Vertrag zur Auftragsverarbeitung
gem. Art. 28 Abs. 3 DSGVO

zwischen der

_____
_____

_____
(Verantwortlicher gem. Art. 4 Nr. 7 DSGVO)
nachstehend **Auftraggeber** genannt

und der

Tricad GmbH
Wilhelm-Wagenfeld-Str. 22
80807 München
(Auftragsverarbeiter gem. Art. 4 Nr. 8 DSGVO)
nachstehend **Auftragnehmer**,
gemeinschaftlich **Vertragsparteien** oder **Parteien** genannt.

1 Allgemeine Regelungen

Die „Allgemeinen Regelungen“ im Anhang sind Bestandteil dieses Vertrages.

2 Gegenstand des Auftrags

Der Gegenstand des Auftrags ergibt sich aus der zugrundeliegenden
Servicevertrag WV-_____
auf den hier verwiesen wird.
(im Folgenden Leistungsvereinbarung)

3 Dauer des Auftrags und Kündigung

Die Dauer dieses Vertrags entspricht der Laufzeit der Leistungsvereinbarung.

4 Art und Zweck der Verarbeitung

Bei der Durchführung von Service- und Wartungsarbeiten kann ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden.

5 Art der Daten / Kategorien betroffener Personen

Beim Service- und Wartungszugriff kann es zum Zugriff auf alle personenbezogenen Daten kommen, die im Zugriff des angemeldeten Users liegen.

Die Art der Daten und die Kategorien der betroffenen Personen umfassen somit ggf. alle, die der Verantwortliche verarbeitet.

Eine Verarbeitung von besonderen Kategorien personenbezogener Daten gem. Art. 9 DSGVO kann ausgeschlossen werden.

6 Unterbeauftragung

Durch den Auftragnehmer mit Zustimmung der Auftraggeberin beauftragte Unterauftragnehmer sind:

Vertrieblich

Bentley Systems Germany GmbH
Bentley Systems International Ltd.
SOLAR-COMPUTER GmbH
IDAT GmbH
HEXAGON ppm
BIM collab

Support

Bentley Systems Germany GmbH
Bentley Systems International Ltd.
SOLAR-COMPUTER GmbH
HEXAGON ppm
SC CADINTER SRL

7 Datenschutzbeauftragter (DSB) / Zuständige Person des Auftragnehmers

Der Auftragnehmer hat einen Datenschutzbeauftragten benannt:

Heiko Stelter
c/o GABO mbH & Co. KG
Louis-Braille-Str. 1
01099 Dresden
E-Mail: datenschutz@tricad.eu

8 Weisungsberechtigte Personen des Auftraggebers

(Name und Kontaktdaten)

_____

_____

_____

_____

9 Autorisierte Personen des Auftragnehmers

Stefan Eisen	Tel. 069-7137899-0
Maurice Kuske	Tel. 069-7137899-0

10 Mögliche Verlagerung in ein Drittland

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

11 Vom Auftragnehmer zu treffende technische und organisatorische Maßnahmen

Der Auftragnehmer sichert zu, unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen jederzeit geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau im Sinne von Ziffer 3 der Allgemeinen Regelungen zu gewährleisten.

Die als vereinbart geltenden getroffenen Maßnahmen sind im Anhang 2 aufgeführt.

_____	München, _____
Ort, Datum	Ort, Datum
_____	_____
Auftraggeber	Auftragnehmer
_____	_____
Unterzeichner in Druckbuchstaben	Unterzeichner in Druckbuchstaben

ANHANG – Allgemeine Regelungen

1 Gegenstand der Vereinbarung

1.1
Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Gegenstand der Vereinbarung ist die Erbringung aller Dienstleistungen des Auftragnehmers für den Auftraggeber in deren Rahmen personenbezogene Daten verarbeitet werden, soweit dies in der Beauftragung dokumentiert ist. Die Verarbeitung von Daten durch den Auftragnehmer erfolgt nur nach vorheriger schriftlicher Auftragserteilung und -bestätigung durch den Auftraggeber und nur im vertraglich festgelegten Umfang und für den vorgegebenen Zweck und nach den Weisungen des Auftraggebers.

