

Cloudsoftware Nutzungsvertrag (SaaS)

zwischen

ic-solution GmbH

Möckernsche Straße 3, 04155 Leipzig
(nachfolgend: „ICS“ und/oder „Vermittler“)

und

ics cloud services GmbH

Möckernsche Straße 3, 04155 Leipzig
(nachfolgend: „ICSCS“ und/oder „Anbieter“)

und

Firma

Straße

Ort

(nachfolgend: „**Kunde**“)

**Kontaktdaten der
Ansprechpartner**

Für diesen Vertrag

E-Mail-Adresse

Für Datenschutz und
AVV:

E-Mail-Adresse:

1 Geltungsbereich

- 1.1 ICS tritt im Rahmen dieses Vertrags ausschließlich als Vermittler auf und ist nicht Anbieter der SaaS-Lösung. Der Nutzungsvertrag über die CloudSoftware kommt ausschließlich zwischen dem Kunden und der ICSCS als Anbieter zustande. ICS übernimmt keine vertraglichen Pflichten aus diesem Nutzungsvertrag, außer der Rechnungsstellung im Auftrag von ICSCS sowie, auf Wunsch des Kunden, der unterstützenden Einrichtung der Software.
- 1.2 Die nachfolgenden Vertragsbedingungen finden auf alle Einzelvertragsverhältnisse zwischen ICSCS und dem Kunden Anwendung, die die Nutzung der von ICSCS über das Internet bereitgestellten Plattform, für Input-Management sowie Klassifikation und Extraktion von Dokumenten u. a. auf Basis der Technologien mit dem Namen „SPICE“ des Herstellers ic forty two GmbH sowie die in diesem Zusammenhang erbrachten Hosting-Leistungen zum Gegenstand haben.
- 1.3 Auf das Vertragsverhältnis finden die Allgemeinen Geschäftsbedingungen von ICSCS Anwendung. Für den Fall, dass sich Regelungen widersprechen, haben die Regelungen dieses Nutzungsvertrags Vorrang. Auf das Vertragsverhältnis finden ferner die besonderen Vertragsregelungen Anwendung, wenn und soweit die Erbringung spezieller Leistungselemente vereinbart ist. Für den Fall, dass Regelungen hieraus im Widerspruch mit den Bestimmungen dieses Nutzungsvertrags stehen, haben die besonderen Vertragsregelungen Vorrang.
- 1.4 Der Einbeziehung abweichender Regelungen wird widersprochen. Diese finden auch dann keine Anwendung, wenn diese Angebotsaufforderungen, Bestellungen, Annahmeerklärungen oder sonstiger Korrespondenz mit ICSCS beigefügt sind, unabhängig davon, ob ICSCS der Anwendung solcher Regelungen ausdrücklich oder konkludent widersprochen oder hierzu geschwiegen hat. Abweichende Regelungen gelten nur, wenn ICSCS ihrer Geltung zuvor in Textform im Sinne des § 126b BGB („Textform“) zugestimmt hat.

2 Vertragsgegenstand

- 2.1 ICSCS bleibt alleiniger Vertragspartner des Kunden für die Bereitstellung und Nutzung der SaaS-Lösung. ICS vermittelt diese Leistungen und erbringt auf Wunsch des Kunden eine technische Einrichtung der Software und Anpassung nach Kundenvorgaben auf den Systemen von ICSCS. Diese Einrichtungstätigkeit stellt keine eigenständige vertragliche Verpflichtung von ICS dar und begründet keine Haftung für die Funktionsfähigkeit oder Verfügbarkeit der Software.
Erbringt ICS in solchen Fällen Unterstützung, so erfolgt dies ausschließlich als Erfüllungsgehilfe von ICSCS und ohne Begründung eines eigenen Vertragsverhältnisses zwischen ICS und dem Kunden. Die Rechnungsstellung für die SaaS-Lösung erfolgt über ICS im Auftrag von ICSCS, wobei ICSCS als Anbieter der SaaS-Lösung verantwortlich bleibt.
- 2.2 Vertragsgegenstand ist die von ICSCS auf Grundlage des zuletzt von ICSCS erteilten Angebots (nachfolgend: „**Angebot**“) bereitgestellte cloudbasierte Softwareanwendung, mit dem in dem Angebot beschriebenen Funktionsumfang (nachfolgend: „**Software**“). Der Vertragsgegenstand beinhaltet für die vereinbarte Laufzeit die Gestattung der Nutzung der Software im Wege des Fernzugriffs über das Internet sowie die Möglichkeit zur Speicherung von Daten durch den Kunden auf Servern, die ICSCS selbst betreibt oder im Auftrag von ICSCS betrieben werden. Die Anbindung des Kunden an das Internet ist nicht Vertragsgegenstand.
- 2.3 ICSCS hält ab dem mitgeteilten Zeitpunkt auf einer zentralen Datenverarbeitungsanlage oder mehreren Datenverarbeitungsanlagen (Server) die Software in der jeweils aktuellen Version zur Nutzung bereit. Dies umfasst die technische Nutzbarkeit am Übergabepunkt nach Ziffer 5 zum

Gebrauch durch den Kunden unter Verwendung einer geeigneten Zugriffssoftware über eine geeignete Telekommunikationsverbindung. Eine Überlassung der Software an den Kunden erfolgt nicht. Die Software wird ausschließlich für den in dem Angebot referenzierten Zweck bereitgestellt. ICSCS übernimmt keine Gewähr dafür, dass die Software für andere, vom Kunden vorgestellte Zwecke geeignet ist.

- 2.4 ICSCS stellt dem Kunden in die Software integrierte Benutzerhinweise zur Verfügung. Der Kunde akzeptiert dies als Dokumentation und Benutzerhandbuch (Dokumentation). Aufgrund der Integration und Bereitstellung der Dokumentation per Online-Zugriff sowie der permanenten Erweiterung und Aktualisierung der Dokumentation kann der Kunde diese nur bedingt auf seinem eigenen System speichern und vervielfältigen.
- 2.5 ICSCS behält sich das Recht vor, die Software in angemessenem Umfang zu ändern oder weiterzuentwickeln. Sofern und soweit mit der Bereitstellung einer neuen Version oder einer Änderung eine wesentliche Änderung von vertraglich zugesicherten Funktionalitäten oder Beschränkungen in der Verwendbarkeit bisher erzeugter Daten einhergehen, wird ICSCS dies dem Kunden spätestens sechs Wochen vor dem Wirksamwerden einer solchen Änderung in Textform ankündigen. Widerspricht der Kunde der Änderung nicht mindestens in Textform innerhalb einer Frist von zwei Wochen ab Zugang der Änderungsmitteilung, wird die Änderung Vertragsbestandteil. ICSCS wird den Kunden bei jeder Ankündigung von Änderungen auf die vorgenannte Frist und die Rechtsfolgen ihres Verstreichens bei Nichtwahrnehmung der Widerspruchsmöglichkeit hinweisen.
- 2.6 ICSCS hält auf dem Server ab dem vereinbarten Zeitpunkt der betriebsfähigen Bereitstellung für die vom Kunden durch Nutzung der Software erzeugten bzw. die zur Nutzung der Software erforderlichen Daten (nachfolgend: „**Anwendungsdaten**“) Speicherplatz in dem vertragsgemäßen Umfang bereit. ICSCS stellt dem Kunden auf Verlangen des Kunden am Ende der vereinbarten Vertragslaufzeit eine Kopie der Anwendungsdaten zum Abruf zur Verfügung.
- 2.7 Wenn mit dem Kunden die Gewährung des Zugriffs auf die Konfiguration und Administration der Software und/oder der für den Betrieb der Software erforderlichen Systemanwendungen vereinbart ist, ist die Übernahme der Konfiguration und Administration der Software und der für den Betrieb der Software erforderlichen Systemanwendungen durch ICSCS nicht Vertragsgegenstand.

