiten ansetzen, mindestens aber die in Bezug auf solche Daten verkehrsübliche und üblicherweise vorauszusetzende Sorgfalt.

15.5 Eine Geheimhaltungspflicht besteht nicht, wenn die betreffenden Informationen/Daten bereits vor ihrer Entgegennahme rechtmäßiges Eigentum der empfangenden Partei gewesen sind, von der empfangenden Partei unabhängig selbst entwickelt wurden, allgemein bekannt sind oder werden oder allgemein zugänglich gemacht werden, es sei denn, dies geschieht durch eine Unterlassung der empfangenden Partei, oder der empfangenden Partei von Dritten mitgeteilt werden,

ohne dass hierin gegenüber der offenbarenden Partei eine Geheimhaltungspflicht verletzt wird.

15.6 Die Geheimhaltungspflicht entfällt, wenn vertrauliche Informationen der anderen Partei aufgrund eines Gesetzes, einer Verordnung, einer gerichtlichen Anordnung oder der Anordnung einer anderen Behörde offenbart werden müssen.

15.7 Die Offenlegung ist sowohl hinsichtlich des Umfangs als auch hinsichtlich des Adressatenkreises auf das rechtlich zwingende Mindestmaß zu beschränken.

15.8 Diese Geheimhaltungspflicht gilt sinngemäß für sämtliche Mitarbeiter der Parteien. Die Parteien haben sicherzustellen und fortlaufend zu überwachen, dass alle Personen, die von ihnen mit der Bearbeitung und Erfüllung dieses Vertrages betraut sind, diese Geheimhaltungs- und Sorgfaltspflichten beachten.

16 Anwendbares Recht und Gerichtsstand

16.1 Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.

16.2 Gerichtsstand für sämtliche Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung und datenschutzrelevante Streitigkeiten ist Nürnberg.

Anlage 1: Technische und organisatorische Maßnahmen

1 Vertraulichkeit

1.1 Zutrittskontrolle: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen. Legitimation der Berechtigten durch Schlüsselvergabe und Schlüssel an den Innentüren zu besonders gesicherten Bereichen (z. B. Serverraum);

1.2 Zugangskontrolle: Keine unbefugte Systembenutzung durch Benutzeridentifikation und Authentifizierung durch Verwendung von sicheren Kennwörtern nach aktuellem Stand der Technik festgelegten Mindestanforderungen an die Passwortlänge, Verwendung von Sonderzeichen und Änderungsfristen, automatischer Sperrung, Einrichtung eines Benutzerstammsatzes für jeden Benutzer, Verschlüsselung von Datenträgern;

1.3 Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung durch differenzierte Berechtigungen, Protokollierung und Auswertung von Zugriffen;

1.4 Trennungskontrolle: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden durch interne Mandantenfähigkeit, Zweckbindung, Funktionstrennung nach Produktions- und Testbetrieb;

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, wobei diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

2 Integrität

2.1 Weitergabekontrolle: Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch), um unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport zu verhindern durch Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur, Protokollierung, Transportsicherung;

2.2 Eingabekontrolle: Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind, durch Protokollierungs- und Protokollauswertungssysteme.

3 Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch Backup-Verfahren, Spiegeln von Festplatten, z.B. RAID-Verfahren, getrennte Aufbewahrung, Virenschutz / Firewall, Notfallplan;

3.2 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO) insbesondere regelmäßige Prüfung, ob die erstellen Datensicherungen (Backups) zur Wiederherstellung verlorener Daten genutzt werden können.

4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1 Datenschutz-Management inkl. Durchführung regelmäßiger Penetrationstests zur Prüfung der Sicherheit der Systeme gemäß dem jeweils aktuellen Stand der Technik;

4.2 Incident-Response-Management;

5 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);

5.1 Auftragskontrolle: Keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers durch eindeutige Vertragsgestaltung, formalisierte Auftragserteilung (Auftragsformular), Kriterien zur Auswahl des Auftragnehmers, Kontrolle der Vertragsausführung.