1.2
Die durch den Auftragnehmer verarbeiteten personenbezogenen Daten dienen ausschließlich den Zwecken der Vertragserfüllung. Der Auftragnehmer beachtet dabei die einschlägigen datenschutzrechtlichen Bestimmungen. Er verpflichtet sich insbesondere, bei der Erbringung seiner Leistungen die Grundsätze der Datenvermeidung und der Datensparsamkeit zu beachten. Eine Verwendung der Daten für andere Zwecke darf nicht erfolgen. Eine anderweitige Nutzung und Übermittlung für eigene oder fremde Zwecke, einschließlich Marketingzwecke, ist nicht gestattet.

1.3
Im Fall von wiederholten oder schwerwiegenden Verstößen gegen die Bestimmungen dieser Vereinbarung oder gegen sonstige Bestimmungen zum Schutz von personenbezogenen Daten ist der Auftraggeber zu einer außerordentlichen Kündigung der Vereinbarung berechtigt. Das gesetzliche Recht zur außerordentlichen Kündigung aus sonstigem wichtigem Grund bleibt davon unberührt.

2 Pflichten des Auftraggebers

2.1
Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der betroffenen Personen ist der Auftraggeber verantwortlich. Das alleinige Verfügungsrecht über die Daten verbleibt beim Auftraggeber.

2.2
Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung des Ergebnisses der Auftragsleistung feststellt.

3 Technische und organisatorische Maßnahmen

3.1
Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Soweit die Prüfung durch den Auftraggeber einen Anpassungsbedarf ergibt, ist dieser umzusetzen.

3.2
Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c), 32 DSGVO insbesondere in Verbindung mit Art. 24 Abs. 1, Abs. 2 DSGVO auf Dauer herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik sowie die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

3.3
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.

3.4
Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

4 Berichtigung, Einschränkung und Löschung von Daten

4.1

Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung.

4.2

Soweit der Auftraggeber eine entsprechende Weisung erteilt, sind Umsetzung des Löschkonzepts, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5 Qualitätssicherung und Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Der Auftragnehmer teilt dem Auftraggeber die Kontaktdaten eines von ihm benannten Datenschutzbeauftragten mit. Sollte es für den Auftragnehmer nicht verpflichtend sein, einen Datenschutzbeauftragten zu benennen, teilt er die Kontaktdaten des für die Einhaltung des Datenschutzes verantwortlichen Ansprechpartners mit.

b) Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die schriftlich zur Wahrung der Vertraulichkeit gem. Artt. 28 Abs. 3 S. 2 lit. b), 29, 32 Abs. 4 DSGVO und - soweit relevant - auf das Telekommunikationsgeheimnis gem. § 88 Telekommunikationsgesetz verpflichtet und in geeigneter Weise mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden oder gesetzlich hinreichend zur Geheimhaltung verpflichtet sind.

c) Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisungen des Auftraggebers einschließlich der in dieser Vereinbarung eingeräumten Befugnisse verarbeiten, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Der Auftragnehmer muss durch entsprechende (technische und organisatorische) Maßnahmen jederzeit sicherstellen, dass kein Zugriff auf die Daten durch Unbefugte erfolgen kann.

d) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c), 32 DSGVO.

e) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

f) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

g) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieser Vereinbarung.

i) Ein ggf. vorhandenes Sicherheitshandbuch, das Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO) sowie die Dokumentation der Datenschutzfolgeabschätzung (Art. 35 DSGVO) ist dem Auftraggeber auf Anfrage jederzeit kostenlos zur Verfügung zu stellen.

j) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DSGVO erfüllt sind.