3 Verfügbarkeit

- 3.1 ICSCS gewährleistet die in **ANLAGE: Verfügbarkeit** festgelegte Verfügbarkeit. Verfügbarkeit meint die gegebene Möglichkeit des Kunden, die gesamten Funktionalitäten der Software sowie die Anwendungsdaten, welche vom Vertragsgegenstand umfasst sind, am Übergabepunkt zu nutzen. Festgelegte Zeiten, in denen die Verfügbarkeit gegeben sein soll, werden als Systemlaufzeit bezeichnet. Soweit nicht anders vereinbart, gilt eine Systemlaufzeit von Montag bis Sonntag zwischen 06:00 Uhr und 24:00 Uhr als vereinbart.
- 3.2 Bei der Ermittlung der Verfügbarkeit gemäß Ziffer 3.1 bleiben Ausfallzeiten oder Zeiten bzw. Zeiträume eingeschränkter Nutzbarkeit unberücksichtigt, wenn und soweit der Ausfall oder die Einschränkung durch Störungen oder Ereignisse verursacht ist,
 - die in Teilen in der für die Ausführung der Software erforderlichen technischen Infrastruktur auftreten, die nicht von ICSCS oder dessen Erfüllungsgehilfen bereitgestellt werden;

- die nicht von ICSCS oder einem seiner Erfüllungsgehilfen (mit-)verursacht sind, zum Beispiel durch die Überschreitung einer vereinbarten zugelassenen Beanspruchung der Software durch den Kunden;
 - mit denen lediglich eine unerhebliche Minderung der Tauglichkeit zum vertragsgemäßen Gebrauch verbunden ist;
- 3.3 Ziffer 3.2 gilt entsprechend, wenn ICSCS gemäß Ziffer 2.7 keine Konfiguration und Administration der Systemanwendungen schuldet, es sei denn, dass der Ausfall oder die Einschränkung der Nutzbarkeit der Software in Teilen in der für die Ausführung der Software erforderlichen technischen Infrastruktur auftreten, auf die die Konfiguration und Administration der Software und der für den Betrieb der Software erforderlichen Systemanwendungen durch den Kunden nachweislich keinen Einfluss hat.
- 3.4 Bei der Ermittlung der Verfügbarkeit bleiben Zeiten geplanter Nichtverfügbarkeit unberücksichtigt. Zeiten geplanter Nichtverfügbarkeit sind Zeiten, in denen die Möglichkeit des Anwenders, die gesamten Funktionalitäten der Software sowie die Anwendungsdaten, welche vom Vertragsgegenstand umfasst sind, am Übergabepunkt innerhalb der vereinbarten Zeiten zu nutzen aufgrund von regulären Maßnahmen zur Wartung und Pflege sämtlicher Hard- und Software-Bestandteile des Systems sowie zur Durchführung der Datensicherheit oder sonstiger regulärer Arbeiten, nicht besteht (nachfolgend: „**Zeiten geplanter Nichtverfügbarkeit**“). ICSCS ist berechtigt, vorstehende Maßnahmen außerhalb der Systemlaufzeiten durchzuführen sowie nach rechtzeitiger Ankündigung an den Kunden innerhalb der Systemlaufzeit. Eine Ankündigung, die ICSCS mit einer Vorlaufzeit von zehn (10) Werktagen vor der Durchführung der angekündigten Maßnahmen vornimmt, gilt als rechtzeitig. ICSCS kann die Ankündigungsfrist in Ausnahmefällen, insbesondere bei Gefahr im Verzug für die (Daten)-Sicherheit des Systems, z. B. bei drohenden Hardwareausfällen, drohenden Computervirenepidemien oder Ähnlichem, unter Berücksichtigung der berechtigten Interessen des Kunden entsprechend verkürzen.
- 3.5 ICSCS weist darauf hin, dass es aufgrund von Wartungsprozessen in der Zeit von 20:00 Uhr bis 06:00 Uhr zu kleineren systemseitigen Leistungsschwankungen kommen kann. Die vorstehenden Regelungen bleiben hiervon unberührt.

4 Störungsbeseitigung

- 4.1 ICSCS trägt dafür Sorge, dass ICSCS beginnend ab dem Zeitpunkt, zu dem eine qualifizierte Störungsmeldung gemäß Ziffer 8.6 des Kunden bei ICSCS eingeht, in Abhängigkeit von der Schwere der jeweiligen Störung, innerhalb der in der **ANLAGE: Störungsbeseitigung** definierten Reaktions- und Wiederherstellungszeit die Beseitigung der Störung einleitet und beseitigt.
- 4.2 Ist die Übernahme der Konfiguration und Administration der Software und der für den Betrieb der Software erforderlichen Systemanwendungen durch ICSCS nicht Vertragsgegenstand (Ziffer 2.7) findet die vorstehende Regelung gemäß Ziffer 4.1 keine Anwendung.
- 4.3 ICS übernimmt für ICSCS als Erfüllungsgehilfe (§ 278 BGB) den 1st-Level-Support gegenüber dem Kunden. Der Kunde kann sich bei allen Fragen und Problemen, die die Nutzung der SaaS-Lösung betreffen, unmittelbar an ICS wenden. Die Kontaktdaten von ICS für den 1st-Level-Support werden dem Kunden in geeigneter Form zur Verfügung gestellt.
- 4.4 ICS handelt bei Erbringung des 1st-Level-Supports ausschließlich im Auftrag und auf Weisung von ICSCS. ICSCS bleibt alleiniger Anbieter und Vertragspartner des Kunden hinsichtlich der

SaaS-Leistungen. Ein eigenständiges Vertragsverhältnis zwischen ICS und dem Kunden über Supportleistungen kommt nicht zustande.

- 4.5 Da ICS den 1st-Level-Support als Erfüllungsgehilfe der ICSCS erbringt, haftet ICSCS für etwaige Pflichtverletzungen von ICS bei der Support-Dienstleistung nach Maßgabe der gesetzlichen Vorschriften und der vertraglich vereinbarten Haftungsregelungen. Eine eigenständige Haftung von ICS gegenüber dem Kunden wird nicht begründet.
- 4.6 Sobald sich herausstellt, dass eine Support-Anfrage nicht im Rahmen des 1st-Level-Supports durch ICS gelöst werden kann, leitet ICS die Anfrage unverzüglich an den 2nd-Level- bzw. 3rd-Level-Support der ICSCS weiter. ICSCS bleibt für die Einhaltung der in diesem Vertrag geregelten Service-Level-Agreements (SLAs) und für die vollständige Störungsbeseitigung verantwortlich.

5 Übergabepunkt, Systemvoraussetzungen

- 5.1 Mit der Bereitstellung der vertragsgemäßen Leistungen am Router-Ausgang des Rechenzentrums von ICSCS (nachfolgend: „**Übergabepunkt**“) geht die Gefahr auf den Kunden über.
- 5.2 Der Zugriff auf Funktionen der Software erfolgt mittels einer Zugriffssoftware über eine Telekommunikationsverbindung. Die Zugriffssoftware und die Gestellung einer Telekommunikationsverbindung sind nicht Vertragsbestandteil. Der Kunde beschafft sich diese selbständig auf eigenes Risiko.
- 5.3 Soweit nichts anderes mitgeteilt worden ist, empfiehlt ICSCS die Nutzung der Software mit einem dem jeweils aktuellen Stand der Technik entsprechenden PC, einem gängigen, aktuellen Internetbrowser sowie einer Telekommunikationsanbindung mit einer Übertragungsrate von mindestens [16.000 kbit/s] als Systemvoraussetzung.

6 Nutzungsrechte

- 6.1 Der Kunde erhält an der Software ein einfaches, nicht übertragbares, auf die Vertragslaufzeit beschränktes Nutzungsrecht zur Nutzung der vom Vertragsgegenstand nach Ziffer 2 umfassten Anwendung auf den von ICSCS bereitgestellten Servern. Der Umfang des eingeräumten Nutzungsrechts ist auf die in dem vereinbarten Lizenzmodell im Zeitpunkt des Vertragschlusses angegebene Anzahl an Nutzern beschränkt.
- 6.2 Der Kunde darf die Nutzung der Software nur für eigene geschäftliche Tätigkeit durch Nutzer gestatten, die ihm vereinbarungsgemäß als ihm zuzuordnende Nutzer zuzurechnen sind. Darüber hinaus ist dem Kunden nicht gestattet, Dritten die Nutzung der Software zu gestatten, insbesondere darf der Kunde die Software nicht weitervermieten.
- 6.3 Der Kunde ist nicht berechtigt, Änderungen an der Software vorzunehmen. Dies gilt nicht für Änderungen, die für die Berichtigung von Fehlern notwendig sind, sofern ICSCS sich mit der Behebung des Fehlers in Verzug befindet, die Fehlerbeseitigung ablehnt oder wegen der Eröffnung des Insolvenzverfahrens zur Fehlerbeseitigung außer Stande ist.
- 6.4 Sofern ICSCS während der Laufzeit neue Versionen, Updates, Upgrades oder andere Neulieferungen der Software bereitstellt, gelten die vorstehenden Rechte auch für diese.

7 Nutzungsrecht an verfügbaren Inhalten

- 7.1 Die Nutzung von verfügbaren Daten und Inhalten ist nur insoweit erlaubt, soweit durch eine entsprechende Funktionalität die Möglichkeit zur Nutzung eingeräumt worden ist. Verfügbare

Daten und Inhalte dürfen ausschließlich für eigene geschäftliche Zwecke des Kunden online abgerufen und angezeigt werden. Dem Kunden ist es untersagt, Urhebervermerke, Logos und sonstige Kennzeichen oder Schutzvermerke zu entfernen oder zu verändern.

- 7.2 Der Kunde ist zum Herunterladen und Ausdrucken von Inhalten nur insoweit berechtigt, soweit eine entsprechende Funktionalität zur Verfügung steht. Im Übrigen verbleiben sämtliche Rechte an den Inhalten beim ursprünglichen Rechteinhaber.