k) Daten des Auftraggebers dürfen nicht im öffentlichen Raum (z. B. Flughafen, Bahn etc.) verarbeitet werden. Die Verarbeitung der Daten des Auftraggebers außerhalb der Geschäftsräume des Auftragnehmers ist nur im nichtöffentlichen Raum zulässig und nur mit gesicherten firmen-

eigenen Geräten des Auftragnehmers. Es muss sich dabei um verschlüsselte Datenträger, ausreichend geschützte Verbindungen und fortschrittliche Sicherheitsvorkehrungen nach dem jeweils aktuellen Stand der Technik handeln, sowie aktuelle Signaturen von Viren- und Malwarescannern. Die Verwendung von Privatrechnern ist nicht zulässig.

l) Der Arbeitsablauf wird vom Auftragnehmer lückenlos dokumentiert. Hierzu gehört insbesondere eine vollständige Protokollierung der Systemleistungen, vor allem, wenn Dritte auf das DV-System des Auftragnehmers zum Zwecke der Fernwartung zugreifen. Die Dokumentation ist dem Auftraggeber auf Verlangen vorzulegen. Der Auftragnehmer hält die gängigen Konventionen, wie Kennzeichnung von Vorgangsanfang und -ende, Aufzeichnung des Verarbeitungsdatums mit dem Namen des Verarbeitenden, ein.

m) Der Auftragnehmer hat die in seinen Besitz gelangten Daten, Datenträger und Unterlagen des Auftraggebers so zu kennzeichnen, dass ohne weiteres ersichtlich ist, dass die Daten, Datenträger und Unterlagen im Eigentum des Auftraggebers stehen. Die Daten, Datenträger und Unterlagen sind von eigenen Daten, Datenträgern und Unterlagen des Auftragnehmers getrennt zu verwahren und vor dem Zugriff Dritter zu schützen.

6 Unterauftragsverhältnisse

6.1

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer beispielsweise als Telekommunikationsleistungen, Post- oder Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

6.2

Die Beauftragung von Unterauftragnehmern ist grundsätzlich unzulässig. Soweit der Abschluss etwaiger Unterauftragsverhältnisse, die im Zusammenhang mit der für den Auftraggeber erbrachten Dienstleistung stehen unumgänglich ist, verpflichtet sich der Auftragnehmer, den Auftraggeber über den Abschluss vorab zu informieren und dessen Zustimmung einzuholen.

6.3

Soweit eine Zustimmung nach Abs. 2 vorliegt, ist die Auslagerung auf den Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers nur zulässig, soweit eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird und damit die in der vorliegenden Datenschutzvereinbarung getroffenen Regelungen auch gegenüber Unterauftragnehmern gelten.

6.4

Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

6.5

Der Auftragnehmer ist verpflichtet, vor Beginn der Datenverarbeitung durch den Unterauftragnehmer und sodann in regelmäßigen Abständen die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen - insbesondere der vom Unterauftragnehmer getroffenen technischen und organisatorischen Maßnahmen - im erforderlichen Umfang zu kontrollieren. Das Ergebnis ist zu dokumentieren und die vollständigen Kontrollunterlagen sind dem Auftraggeber unaufgefordert zur Verfügung zu stellen.

6.6

Bei der Unterbeauftragung sind dem Auftraggeber, dessen Aufsichtsbehörde, der zuständigen Datenschutzbehörde und sonstigen Beauftragten des Auftraggebers (z. B. Prüfdienstleister) gegenüber dem Unterauftragnehmer Kontroll- und Überprüfungsrechte entsprechend Ziffer 7 dieser Vereinbarung einzuräumen. Darüber hinaus werden dem Auftraggeber seitens des Auftragnehmers gemeinsame Prüfmöglichkeiten gegenüber den Unterauftragnehmern eingeräumt. Alle im Rahmen dieser Prüfung beim Auftragnehmer anfallenden Kosten trägt der Auftragnehmer selbst.

6.7
Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen der Voraussetzungen für eine Unterbeauftragung gestattet.

7 Kontrollrechte des Auftraggebers

7.1
Der Auftraggeber, dessen Aufsichtsbehörde, die zuständigen Datenschutzbehörden, beauftragte Mitarbeiter und sonstige Beauftragte des Auftraggebers (z. B. Prüfdienstleister) sind befugt, Auskünfte beim Auftragnehmer einzuholen, die Umsetzung der technischen und organisatorischen Maßnahmen vor Ort während der Geschäftszeiten und nach Anmeldung (es sei denn, es ist Eile geboten) beim Auftragnehmer zu überprüfen und dazu auch die prüfungsrelevanten Örtlichkeiten zu betreten und Einsicht in die erforderlichen Unterlagen und Systeme/Programme - welche den Auftraggeber betreffen - zu nehmen. Der Auftragnehmer stellt dabei sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO und der vertraglichen Vereinbarung überzeugen kann.

7.2
Der Auftragnehmer hat dem Auftraggeber Einblicke in die tatsächlichen Konfigurationen mit geeigneten technischen Verfahren zu gewähren. Falls der Auftragnehmer seine Leistungen über ein Web-Frontend anbietet oder eine sonstige Verbindung ins Internet unterhält, erhält der Auftraggeber die Genehmigung, nach vorheriger Abstimmung mit dem Auftragnehmer die Wirksamkeit der Schutzmaßnahmen durch den Einsatz von entsprechenden Software-Tools zu überprüfen.

7.3
Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann auch erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO, aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren), eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

7.4
Aufwände und Kosten, die beim Auftragnehmer im Zuge der Prüfung durch den Auftraggeber entstehen, trägt allein der Auftragnehmer. Eine Kostenverrechnung und -weitergabe an den Auftraggeber oder an vom Auftraggeber zur Durchführung der Prüfung beauftragte Dritte ist ausgeschlossen.

8 Verhalten bei Datenschutzverstößen

8.1
Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen.

Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden;
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung;
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde;
f) Meldung von Störungen des Verarbeitungsablaufs;
g) die Meldung bei Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde;
h) die Meldung bei Ermittlungen durch zuständige Behörden nach Art. 83 und/oder 84 DSGVO.

9 Weisungsbefugnis des Auftraggebers

9.1
Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein jederzeitiges, umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, dass er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen.

9.2
Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

9.3
Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

9.4
Falls der Auftragnehmer eine Weisung, gleich aus welchen Gründen, nicht einhält, verpflichtet er sich, den Auftraggeber unverzüglich davon in Kenntnis zu setzen, der unter diesen Umständen berechtigt ist, die Datenweitergabe an den Auftragnehmer auszusetzen. Falls die Nichtdurchführung der Weisung eine Verletzung der Bestimmungen dieser Vereinbarung oder einschlägiger datenschutzrechtlicher gesetzlicher Bestimmungen durch den Auftragnehmer darstellt, ist der Auftraggeber in diesen Fällen berechtigt die Vereinbarung (inklusive aller mit den Leistungen zusammenhängenden Verträge) mit sofortiger Wirkung zu kündigen.

10 Löschung und Rückgabe von personenbezogenen Daten

10.1
Die Löschung personenbezogener Daten, das Recht auf Vergessen werden sowie die Rechte auf Berichtigung, Datenportabilität und Auskunft sind nach dokumentierter Weisung des Auftraggebers durch den Auftragnehmer sicherzustellen.

10.2
Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangten Daten, Datenträger und Unterlagen sowie Verarbeitungs- und Nutzungsergebnisse, die im Zusammenhang mit der Erfüllung der Leistung stehen, dem Auftraggeber auszuhändigen bzw. zu übermitteln. Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten nicht anderweitig und bewahrt sie nicht länger auf, als es zur Vertragserfüllung erforderlich ist und es der Auftraggeber unter Berücksichtigung der Aufbewahrungspflichten bestimmt. Nach Erledigung des Auftrages sind die bei ihm gespeicherten personenbezogene Daten nicht reproduzierbar zu löschen bzw. datenschutzgerecht physisch zu vernichten.