8 Pflichten und Obliegenheiten des Kunden

- 8.1 Der Kunde ist verpflichtet, die ihm bzw. ihm zugeordneten Nutzern bereitgestellten Nutzungs- und Zugangsdaten geheim zu halten, vor dem Zugriff durch Dritte zu schützen und nicht an andere Nutzer oder Dritte weiterzugeben. Der Kunde hat geeignete Vorkehrungen zu treffen, um Missbrauch der Nutzungs- und Zugangsdaten und eine unbefugte Nutzung der Software zu verhindern.
- 8.2 Der Kunde wird ICSCS unverzüglich unterrichten, wenn der Verdacht besteht, dass Zugangsdaten oder Kennwörter nicht berechtigten Personen bekannt geworden sein könnten oder ihm Erkenntnisse vorliegen, dass über die von ihm eröffnete Telekommunikationsverbindung zum Server von ICSCS ein unberechtigter Zugriff auf das System von ICSCS stattgefunden hat.
- 8.3 Der Kunde stellt sicher, dass über die von ihm eröffnete Telekommunikationsverbindung zum Server von ICSCS a) Daten weder aus dem System von ICSCS abgerufen werden, noch in das System von ICSCS übertragen werden, es sei denn, dass dies einer vertragsgemäßen Nutzung entspricht, b) die Sicherheit und/oder Integrität des Systems von ICSCS und/oder der dort gespeicherten Daten nicht gefährdet werden und c) vor der Versendung von Daten und Informationen an ICSCS diese auf Viren geprüft sind. Der Kunde wird hierzu auf Geräten, über die der Kunde auf das System von ICSCS Zugriff nimmt, laufend aktualisierte Virenschutzprogramme nach Stand der Technik einsetzen.
- 8.4 Der Kunde stellt sicher, dass die von ihm zum Server von ICSCS übermittelten Inhalte frei von Rechten Dritter sind oder er über hinreichende Nutzungs- und Verwertungsrechte verfügt.
- 8.5 Der Kunde stellt sicher, dass die von ICSCS zur Verfügung gestellten Funktionen nicht zu rassistischen, diskriminierenden, pornographischen, den Jugendschutz gefährdenden, politisch extremen oder sonst gesetzeswidrigen oder gegen behördliche Vorschriften oder Auflagen verstößenden Zwecken verwendet und insbesondere nicht zur Herstellung entsprechender Daten eingesetzt wird.
- 8.6 Der Kunde bleibt Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO und stellt sicher, dass das Überlassen und die Verarbeitung personenbezogener Daten im Rahmen der Leistungen auf einer geeigneten Rechtsgrundlage beruhen und die Informationspflichten gegenüber Betroffenen erfüllt sind.
- 8.7 Der Kunde ist verpflichtet, Mängel an und Störungen der Software gegenüber ICSCS unverzüglich anzuzeigen und die aufgetretene Störung so präzise wie möglich unter Angabe der ihm bekannten und für die Störungsbeseitigung zweckdienlichen Informationen zu beschreiben („**qualifizierte Störungsmeldung**“).
- 8.8 Der Kunde stellt sicher, sofern und soweit ihm einvernehmlich die technische Möglichkeit dazu eröffnet wird, regelmäßig die auf dem Server von ICSCS gespeicherten Anwendungsdaten durch Download zu sichern.

- 8.9 Der Kunde stellt sicher, dass die auf seine Veranlassung hin ihm zugeordneten Nutzer sich ihrerseits zur Einhaltung der nach diesen Bestimmungen geltenden Pflichten und Obliegenheiten verpflichten.

9 Datensicherung

- 9.1 **Der Kunde stellt sicher, dass die unter Nutzung der von ICSCS zur Verfügung gestellten Funktionen erzeugten Anwendungsdaten regelmäßig und der Bedeutung der Daten entsprechend gesichert werden, um bei Verlust von Daten diese wiederherstellen zu können.**
- 9.2 Da Anwendungsdaten teilweise unmittelbar auf den Servern von ICSCS gespeichert werden, bevor dem Kunden eine technische Zugriffsmöglichkeit auf diese Daten eingeräumt wird, ist dem Kunden eine vorgelagerte Datensicherung dieser Daten faktisch nicht möglich. ICSCS übernimmt daher die Erstverantwortung für die Datensicherung dieser Anwendungsdaten ab dem Zeitpunkt ihres Eingangs im System von ICSCS.
- 9.3 Die Datensicherung erfolgt unter Einsatz dem Stand der Technik entsprechender Sicherheitsmaßnahmen sowie unter Beachtung angemessener organisatorischer und technischer Maßnahmen zur Wahrung der Datenintegrität. ICSCS stellt dem Kunden im Fall eines Datenverlusts – soweit technisch möglich – eine Rücksicherung auf Basis der zuletzt erstellten Sicherung zur Verfügung.
- 9.4 **Unbeschadet der durch ICSCS vorgenommenen serverseitigen Sicherung bleibt der Kunde verpflichtet, zusätzlich regelmäßig eigene Sicherungskopien der Anwendungsdaten durch Download zu erstellen, sofern und soweit ihm dies technisch möglich und zumutbar ist.**
- 9.5 Auf die Haftungsbeschränkungen der Ziffer 14, insbesondere 14.6, wird verwiesen.

10 Sperrung, Löschung

- 10.1 Verletzt der Kunde die Regelungen in Ziffer 8.1, kann ICSCS nach vorheriger Benachrichtigung des Kunden in Textform den Zugriff des Kunden auf die Software oder Anwendungsdaten sperren, wenn die Verletzung hierdurch nachweislich abgestellt werden kann.
- 10.2 Verstößt der Kunde rechtswidrig gegen Ziffer 8.5, ist ICSCS berechtigt, die dadurch betroffenen Daten bzw. Anwendungsdaten zu löschen.

11 Datenbankwerke

- 11.1 Sofern und soweit während der Laufzeit dieses Vertrages, insbesondere durch Zusammenstellung von Anwendungsdaten, durch nach diesem Vertrag erlaubte Tätigkeiten des Kunden auf dem Server von ICSCS eine Datenbank, Datenbanken, ein Datenbankwerk oder Datenbankwerke entstehen, stehen alle Rechte hieran dem Kunden zu. Der Kunde bleibt auch nach Vertragsende Eigentümer der Datenbanken bzw. Datenbankwerke. Nach Ermöglichter Datensicherung und vorheriger Mitteilung in Textform, mit der der Kunde zum Download der Datensicherung in einem gängigen, maschinenlesbaren Format binnen drei Wochen aufgefordert wird, ist ICSCS gleichwohl zum Löschen solcher Werke berechtigt.

12 Vergütung, Zahlungsbedingungen

- 12.1 Die Rechnungsstellung für die Nutzung der SaaS-Lösung erfolgt über ICS im Auftrag von ICSCS. Der Kunde verpflichtet sich, sämtliche Zahlungen an ICS zu leisten, welche die Beträge an ICSCS weiterleitet. Die Zahlungsbedingungen des Vertrags bleiben unberührt. ICS handelt ausschließlich als Zahlungsabwickler und ist nicht Vertragspartner für die Nutzung der SaaS-Dienstleistung und übernimmt keine Haftung für Forderungen oder Reklamationen, die sich auf die Qualität oder Funktionalität der Software beziehen.
- 12.2 Soweit im Angebot gemäß Ziffer 2 nicht anders vereinbart, richtet sich die Höhe der Vergütung nach der von ICSCS zum Zeitpunkt des Vertragsschlusses gültigen Preisliste.
- 12.3 Die vereinbarte Vergütung wird fällig mit Rechnungsstellung mit einer Zahlungsfrist von 14 Tagen, jedoch nicht vor Bereitstellung der Software und Übermittlung der Information über die Bereitstellung an den Kunden.
- 12.4 Zahlungen sind ohne Abzug zu leisten. Skonto wird nur gewährt, soweit dies durch ICSCS schriftlich oder in Textform zugesichert worden ist.
- 12.5 Alle Preise verstehen sich zuzüglich der jeweils geltenden gesetzlichen Umsatzsteuer.
- 12.6 Die Preise für Lieferungen schließen Transport und Verpackung bei körperlichem Versand nicht ein. Bei Bereitstellung zum Abruf über ein Netz trägt ICSCS die Kosten dafür, die Software abrufbar ins Netz zu stellen, der Kunde die Kosten für den Abruf.

13 Rechte des Kunden bei Mängeln

- 13.1 ICSCS gewährleistet, dass die Software frei von Mängeln ist, insbesondere keine Viren und ähnliche Schadsoftware enthält, welche die Tauglichkeit der Software zum vertragsgemäßen Gebrauch aufheben.
- 13.2 ICSCS ist verpflichtet, Mängel an der bereitgestellten Software einschließlich der Dokumentation zu beheben.
- 13.3 Die Behebung von Mängeln erfolgt nach Wahl von ICSCS durch kostenfreie Nachbesserung oder Ersatzlieferung.
- 13.4 Eine Kündigung des Kunden gem. § 543 Abs. 2 Satz 1 Nr. 1 BGB wegen Nichtgewährung des vertragsgemäßen Gebrauchs ist erst zulässig, wenn ICSCS ausreichende Gelegenheit zur Mängelbeseitigung gegeben wurde und diese fehlgeschlagen ist. Von einem Fehlschlagen der Mängelbeseitigung ist erst auszugehen, wenn diese unmöglich ist, wenn sie von ICSCS verweigert oder in unzumutbarer Weise verzögert wird, wenn begründete Zweifel bezüglich der Erfolgsaussichten bestehen oder wenn aus anderen Gründen eine Unzumutbarkeit für den Kunden gegeben ist.