10.3
Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

10.4
Die bei der Verarbeitung ggf. entstandenen Arbeitsdateien, die personenbezogene Daten enthalten, sind unmittelbar nach Beendigung der Produktion/nach dem Versand zu löschen. Ebenso sind alle elektronischen Dateien und Datenbanken sowie Datenträger nicht reproduzierbar zu löschen bzw. datenschutzgerecht physisch zu vernichten. Dies gilt auch für erzeugte Test- und Zwischenergebnisse und Ausschussmaterial.

10.5
Der Auftragnehmer stellt das für sein Unternehmen vorliegende Löschkonzept dem Auftraggeber auf Anfrage unverzüglich in Kopie kostenlos zur Verfügung. Liegt ein Löschkonzept noch nicht vor, ist dieses zu erstellen und dem Auftraggeber auf Anfrage unverzüglich in Kopie kostenlos zur Verfügung zu stellen. Die Löschung der personenbezogenen Daten hat nach der DIN-Norm 66399 zu erfolgen und ist mit geeigneten Maßnahmen zu protokollieren. Personenbezogene Daten und/oder Betriebs- und Geschäftsgeheimnisse des Auftraggebers sind mindestens auf Schutzklasse 2 und Sicherheitsstufe 4 zu vernichten. Der Auftragnehmer wird vertraglich sicherstellen, dass die Vorgabe des Auftraggebers zu DIN-Norm 66399 auch gegenüber Unterauftragnehmern gelten.

10.6
Hinsichtlich sämtlicher Löschvorgänge hat der Auftragnehmer dem Auftraggeber Löschprotokolle zu übergeben. Es sind folgende Mindestinhalte für ein Löschprotokoll zu berücksichtigen:

a) Datum und Uhrzeit der Löschung,
b) das gültige Löschkonzept (Version, Datum),
c) die Methode der Datenlöschung (Verfahren),
d) das betroffene Verfahren (Beschreibung der zu löschenden Daten),
e) die angewandte Löschregel,
f) die für die Löschung verantwortliche Person,
g) die ausführenden Personen,
h) die Anzahl der zu löschenden Daten (Summenprotokolle, Zählreport) und
i) die Anzahl der gelöschten Daten (Summenprotokolle, Zählreport, Löschlaufreport).

Das Löschprotokoll darf keine personenbezogenen Daten enthalten.

10.7
Der Auftragnehmer schließt durch geeignete Maßnahmen eine unbefugte Duplizierung der auftragsgemäß verarbeiteten Datenbestände aus. Die bei der Verarbeitung ggf. entstandenen Arbeitsdateien, die personenbezogene Daten enthalten, sind unmittelbar nach Beendigung der Produktion/nach dem Versand zu löschen. Bei einem eventuell erforderlichen Hardware- und/oder Softwareaustausch hat der Auftragnehmer dafür zu sorgen, dass keine Daten des Auftraggebers an Dritte weitergegeben werden, insbesondere, dass Datenspeicher vor der Weitergabe an Dritte datenschutzkonform (nichtreproduzierbar bzw. physisch) vernichtet werden.

11 Haftung

11.1
Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen sowie untereinander entsprechend der in Art. 82 DSGVO getroffenen Regelung.

11.2
Der Auftragnehmer bestätigt, sich gegen die Inanspruchnahme wegen Verletzung von Datenschutzvorschriften hinreichend versichert zu haben.

12 Geheimhaltung

Der Auftragnehmer verpflichtet sich, alle Informationen, die ihm aus dem Geschäftsbereich des Auftraggebers bekannt werden, zeitlich unbegrenzt streng vertraulich zu behandeln und nur zur Durchführung der Vereinbarung zu verwenden.