14 Haftungsbeschränkungen

- 14.1 ICSCS haftet im Rahmen der gesetzlichen Bestimmungen jeweils unbeschränkt für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, die auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung bzw. sonst auf vorsätzlichem oder grob fahrlässigem Verhalten von ICSCS oder eines seiner gesetzlichen Vertreter oder Erfüllungsgehilfen beruhen, wegen des Fehlens oder des Wegfalls einer zugesicherten Eigenschaft, die auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung bzw. sonst auf vorsätzlichem oder grob fahrlässigem Verhalten von ICSCS oder eines seiner gesetzlichen Vertreter oder Erfüllungsgehilfen beruhen.

- 14.2 ICSCS haftet unter Begrenzung auf Ersatz des vertragstypischen vorhersehbaren Schadens für solche Schäden, die auf einer leicht fahrlässigen Verletzung von wesentlichen Vertragspflichten durch ICSCS oder einer seiner gesetzlichen Vertreter oder Erfüllungsgehilfen beruhen.
- 14.3 ICSCS haftet für sonstige Fälle leicht fahrlässigen Verhaltens begrenzt auf das Dreifache der monatlichen Nutzungsvergütung je Schadensfall.
- 14.4 Die vorstehenden Bestimmungen gelten sinngemäß auch für die Haftung von ICSCS im Hinblick auf den Ersatz vergeblicher Aufwendungen.
- 14.5 Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.
- 14.6 **Soweit es sich um solche Daten handelt, die der Kunde vor der Verarbeitung durch ICSCS bereits in seinem Besitz oder Verantwortungsbereich hatte, trifft den Kunden die Pflicht, regelmäßig und in angemessenem Umfang Datensicherungen vorzunehmen. ICSCS haftet für Verluste oder Beschädigungen solcher Kundendaten nur bei vorsätzlicher oder grob fahrlässiger Verursachung. Eine weitergehende Haftung für leichte Fahrlässigkeit ist insoweit ausgeschlossen.**

Soweit es sich um Daten handelt, die vor ihrer Verarbeitung durch ICSCS nicht bereits im Besitz oder Verantwortungsbereich des Kunden waren (z. B. neu generierte oder von ICSCS bereitgestellte Daten), haftet ICSCS für Verluste oder Beschädigungen solcher Kundendaten nur bei Vorsatz und grober Fahrlässigkeit unbeschränkt, sowie bei leichter Fahrlässigkeit beschränkt auf das Dreifache der monatlichen Nutzungsvergütung je Schadensfall.

Die gesetzlichen Bestimmungen zur zwingenden Haftung von ICSCS bleiben unberührt, insbesondere die Haftung für Schäden aus der Verletzung von Leben, Körper oder Gesundheit, nach dem Produkthaftungsgesetz sowie für das Fehlen zugesicherter Eigenschaften. Gleiches gilt für die in Ziffer 14.1–14.5 geregelten Ausnahmen und Haftungsgrundsätze, die Anwendung finden, soweit diese Klausel nicht vorrangige Sonderregelungen trifft.

- 14.7 ICS ist nicht Anbieter der SaaS-Lösung und haftet weder für Mängel, Systemausfälle, Datenverluste oder sonstige Schäden, die aus der Nutzung der Software der von ICSCS bereitgestellten SaaS-Lösung oder aus einer Pflichtverletzung von ICSCS resultieren. ICS ist nicht verantwortlich für die Erfüllung der vertraglichen Pflichten von ICSCS und übernimmt keinerlei Garantien oder Gewährleistungen im Zusammenhang mit der Nutzung oder Bereitstellung der Software. Sollte ICS trotz dieses Haftungsausschlusses aus gesetzlichen Gründen haften müssen, gelten die Haftungsbeschränkungen der 14.1, 14.2 sowie 14.4, 14.5 auch für ICS.
- 14.8 ICS erbringt den 1st-Level-Support ausschließlich als Erfüllungsgehilfe (§ 278 BGB) von ICSCS. Eine eigenständige vertragliche oder deliktische Haftung von ICS gegenüber dem Kunden ist ausgeschlossen, sofern nicht gesetzlich zwingend eine Haftung besteht (vgl. § 823 ff. BGB)

15 Vertraulichkeit

- 15.1 Die Vertragspartner verpflichten sich, alle im Rahmen der Vertragsanbahnung und Vertragsdurchführung erlangten Kenntnisse von vertraulichen Informationen und Betriebsgeheimnissen des jeweils anderen Vertragspartners zeitlich unbegrenzt vertraulich zu behandeln und nur für Zwecke der Durchführung dieses Vertrages zu verwenden.
- 15.2 Der Kunde wird Vertragsgegenstände Mitarbeitern und sonstigen Dritten nur zugänglich machen, soweit dies zur Ausübung der ihm eingeräumten Nutzungsbefugnisse erforderlich ist. Er wird alle Personen, denen er Zugang zu Vertragsgegenständen gewährt, über die Rechte von

ICSCS an den Vertragsgegenständen und die Pflicht zu ihrer Geheimhaltung belehren und diese Personen nachweisbar zur entsprechenden Geheimhaltung verpflichten, soweit die betreffenden Personen nicht aus anderen Rechtsgründen zur Geheimhaltung mindestens in vorstehendem Umfang verpflichtet sind.

- 15.3 Die vorstehenden Verpflichtungen gelten nicht für Betriebsgeheimnisse, die (i) zur Zeit ihrer Übermittlung durch den Vertragspartner bereits offenkundig oder der anderen Vertragspartei bekannt waren; (ii) nach ihrer Übermittlung durch den Vertragspartner ohne Verschulden der anderen Vertragspartei offenkundig geworden sind; (iii) nach ihrer Übermittlung durch den Vertragspartner der anderen Vertragspartei von dritter Seite auf nicht rechtswidrige Weise und ohne Einschränkung in Bezug auf Geheimhaltung oder Verwertung zugänglich gemacht worden sind; (iv) die von einer Vertragspartei eigenständig, ohne Nutzung der Betriebsgeheimnisse des Vertragspartners, entwickelt worden sind; (v) die gemäß Gesetz, behördlicher Verfügung oder gerichtlicher Entscheidung veröffentlicht werden müssen – vorausgesetzt, die veröffentlichende Partei informiert den Vertragspartner hierüber unverzüglich und unterstützt ihn in der Abwehr derartiger Verfügungen bzw. Entscheidungen; oder (vi) soweit dem Vertragspartner die Nutzung oder Weitergabe der Betriebsgeheimnisse auf Grund zwingender gesetzlicher Bestimmungen oder auf Grund dieses Vertrages gestattet ist.

16 Datenschutz

- 16.1 ICSCS hält die Regeln des Datenschutzes ein, insbesondere wenn ihm Zugang zum Betrieb oder zu Hard- und Software des Kunden gewährt wird. ICSCS stellt sicher, dass seine Erfüllungsgehilfen diese Bestimmungen ebenfalls einhalten. Sofern Tätigkeiten der ICSCS eine Auftragsverarbeitung gem. Art. 28 DSGVO darstellen gilt für diese die ANLAGE: Auftragsverarbeitungsvereinbarung, die Bestandteil dieses Vertrages ist.
- 16.2 ICS erhält Zugriff auf Kundendaten ausschließlich in dem Umfang, wie es für die Durchführung dieses Vertrags erforderlich ist. Dies umfasst insbesondere die Verarbeitung von Kundendaten zur Rechnungsstellung, sofern durch den Kunden gewünscht bei der Einrichtung der SaaS-Lösung, sowie zur Unterstützung bei der Einhaltung von Service-Level-Agreements, sofern ICSCS dies verlangt. ICS verpflichtet sich, alle dabei bekannt werdenden Informationen und Daten gemäß der Datenschutz-Grundverordnung (DSGVO) sowie den geltenden Datenschutzgesetzen vertraulich zu behandeln. Eine Nutzung oder Weitergabe der Kundendaten durch ICS zu anderen als den vertraglich vorgesehenen Zwecken ist ausgeschlossen. Falls ICS im Auftrag von ICSCS personenbezogene Daten des Kunden verarbeitet, wird eine separate Auftragsverarbeitungsvereinbarung gemäß Art. 28 DSGVO zwischen ICS und ICSCS geschlossen.

17 Vertragslaufzeit, Kündigung

- 17.1 Der Vertrag kommt mit allseitiger Unterzeichnung des Vertrags und Bereitstellung gemäß Ziffer 2.6 zustande. Soweit nicht im Angebot anders bestimmt, hat der Vertrag eine Mindestvertragslaufzeit von 36 Kalendermonaten und verlängert sich um jeweils weitere zwölf (12) Kalendermonate, sofern nicht eine der Vertragsparteien der Verlängerung der Vertragslaufzeit rechtzeitig widerspricht. Der Widerspruch gegen die Verlängerung der Vertragslaufzeit gilt als rechtzeitig, wenn der Widerspruch bis zum 30.09. des laufenden Jahres erklärt worden ist. Der Vertrag endet nach Ablauf der jeweiligen Vertragslaufzeit zum 31.12. des laufenden Kalenderjahres.

- 17.2 Während der Vertragslaufzeit ist das Recht zur Kündigung für beide Vertragsparteien, Anbieter und Kunde, ausgeschlossen. Das Recht zur Kündigung aus wichtigem Grund bleibt hiervon unberührt.
- 17.3 Der Widerspruch gegen die Verlängerung der Vertragslaufzeit gemäß Ziffer 17.1 und die Kündigung gemäß Ziffer 17.2 bedürfen der Textform.
- 17.4 ICS hat im Rahmen dieses Vertrags keine eigenständigen Kündigungsrechte. Der SaaS-Nutzungsvertrag besteht ausschließlich zwischen ICSCS und dem Kunden. Kündigungen oder Änderungen des Vertrags können nur durch den Kunden oder die ICSCS erklärt werden und wirken sich automatisch auf die von ICS im Rahmen dieses Vertrags erbrachten Leistungen aus, ohne dass es einer gesonderten Kündigungserklärung gegenüber oder durch ICS bedarf.

18 Vertragsbeendigung

- 18.1 Bei Beendigung des Vertragsverhältnisses hat der Kunde ICSCS die im Rahmen der vertragsgemäßen Nutzung überlassenen Gegenstände in ordnungsgemäßem Zustand zurückzugeben. Die Rückgabepflicht umfasst auch die überlassenen Handbücher und Dokumentation. Gegebenenfalls erstellte Kopien sind zu vernichten.

19 Anpassung von Vertragslaufzeit und Vergütung bei Entwicklungsleistungen

- 19.1 Kommt es aufgrund von vom Kunden in Auftrag gegebenen Entwicklungsleistungen zu einer nicht nur unerheblichen Ausweitung des Nutzungs- und Funktionsumfangs der Software, weist der Anbieter den Kunden hierauf sowie auf die daraus folgende Verlängerung der Mindestvertragslaufzeit rechtzeitig vor der Beauftragung in Textform hin. Erteilt der Kunde die Beauftragung, beginnt die Mindestvertragslaufzeit neu zu laufen. Ziffer 17.1 gilt entsprechend.
- 19.2 In den Fällen der Ziffer 19.1 ist der Anbieter berechtigt, die laufende Vergütung angemessen an den erweiterten Nutzungs- und Funktionsumfang anzupassen. Einmalige Entgelte für die Entwicklungsleistungen bleiben hiervon unberührt. Die Höhe der Anpassung teilt der Anbieter dem Kunden im Rahmen der Beauftragung gemäß Ziffer 19.1 in Textform mit. Mit Erteilung der Beauftragung gilt die mitgeteilte Anpassung als vereinbart. Der Zeitpunkt der Wirksamkeit der Anpassung ergibt sich aus der Mitteilung.

20 Höhere Gewalt

- 20.1 Keiner der Vertragspartner ist zur Erfüllung der vertraglichen Verpflichtungen im Fall und für die Dauer höherer Gewalt verpflichtet. Insbesondere folgende Umstände sind als höhere Gewalt in diesem Sinne anzusehen:
- von dem Vertragspartner nicht zu vertretende(s) Feuer, Explosion, Überschwemmung,
 - Krieg, Meuterei, Blockade, Embargo, Pandemie
 - über sechs (6) Wochen andauernder und von dem Vertragspartner nicht schuldhaft herbeigeführter Arbeitskampf,
 - nicht von einem Vertragspartner beeinflussbare technische Probleme des Internets.
- 20.2 Jeder Vertragspartner hat den anderen über den Eintritt eines Falls höherer Gewalt unverzüglich mindestens in Textform in Kenntnis zu setzen.

21 Schlussbestimmungen

- 21.1 Nebenabreden zu diesem Vertrag wurden zwischen den Parteien nicht getroffen.
- 21.2 Diese Vereinbarung sowie Änderungen und Ergänzungen bedürfen der Textform. Mündliche Nebenabreden bestehen nicht, und auch der Verzicht auf sowie Änderungen dieser Textformklausel bedürfen der Textform. § 305b BGB bleibt unberührt.
- 21.3 Sollte eine der Bestimmungen dieser Vereinbarung unwirksam oder nichtig sein oder werden oder sollte diese Vereinbarung eine Regelungslücke enthalten, so wird hierdurch die Gültigkeit der übrigen Bestimmungen nicht berührt. Anstelle der unwirksamen bzw. nichtigen Bestimmung bzw. anstelle der Regelungslücke soll eine rechtswirksame Ersatzbestimmung treten, die dem wirtschaftlichen Zweck der unwirksamen bzw. nichtigen Bestimmung bzw. dieser Vereinbarung als Ganzes möglichst nahekommt.
- 21.4 Alle Streitigkeiten, die sich aus oder im Zusammenhang mit diesem Vertrag ergeben, unterstehen dem Recht der Bundesrepublik Deutschland unter Ausschluss der Verweisungsnormen des Internationalen Privatrechts. Ausschließlicher Gerichtsstand ist Nürnberg.

Anlagen

ANLAGE: Verfügbarkeit

ANLAGE: Störungsbeseitigung

ANLAGE: Auftragsverarbeitungsvereinbarung

ICSCS

Kunde

Leipzig, den

, den

ics cloud services GmbH

ic-solution GmbH

Kunde

ANLAGE: Verfügbarkeit

- ICSCS gewährleistet eine Verfügbarkeit von 98 Prozent bezogen auf das Monatsmittel. Verfügbarkeit wird unter Anwendung folgender Formel ermittelt:
- Verfügbarkeit (%) =
Verfügbarkeit (h) innerhalb Systemlaufzeit / Systemlaufzeit (h) x 100 %
- Im Falle einer Unterschreitung der vereinbarten Verfügbarkeit ist der Kunde berechtigt, die Vergütung für den folgenden Abrechnungszeitraum wie folgt zu mindern:

von	bis	Minderung
100,0 %	99,01 %	0 %
99,0 %	98,01 %	15 %
98,0 %	97,01 %	25 %
97,0 %	96,01 %	35 %
96,0 %	95,01 %	45 %
95,0 %	-	55 %

- Bei einem durchgehenden Ausfall der Systeme an zwei aufeinander folgenden Arbeitstagen hat der Kunde Anspruch auf Rückerstattung von 75 % des für den Abrechnungszeitraum des Ausfalls gezahlten Zahlungsbetrags. Bei einem durchgehenden Ausfall der Systeme an drei aufeinander folgenden Arbeitstagen beträgt die entsprechende Erstattung 100 %.

ANLAGE: Störungsbeseitigung

Störungsklasse	Reaktionszeit	Wiederherstellungszeit
Klasse 1 (schwere bzw. den Betrieb verhindernde Störungen): Eine oder mehrere Kernfunktionen sind vollständig nicht verfügbar; eine Umgehungslösung existiert nicht.	2 Stunden	4 Stunden
Klasse 2 (bedeutende bzw. den Betrieb beeinträchtigende Störungen): Eine oder mehrere Kernfunktionen sind teilweise nicht verfügbar oder wesentlich beeinträchtigt, ohne dass eine Umgehungslösung zur Verfügung steht.	4 Stunden	8 Stunden
Klasse 3 (minderschwere bzw. den Betrieb nicht beeinträchtigende Störungen): Sporadische Fehler, die die Verfügbarkeit der Kernfunktionen nicht beeinträchtigen.	8 Stunden	16 Stunden

Anlage Vereinbarung zur Auftragsverarbeitung nach Art. 28 DS-GVO

zwischen

dem im zustande gekommenen Leistungsvertrag
genannten „Kunde“

– nachstehend „Auftraggeber“ genannt –

als Verantwortlicher

und

ics cloud services GmbH
Möckernsche Str. 3
04155 Leipzig

– nachstehend „Auftragnehmer“ genannt –

als Auftragsverarbeiter

– gemeinsam „Vertragsparteien“ oder „Parteien“ –

§ 1 Generelles

- (1) Die vorliegende Vereinbarung (nebst ihrer unten näher bezeichneten Anlagen) zur Auftragsverarbeitung (nachfolgend auch „Vereinbarung“) konkretisiert gesetzliche Rechte und Pflichten, die sich für die Parteien aus der Datenschutzgrundverordnung (VO (EU) 2016/679, nachfolgend auch „DS-GVO“) im Hinblick auf die Verarbeitung personenbezogener Daten ergeben.
- (2) Der Auftragnehmer erkennt an, dass die DS-GVO die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten schützt und diese Prinzipien auch für den Auftragnehmer gelten.

§ 2 Begriffsbestimmungen

- (1) Es gelten die Begriffsbestimmungen aus Art. 4 und Art. 9 DS-GVO sowie folgende zusätzlichen Begriffsbestimmungen:
 - a) **„Leistungsvertrag“** meint das Rechtsverhältnis zwischen dem Auftraggeber und dem Auftragnehmer, aufgrund dessen der Auftragnehmer für den Auftraggeber bestimmungsgemäß Auftragsverarbeitung betreibt. Dabei kann es sich auch um aufeinanderfolgende Aufträge handeln.
 - b) **„Unterauftragnehmer“** meint Dritte im Sinne des Art. 4 Nr. 10 DS-GVO, die der Auftragnehmer mit schriftlicher Gestattung des Auftraggebers zur Leistungserbringung im Rahmen des Leistungsvertrags einsetzt.
- (2) Weitere Begriffsbestimmungen können kontextbezogen in der jeweiligen Ziffer dieser Vereinbarung getroffen werden.