13 Wirksamkeit der Vereinbarung und Gerichtsstand

13.1
Diese Vereinbarung tritt mit ihrer Unterzeichnung in Kraft und ersetzt damit ggfs. zuvor zwischen den Parteien geschlossene Vereinbarungen zur Auftragsverarbeitung.

13.2
Für diese Vereinbarung gilt die Schriftform. Soweit in dieser Vereinbarung die Schriftform vereinbart wird, genügt dafür die Übermittlung der Erklärung per Telefax oder E-Mail. Alle Änderungen und Ergänzungen dieser Vereinbarung bedürfen zu ihrer Wirksamkeit ebenfalls der Schriftform. Das gilt auch für die Änderung des Schriftformerfordernisses selbst.

13.3
Wesentlicher Vertragsbestandteil sind auch alle während der Laufzeit dieser Vereinbarung abgeschlossenen Anhänge, die ebenfalls der Schriftform bedürfen.

13.4
Etwaige Allgemeine Geschäftsbedingungen des Auftragnehmers finden auf die Rechtsbeziehungen zwischen den Parteien keine Anwendung. Dies gilt auch dann, wenn der Auftraggeber deren Anwendbarkeit im Einzelfall nicht ausdrücklich widersprechen sollte.

13.5
Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen. Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

13.6
Sollte eine der Bestimmungen dieser Vereinbarung unwirksam sein oder werden, wird die Wirksamkeit der anderen Bestimmungen dieser Vereinbarung dadurch nicht berührt. Anstelle der unwirksamen Bestimmungen oder zur Ausfüllung der Regelungslücken verpflichten sich die Parteien, diejenige rechtlich zulässige Bestimmung zu vereinbaren, die so weit wie möglich dem entspricht, was die Vertragsparteien gewollt haben oder nach dem Sinn und Zweck dieser Vereinbarung gewollt haben würden, wenn sie die Unwirksamkeit der Bestimmung bzw. die Regelungslücke erkannt haben würden.

13.7
Der Gerichtsstand für sämtliche Streitigkeiten aus dieser Vereinbarung ist Sitz des Auftraggebers.

ANHANG 2 – Beschreibung der technischen und organisatorische Maßnahmen

1 Grundlegende Maßnahmen

1.1 Datenschutzorganisation / Datenschutzbeauftragter

Der Auftragnehmer hat einen externen Datenschutzbeauftragten (DSB) benannt.

Der DSB wird gem. Art. 38 Abs. 1 DSGVO ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden.

Der DSB erhält gem. Art. 38 Abs. 2 DSGVO alle erforderliche Unterstützung und notwendige Ressourcen zur Erfüllung seiner Aufgaben.

Der DSB arbeitet bei der Erfüllung seiner Aufgaben vollkommen weisungsfrei.

1.2 Meldeverfahren

Ein Meldeverfahren für Verletzungen des Datenschutzes ist eingerichtet.

Ein Meldeverfahren für Ereignisse der Informationssicherheit ist eingerichtet.

Alle gemeldeten Ereignisse werden zur Verbesserung der Sicherheit herangezogen.

1.3 Richtlinien

Leitlinien für Datenschutz und Informationssicherheit sind vorhanden.

Für alle relevanten Einrichtungen der Informationsverarbeitung existieren Richtlinien zum Umgang.

Alle Beschäftigten sind auf die Einhaltung der Leitlinien und Richtlinien verpflichtet. Die Einhaltung wird überwacht, Verstöße sanktioniert.

1.4 Schulungen

Alle eingesetzten Beschäftigten werden in den relevanten Aspekten des Datenschutzes regelmäßig geschult.

Alle eingesetzten Beschäftigten werden im Umgang mit IT-Systemen regelmäßig geschult.

Alle eingesetzten Beschäftigten werden in den relevanten Aspekten der Informationssicherheit regelmäßig geschult.