§ 3 Gegenstand und Bestandteile der Vereinbarung

- (1) Die Auftragsverarbeitung durch den Auftragnehmer erfolgt stets auf der Grundlage eines Leistungsvertrags zwischen dem Auftragnehmer und dem Auftraggeber. Im Rahmen der Ausführung der in diesem Vertrag vereinbarten Leistungen wird dem Auftragnehmer Zugriff auf Testsysteme, teilweise aber auch auf Produktivsysteme, des Auftraggebers gewährt, wobei eine Verarbeitung personenbezogener Daten nicht ausgeschlossen werden kann. Daher gehen die Vertragsparteien von einer Auftragsverarbeitung i.S.d. Art. 28 DS-GVO aus.
- (2) Grundsätzlich ist der Leistungsvertrag maßgeblich für den Gegenstand, die Dauer, die Art und den Zweck der Auftragsverarbeitung, sowie für die Frage, welche Art personenbezogener Daten betroffen sind. Die Art oder Arten der personenbezogenen Daten und der Kreis der betroffenen Personen werden vom Auftraggeber bestimmt und sind in der als Anlage 1 dieser Vereinbarung beigefügten Auflistung aufgeführt. Bei Änderungen bezüglich dieser Auflistung wird der Auftraggeber den Auftragnehmer unverzüglich informieren.
- (3) Soweit in dem Leistungsvertrag nichts anderes geregelt ist, erfolgt die Auftragsverarbeitung zum Zweck der Einrichtung, Anpassung und Wartung von Softwaresystemen, welche der Auftraggeber von dem Auftragnehmer erworben hat.
- (4) Verbindliche Vertragsbestandteile dieser Vereinbarung, neben dem Leistungsvertrag, sind:

- a) Anlage 1 Art der personenbezogenen Daten und Kategorien von Betroffenen
 - b) Anlage 2 Sicherheit der Verarbeitung / TOM's
 - c) Anlage 3 Unterauftragnehmer
 - d) Anlage 4 Anonymisiertes Training
- (5) Die Bestimmungen dieser Vereinbarung einschließlich ihrer Anlagen gehen etwaigen widersprüchlichen Regelungen des zugrundeliegenden Leistungsvertrags vor, soweit es um die Verarbeitung personenbezogener Daten geht.

§ 4 Wirksamkeit und Dauer der Auftragsverarbeitung

- (1) Diese Vereinbarung tritt mit dem Vertragsbeginn aus dem Leistungsvertrag in Kraft. Ist kein gesondertes Datum vermerkt, so gilt als Datum der Beginn der Leistungen als vereinbart.
- (2) Ist der Leistungsvertrag zeitlich befristet, endet diese Vereinbarung mit Ablauf des Leistungsvertrages. Ansonsten endet sie automatisch und ohne dass es einer Kündigung bedarf, wenn der Auftragnehmer für den Auftraggeber insgesamt keine Auftragsverarbeitung oder -wartung mehr betreibt.
- (3) Das Recht zu ordentlichen Kündigungen ist ausgeschlossen. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund nach Maßgabe des § 314 BGB bleibt unberührt.

§ 5 Grundsätze zur Auftragsverarbeitung

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich nach Maßgabe des Leistungsvertrags, nach Maßgabe dieser Vereinbarung sowie im Rahmen von Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO). Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).
- (2) Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt. Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden. Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.
- (3) Die Arten bzw. Kategorien der personenbezogenen Daten, die auf der Grundlage des Leistungsvertrages und dieser Vereinbarung verarbeitet werden, und die Kategorien betroffener Personen sind in der Anlage 1 zu dieser Vereinbarung aufgeführt.

§ 6 Ort der Auftragsverarbeitung

- (1) Die Auftragsverarbeitung wird vorerst ausschließlich – vorbehaltlich der nachfolgenden Bestimmungen – in Deutschland, einem anderen Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erfolgen.
- (2) Jede Verlagerung der Auftragsverarbeitung in ein Gebiet außerhalb eines Mitgliedsstaates der Europäischen Union oder außerhalb eines anderen Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum (im Folgenden „Drittland“) bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers.
- (3) Die Zustimmung zur Auftragsverarbeitung in einem Drittland wird insbesondere dann nicht erteilt, soweit die besonderen Voraussetzungen der Art. 44 f. DS-GVO nicht dauerhaft erfüllt sind, insbesondere ein angemessenes Schutzniveau im Drittland nicht besteht, oder keine geeigneten Garantien bestehen, die ein angemessenes Schutzniveau sicherstellen.
- (4) Der Auftragnehmer trägt auf seine Kosten dafür Sorge, dass ein angemessenes Schutzniveau im Drittland sichergestellt ist und weist dies dem Auftraggeber im Rahmen der Zustimmungseinholung nach, insbesondere durch:
 - einen Angemessenheitsbeschluss der EU-Kommission (Art. 45 Abs. 3 DSGVO);
 - verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit b. i.V.m Art. 47 DS-GVO);
 - Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c und lit. d DS-GVO);
 - genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit e i.V.m Art. 40 DS-GVO);
 - genehmigte Zertifizierungsmechanismen (Art. 46 Abs. 2 lit f. i.V.m Art 42 DS-GVO); oder
 - sonstige Maßnahmen (Art. 46 Abs. 2 lit a., Abs. 3 lit. a und lit. b DS-GVO).

§ 7 Sicherheit der Verarbeitung

- (1) Der Auftragnehmer hat für die zu verarbeitenden Daten angemessene technische und organisatorische Sicherheitsmaßnahmen im Sinne des Art. 28 Abs. 3 lit. c, Art. 32 DS-GVO in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO, bzw. der für das Auftragsverhältnis geltenden speziellen Vorschriften (Landesdatenschutzgesetze, SGB) getroffen, die in der Anlage 2 dieses Vertrages dokumentiert sind. Er hat diese Sicherheitsmaßnahmen für die gesamte Dauer der Auftragsverarbeitung aufrecht zu erhalten.
- (2) 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, 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 DS-GVO zu berücksichtigen.
- (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) Bei der Verarbeitung personenbezogener Daten, der Auslegung der Anforderungen der DS-GVO sowie der Auslegung dieser Vereinbarung sind die jeweils geltenden Empfehlungen der Art. 29 Datenschutzgruppe oder deren Nachfolgeorganisation (Europäischer Datenschutzausschuss) angemessen zu berücksichtigen.

§ 8 Verschwiegenheitspflicht

- (1) Der Auftragnehmer garantiert, dass er die bei ihm mit der Verarbeitung beschäftigten Personen zur Vertraulichkeit verpflichtet hat, und er diese Verpflichtung durch organisatorische Vorkehrungen auch nachhält, insbesondere dass personenbezogene Daten nicht unbefugt, nur auftragsgemäß bzw. nach Weisungen verarbeitet werden, und dass diese Verpflichtung auch nach Beendigung ihrer Tätigkeit fortbesteht (Art. 28 Abs. 3 lit b); Art. 29; Art. 32 Abs. 4 DS-GVO). Entsprechendes gilt für weitere datenschutzrechtliche Vertraulichkeits- und/oder Schutzbestimmungen, soweit diese für die Verarbeitung einschlägig sind. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Dies gilt insbesondere in den Fällen, in denen der Auftraggeber zur Einhaltung der Schweigepflicht aus § 203 StGB verpflichtet ist. Der Auftraggeber wird dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitteilen. Dem Auftraggeber sind auf Verlangen entsprechende Nachweise unentgeltlich zur Verfügung zu stellen.
- (2) Der Auftragnehmer kann den Nachweis, dass er die oben genannten Pflichten einhält, auch dadurch erbringen, dass er die Einhaltung genehmigter Verhaltensregeln (Art. 40 DS-GVO) oder die Einhaltung eines genehmigten Zertifizierungsverfahrens (Art. 42 DS-GVO) nachweist, soweit hieraus hervorgeht, dass die bei der Verarbeitung eingesetzten Personen nach § 8 Abs. 1 zur Vertraulichkeit verpflichtet sind.
- (3) Der Nachweis kann nur (und nur solange) dadurch erfolgen, dass der Auftragnehmer dem Auftraggeber ein gültiges Zertifikat vorweist, welches von einer akkreditierten Zertifizierungsstelle nach Art. 43 DS-GVO für diejenigen Verarbeitungsverfahren und -orte erteilt ist, die für die Verarbeitungen unter dieser Vereinbarung beziehungsweise den entsprechenden Leistungsvertrag relevant sind. Veränderungen am Zertifikat oder dessen Ablauf hat der Auftragnehmer dem Auftraggeber unverzüglich mitzuteilen.

§ 9 Fernwartung

- (1) Sofern der Auftragnehmer die Wartung und Pflege der IT-Systeme im Wege der Fernwartung durchführt, ist der Auftragnehmer verpflichtet, dem Auftraggeber eine wirksame Kontrolle der Fernwartungsarbeiten zu ermöglichen. Dies kann z. B. durch Einsatz einer Technologie erfolgen, die dem Auftraggeber ermöglicht, die vom Auftragnehmer durchgeführten Arbeiten auf einem Monitor o.ä. Gerät zu verfolgen.
- (2) Wenn der Auftraggeber bei Fernwartungsarbeiten nicht wünscht, die Tätigkeiten an einem Monitor o.ä. Gerät zu beobachten, wird der Auftragnehmer die von ihm durchgeführten Arbeiten in geeigneter Weise dokumentieren.
- (3) Für den Fall, dass der Auftraggeber einer Berufsgeheimnispflicht i.S.d. § 203 StGB unterliegt, hat dieser Sorge dafür zu tragen, dass eine unbefugte Offenbarung i.S.d. § 203 StGB durch die Fernwartung nicht erfolgt. Der Auftragnehmer ist diesbezüglich verpflichtet,

Technologien einzusetzen, die nicht nur ein Verfolgen der Tätigkeit auf dem Bildschirm ermöglicht, sondern dem Auftraggeber auch eine Möglichkeit gibt, die Fernwartungsarbeiten jederzeit zu unterbinden.

§ 10 Unterauftragnehmer

- (1) Der Auftraggeber stimmt der Beauftragung der in der Anlage 3 aufgeführten Unterauftragnehmer zu.
- (2) Der Auftragnehmer sichert zu, dass er die Unterauftragnehmer sorgfältig ausgewählt hat und dass diese Unterauftragnehmer vertraglich verpflichtet sind, bei der Ausführung der Leistungen dieselben datenschutzrechtlichen und sonstigen Pflichten einzuhalten, die in dieser Vereinbarung und den einschlägigen gesetzlichen Bestimmungen, insbesondere der DS-GVO, statuiert sind. Dies bedeutet insbesondere, dass beim Unterauftragnehmer geeignete technische und organisatorische Maßnahmen entsprechend durchgeführt werden und dass der Auftraggeber während der Laufzeit der Unterbeauftragung alle Rechte, die dem Auftraggeber gegenüber dem Auftragnehmer zustehen, auch gegenüber dem Unterauftragnehmer ausüben kann; dies beinhaltet auch Einsichtsrechte in datenschutzrelevante Unterlagen und Verträge und Auskunft über datenschutzrechtliche relevante Vorgänge.
- (3) Die Unterbeauftragung der Verarbeitung durch den Auftragnehmer an weitere Unterauftragnehmer ist nur mit schriftlicher Genehmigung des Auftraggebers und unter Einhaltung der gleichen Voraussetzungen zulässig.
- (4) Der Auftraggeber kann die Zustimmung zum Einsatz eines Unterauftragnehmers in begründeten Fällen, insbesondere im Falle einer Gesetzes- oder sonstigen Pflichtverletzung, widerrufen. Der Auftragnehmer hat unverzüglich die Unterbeauftragung der Verarbeitung einzustellen.

§ 11 Rechte der betroffenen Personen

- (1) Der Auftraggeber ist für die Wahrung der Rechte der betroffenen Personen nach dem 3. Kapitel DS-GVO verantwortlich. Dem Auftragnehmer ist eine Umsetzung der Rechte betroffener Personen nur nach Weisung des Auftraggebers gestattet. Der Auftragnehmer ist jedoch verpflichtet, den Auftraggeber bei der Erfüllung von Anfragen und Ansprüchen betroffener Personen nach dem 3. Kapitel der DS-GVO vollumfänglich zu unterstützen.
- (2) Werden Betroffenenrechte unmittelbar gegenüber dem Auftragnehmer geltend gemacht, hat der Auftragnehmer das Ersuchen unverzüglich an den Auftraggeber weiterzuleiten. Ist dem Auftragnehmer eine Zuordnung des Ersuchens zu einer Person nicht möglich, weist er die fehlende Identifizierbarkeit gegenüber dem Auftraggeber entsprechend Art. 11 Abs. 2 DS-GVO nach.

§ 12 Meldung von Datenschutzvorfällen

- (1) Der Auftragnehmer erstattet in jedem Fall dem Auftraggeber Meldung, in dem er (i) von einer Verletzung des Schutzes personenbezogener Daten durch ihn oder die bei ihm beschäftigten Personen, (ii) von einem Verstoß gegen Vorschriften zum Schutz personenbezogener Daten

oder (iii) von einem Verstoß gegen die in dieser Vereinbarung getroffenen Festlegungen Kenntnis erlangt (im folgenden „Datenschutzvorfall“).

- (2) Die Meldung hat unverzüglich, ab Kenntniserlangung, zu erfolgen.
- (3) Nach Kenntniserlangung eines Datenschutzvorfalls trifft der Auftragnehmer unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Abmilderung nachteiliger Auswirkungen für die betroffenen Personen und den Auftraggeber.
- (4) Die Meldung eines Datenschutzvorfalls hat – soweit möglich – sämtliche Informationen zu enthalten, die der Auftraggeber zur Erfüllung seiner Pflichten nach Art. 33 und Art. 34 DS-GVO benötigt; insbesondere
 - 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;
 - den Namen und die Kontaktdaten des Datenschutzbeauftragten des Auftragnehmers oder einer in der Sache auskunftsfähigen Person des Auftragnehmers;
 - eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
 - eine Beschreibung der vom Auftragnehmer bereits ergriffenen und der vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.
 - Der Auftragnehmer ist verpflichtet, Datenschutzvorfälle ausführlich zu dokumentieren einschließlich deren Auswirkungen und der ergriffenen Abhilfemaßnahmen; die Dokumentation ist dem Auftraggeber unverzüglich zur Verfügung zu stellen.
- (5) Der Aufwand und die Kostenlast einer Kontrolle beim Auftragnehmer ist grundsätzlich auf einen Tag pro Kalenderjahr begrenzt. Für zusätzliche Aufwände oder Kontrollen, denen nicht ein konkreter Anlass oder ein begründeter Verdacht der Verletzung personenbezogener Daten zu Grunde liegt, kann der Auftragnehmer die Erstattung sämtlicher angemessenen und nachgewiesenen Aufwendungen und Kosten (einschließlich Personalzeit nach den jeweils gültigen Stundensätzen, Vorbereitung und Bereitstellung von Unterlagen, Mitwirkungshandlungen sowie Reise- und Nebenkosten) verlangen.

§ 13 Mitwirkungspflichten des Auftragnehmers

- (1) Bezogen auf seinen Verantwortungsbereich ist der Auftragnehmer verpflichtet, die für das Verzeichnis der Verarbeitungstätigkeiten des Auftraggebers nach Art. 30 Abs. 1 DS-GVO erforderlichen Angaben und Informationen bereitzustellen.
- (2) Der Auftragnehmer wird – bezogen auf seinen Verantwortungsbereich – den Auftraggeber bei der Einhaltung der Pflichten nach Art. 32 bis 36 DS-GVO vollumfänglich beraten und unterstützen. Hierzu wird der Auftragnehmer dem Auftraggeber sämtliche für Art. 32 bis 36 DS-GVO erforderlichen Unterlagen, Dokumente und Nachweise zur Verfügung stellen.

- (3) Der Auftragnehmer ist verpflichtet, die Durchführung der Verarbeitung regelmäßig auf ihre Vertragskonformität hin selbst zu überprüfen. Werden im Rahmen der Prüfung Fehler oder Unregelmäßigkeiten bekannt, ist der Auftraggeber unverzüglich zu informieren.
- (4) Der Auftragnehmer ist verpflichtet, soweit gesetzlich vorgeschrieben, einen Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 37, 38 DS-GVO ausüben kann, zu bestellen. Die Kontaktdaten des Datenschutzbeauftragten oder eines anderen Ansprechpartners für Datenschutzfragen – soweit ein Datenschutzbeauftragter nicht zu bestellen ist – werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.

§ 14 Herausgabe von personenbezogenen Daten

- (1) Der Auftragnehmer erkennt an, dass der Auftraggeber infolge seiner Rolle als Verantwortlicher jederzeit dazu berechtigt sein muss, vom Auftragnehmer die Herausgabe von personenbezogenen Daten zu verlangen. Der Auftragnehmer garantiert dem Auftraggeber daher, technische und organisatorische Maßnahmen getroffen zu haben, um den Herausgabeanspruch unverzüglich erfüllen zu können, und verzichtet darauf, etwaige Einwendungen und Einreden gegen den Herausgabeanspruch zu erheben.
- (2) Der Herausgabeanspruch umfasst sämtliche personenbezogenen Daten, die der Auftragnehmer unter der Verantwortung des Auftraggebers verarbeitet, insbesondere vom Auftraggeber übermittelte personenbezogene Daten sowie personenbezogene Daten, die im Rahmen der Durchführung eines Leistungsvertrages verändert, entstanden oder geschaffen worden sind.
- (3) Nach vom Auftraggeber in Schrift- oder Textform bestätigter erfolgreicher Herausgabe der personenbezogenen Daten sind diese unverzüglich von den Speichermedien des Auftragnehmers derart zu löschen, sodass diese nicht mehr reproduziert werden können. Der Auftragnehmer übernimmt die Garantie für eine entsprechende Löschung dieser personenbezogenen Daten auf Speichermedien seiner etwaigen Unterauftragnehmer. Der Auftragnehmer hat dem Auftraggeber auf Verlangen die Durchführung dieser Löschung durch geeignete Dokumente oder einer entsprechenden Versicherung nachzuweisen. Vorstehendes gilt entsprechend, wenn die Verarbeitung personenbezogener Daten durch den Auftragnehmer endet, der Auftraggeber gegenüber dem Auftragnehmer jedoch ausdrücklich auf die Herausgabe verzichtet, und keine einer Löschung entgegenstehende Vereinbarung getroffen wurde.
- (4) Der Auftragnehmer darf bestimmte personenbezogene Daten anstelle ihrer Löschung in gesperrter Form speichern, solange und soweit der Auftragnehmer zwingenden gesetzlichen Bestimmungen unterliegt, die ihn zu einer Aufbewahrung verpflichten. Die Rechtmäßigkeit eines Zugriffs auf gesperrte Daten beurteilt sich nach der gesetzlichen Bestimmung, aufgrund derer die personenbezogenen Daten gesperrt werden mussten.
- (5) Im Fall der Wegnahme oder der Pfändung eines Speichermediums durch einen Dritten, auf dem personenbezogene Daten des Auftraggebers gespeichert sind, oder bei Betreibung der Zwangsvollstreckung in ein solches Speichermedium durch einen Dritten, hat der Auftragnehmer sowohl den Dritten über den Umstand, dass sich personenbezogene Daten des Auftraggebers auf dem betroffenen Datenträger befinden, als auch den Auftraggeber über die