2 Maßnahmen zur Pseudonymisierung und Verschlüsselung

2.1 Pseudonymisierung

Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

Maßnahmen im Zusammenhang mit der Pseudonymisierung

Die Pseudonymisierung von Daten des Auftraggebers erfolgt nur nach Weisung und nur in Abstimmung mit dem Auftraggeber.

2.2 Verschlüsselung

Durch Verschlüsselung soll die Kenntnisnahme in personenbezogene Daten durch Unbefugte geschützt oder diese zur Kenntnis genommen werden (z. B. durch Hackerangriffe oder Spionage). Verschlüsselung bezeichnet die Umwandlung von Daten in eine Form, die man als Chiffretext bezeichnet und die von nicht autorisierten Personen nicht zu verstehen ist.

Maßnahmen im Zusammenhang mit der Verschlüsselung

Für den Transport von personenbezogenen Daten kommen nur stark verschlüsselte Transportwege und Geräte zum Einsatz.

Die Daten auf mobilen Geräten werden ohne Ausnahme stark verschlüsselt.

Alle on-premise-Systeme des Auftragnehmers werden ohne Ausnahme stark verschlüsselt.

3 Maßnahmen zu Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit

3.1 Zutritt zu Räumlichkeiten

Die Eingangstüren der Gebäude, in denen die Datenverarbeitung erfolgt, sind mit einer Schließanlage versehen.

Die Dokumentation der Zutrittsberechtigungen vorgenannter Schließanlage erfolgt namensscharf. Ebenso die Ausgabe und Rücknahme der vergebenen Schlüssel.

Betriebsfremde Personen wie Gäste und Besucher erhalten nur in Begleitung von Betriebspersonal Zutritt.

Die Zutrittsberechtigungen von Reinigungs- und Wartungspersonal erfolgen namensscharf. Der Zutritt zu Räumen, in denen besonders kritische Daten verarbeitet werden, erfolgt in Begleitung und unter Aufsicht von Betriebspersonal oder wird namensscharf protokolliert.

Die Räume der zentralen Datenhaltung (Serverräume etc.), sowie das Büro der IT-Abteilung gehören einem separaten Schließkreis an. Hier erfolgt der Zutritt von betriebsfremden Personen ausschließlich unter Aufsicht von besonders geschultem Betriebspersonal.

Bei Beendigung des Arbeitsverhältnisses unterlaufen alle Zutrittsberechtigungen einem Standardprozess. Hier werden nicht mehr benötigte oder nicht mehr gewünschte Berechtigungen entzogen und nachgehalten.

3.2 Zugang zu Systemen

Das gesamte Unternehmensnetzwerk ist durch ein geschlossenes Firewall-System gesichert. Alle Verbindungen zu den Standorten erfolgen einheitlich durch ein gesichertes virtuelles LAN. Alle Firewalls erfahren regelmäßige Sicherheitsupdates.

An sämtlichen Übergängen zum Unternehmensnetz werden Virenscanner eingesetzt. Ein- und ausgehende E-Mails werden gescannt. Dateiaustausch per FTP-Protokoll wird gescannt. Der Zugriff auf das Web per Webbrowser wird gescannt. Alle Virenscanner werden automatisiert aktuell gehalten. Die Aktualisierungen werden regelmäßig geprüft.

Auf allen genutzten Servern und Einzelplatzrechnern werden Virenscanner eingesetzt. Alle Virenscanner werden automatisiert aktuell gehalten. Die Aktualisierungen werden regelmäßig geprüft.

Auf allen genutzten Servern und Einzelplatzrechnern werden regelmäßig und automatisiert Sicherheitsupdates für Betriebssysteme und relevante Software installiert.

Die Mitarbeiter haben keine lokalen oder sonstige Administratorrechte.

Die Mitarbeiter werden auf die aktuelle Passwort-Richtlinie verpflichtet. Soweit technisch möglich, erfolgt die Umsetzung der Passwort-Richtlinie als Systemvorgabe.

3.3 Zugriff auf Daten

Für alle relevanten Zugriffe auf EDV-Systeme sind Berechtigungskonzepte vorhanden und der Einsatz wird dokumentiert.

Das jeweilige Recht zur Rechtevergabe ist in einem Organisationskonzept namensscharf dokumentiert.

Die Vergabe der Zugriffsberechtigungen wird namensscharf dokumentiert.

Die Administratoren, die Datenbestände des Auftraggebers ganz oder in großen Mengen kopieren oder extrahieren dürfen, sind in einem gesonderten Administratorenkonzept dokumentiert und werden explizit vom Datenschutzbeauftragten im administrativen Umgang mit personenbezogenen Daten geschult. Sie unterliegen einer besonderen Geheimhaltungsverpflichtung für IT-Administratoren.

3.4 Datensicherung

Der gesamte relevante Datenbestand wird täglich vollständig gesichert. Es werden regelmäßig ausreichend viele Generationen der Daten vorgehalten.

Die Datensicherungsmedien werden sicher gelagert. Der Zugriff auf die Medien ist den Datensicherungsadministratoren vorbehalten.

3.5 Trennungsgebot

Die Daten des Auftraggebers werden in einem eigenen Mandanten oder logisch getrennt vorgehalten.

Das Berechtigungskonzept gewährleistet, dass ausschließlich Beschäftigte, die für diesen Auftrag eingesetzt werden, Zugriff erhalten.

3.6 Weitergabe von Daten

Der Datenaustausch zwischen Auftraggeber und Auftragnehmer erfolgt grundsätzlich stark verschlüsselt.

Ein Austausch von Datenträgern findet grundsätzlich nicht statt. Sollte ein Austausch von Datenträgern ausnahmsweise erfolgen, so finden ausschließlich stark verschlüsselte Medien Anwendung.

3.7 Protokollierung

Die Änderung und Löschung von Daten des Auftraggebers auf den Systemen des Auftragnehmers wird ggf. namensscharf protokolliert.

Auf die Logfiles haben ausschließlich dafür eingesetzte und geschulte Administratoren Zugriff.

3.8 Manipulationsschutz

Es erfolgt eine Regelmäßige Prüfung von Logfiles der IT-Systeme.

Eine regelmäßige Prüfung der Geräte auf Manipulation, Keylogger etc. wird durchgeführt.

Awareness-Maßnahmen für die Belegschaft werden regelmäßig durchgeführt.

Ein Meldeverfahren bei Verdacht auf Manipulation ist etabliert.

4 Maßnahmen zur raschen Wiederherstellung der Verfügbarkeit bei Zwischenfall

Ein Notfallmanagement ist etabliert.

Es erfolgen regelmäßige Prüfungen der Wiederherstellbarkeit unter Berücksichtigung angemessener Reaktions- und festgelegter akzeptabler Wiederherstellungszeiten.

Die regelmäßige Wiederanlaufzeit nach einer Zerstörung des Rechenzentrums beträgt etwa zwei Tage.

5 Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Ein Datenschutz-Managementsystem (DSMS) ist eingerichtet.

Für alle datenschutzrelevanten Aspekte werden regelmäßige Audits durchgeführt, die Ergebnisse werden zur kontinuierlichen Verbesserung verwendet.

6 Berücksichtigung der mit der Verarbeitung verbundener Risiken

Alle Verarbeitungen personenbezogener Daten sind gem. Art. 30 DSGVO dokumentiert.

Für alle Verarbeitungen personenbezogener Daten wird regelmäßig eine Risikobewertung durchgeführt und die Maßnahmen zum Schutz der Daten entsprechend angepasst.

7 Maßnahmen zur Sicherstellung der Weisungsgebundenheit unterstellter Personen

Alle Beschäftigten und Dienstleister des Auftragnehmers mit Zugriff auf personenbezogene Daten werden schriftlich verpflichtet, diese nur auf Anweisung und ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen zu verarbeiten.