entsprechende Maßnahme, unverzüglich zu informieren. Etwaige Rechtsmittel des Auftraggebers gegen die Maßnahmen des Dritten bleiben unberührt.

§ 15 Kontrollrechte des Auftraggebers

- (1) Der Auftraggeber hat während der Laufzeit dieser Vereinbarung bis zum Eintritt der allgemeinen Verjährung von Ansprüchen aus dieser Vereinbarung das Recht, Überprüfungen durchzuführen, oder im Einzelfall durch zur Verschwiegenheit verpflichtete Dritte bzw. Prüfer durchführen zu lassen. Der Auftraggeber hat insbesondere das Recht, sich durch Stichprobenkontrollen von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in seinem Geschäftsbetrieb zu den üblichen Geschäftszeiten zu überzeugen. Kontrollen sind in der Regel mit einer Vorlaufzeit von vierzehn (14) Tagen anzukündigen, sofern nicht eine Kontrolle ohne vorherige Anmeldung erforderlich erscheint, weil anderenfalls der Kontrollzweck gefährdet wäre.
- (2) In Abweichung zum Vorgenannten bestehen die genannten Kontrollrechte über die Laufzeit dieser Vereinbarung als auch die allgemeine Verjährung hinaus insoweit fort, als dass und solange der Auftragnehmer personenbezogene Daten entsprechend § 14 speichert.
- (3) Dies umfasst das Recht, das Grundstück, die Geschäftsräume und die Standorte der informationstechnischen Anlagen des Auftragnehmers zu betreten und dort Besichtigungen und Prüfungen vorzunehmen oder vornehmen zu lassen, sowie geschäftliche Unterlagen und gespeicherte Daten und Datenverarbeitungsprogramme einzusehen, soweit dies zur Auftragskontrolle erforderlich ist.
- (4) Kontrollen sind in der Regel mit einer Vorlaufzeit von vierzehn (14) Tagen anzukündigen. In dringenden Fällen kann der Auftraggeber die Ankündigungsfrist auf 24 Stunden verkürzen; ein dringender Fall liegt insbesondere bei Inspektionen durch Datenschutzaufsichtsbehörden, sonstigen hoheitlichen Aufsichtsbehörden, oder bei eventuell meldepflichtigen Vorfällen vor.
- (5) Der Auftragnehmer stellt sicher, dass der Auftraggeber oder die von ihm beauftragten Prüfer sich von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen können.

§ 16 Pflichten des Auftraggebers

- (1) Der Auftraggeber ist für die Einhaltung der auf ihn anwendbaren gesetzlichen Bestimmungen zum Schutz personenbezogener Daten verantwortlich.
- (2) Der Auftraggeber wird den Auftragnehmer unverzüglich und vollständig informieren, wenn er bei Prüfung der Verarbeitungsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
- (3) Der Auftraggeber benennt einen für die im Rahmen des Vertrages anfallenden Datenschutzfragen zuständigen Ansprechpartner und teilt dessen Kontaktdaten zum Zweck der direkten Kontaktaufnahme mit.

§ 17 Home-Office-Regelung

- (1) Der Auftragnehmer darf seinen Beschäftigten, die mit der Verarbeitung von personenbezogenen Daten für den Auftraggeber beauftragt sind, die Verarbeitung von personenbezogenen Daten in Privatwohnungen („Home-Office“) erlauben.
- (2) Der Auftragnehmer hat sicherzustellen, dass die Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen auch im „Home-Office“ der Beschäftigten des Auftragnehmers gewährleistet ist.
- (3) Der Auftragnehmer trägt insbesondere Sorge dafür, dass bei einer Verarbeitung von personenbezogenen Daten im „Home-Office“ die Speicherorte so konfiguriert werden, dass eine lokale Speicherung von Daten auf IT-Systemen, die im „Home-Office“ verwendet werden, ausgeschlossen ist. Sollte dies nicht möglich sein, hat der Auftragnehmer Sorge dafür zu tragen, dass die lokale Speicherung ausschließlich verschlüsselt erfolgt und andere im Haushalt befindliche Personen keinen Zugriff auf diese Daten erhalten.

§ 18 Sonstige Pflichten und Bestimmungen

- (1) Die Parteien sind sich einig, die vorliegende Vereinbarung einschließlich Anlagen im Fall von Änderungen, Anpassungen und/oder Ergänzungen datenschutzrechtlicher Bestimmungen – insbesondere der DS-GVO und/oder der jeweils anwendbaren nationalen Umsetzungs-gesetze – einvernehmlich und für den Auftraggeber anzupassen und zu ändern.
- (2) Jede Änderung dieser Vereinbarung bedarf zu ihrer Wirksamkeit der Schriftform. Dies gilt auch für einen Verzicht auf das Schriftformerfordernis selbst.
- (3) Es gilt das Recht der Bundesrepublik Deutschland.
- (4) Gerichtsstand für sämtliche Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung und datenschutzrelevanter Streitigkeiten aus Leistungsverträgen ist Leipzig. Dabei steht es dem Auftraggeber frei, etwaige Ansprüche aus dieser Vereinbarung auch bei dem für den Sitz des Auftragnehmers sachlich und örtlich zuständigen Gericht geltend zu machen. Gesetzliche Regelungen über ausschließliche Zuständigkeiten bleiben unberührt.

Anlage 1:

Art der personenbezogenen Daten und Kategorien von Betroffenen

Art der personenbezogenen Daten

Folgende Datenarten / -kategorien sind Gegenstand der Auftragsverarbeitung:

- Personenstammdaten
- Kundenstammdaten
- Anmelde-, Zeit- und Arbeitsdaten der Mitarbeiter im Ticketsystem
- Kommunikationsdaten (z. B. Telefon, E-Mail)
- Alle Daten, die im Rahmen der vom Auftragnehmer bereitgestellten bzw. zu implementierenden bzw. zu wartenden Lösung übertragen werden.
- Kundenhistorie (z. B. bei Reklamationen)
- Vertragsabrechnungs- und Zahlungs- und Bankdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, z. B. Auskunfteien oder aus öffentlichen Verzeichnissen)

-

(vom Auftraggeber zu vervollständigen)

Kategorien betroffener Personen

Folgende Kategorien von Betroffenen sind von der Auftragsverarbeitung betroffen:

- Beschäftigte i.S.d. § 26 Abs. 8 BDSG
- Beauftragte des Auftraggebers
- Kunden und Geschäftsteilnehmer des Auftraggebers

-

(vom Auftraggeber zu vervollständigen)

Anlage 2 zur AVV

Dokumentation

Technische und organisatorische Maßnahmen

Inhaltsverzeichnis

1.	Ziel.....	2
2.	Version	2
3.	Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO).....	2
3.1	Zutrittskontrolle.....	2
3.2	Zugangskontrolle.....	3
3.3	Zugriffskontrolle.....	4
3.4	Trennungskontrolle	5
3.5	Pseudonymisierung	5
4.	Integrität (Art. 32 Abs. 1 lit. b DSGVO)	6
4.1	Weitergabekontrolle	6
4.2	Eingabekontrolle.....	7
5.	Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)	8
5.1	Verfügbarkeitskontrolle.....	8
5.2	Rasche Wiederherstellung (Art. 32 Abs. 1 lit. c) DSGVO).....	9
6.	Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)	10
6.1	Datenschutz-Management.....	10
6.2	Incident-Response-Management.....	10
6.3	Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)	11
6.4	Auftragskontrolle.....	11
7.	Schlussbemerkung	12

1. Ziel

Dokumentation der technisch- organisatorischen Maßnahmen.

2. Version

Version	Stand	Bemerkung
1.0	05.04.2024	

3. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Zutrittskontrolle

Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z. B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen.

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z. B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

<input type="checkbox"/>	Es sind keine Maßnahmen zur Zutrittskontrolle erforderlich, weil ...	
<input type="checkbox"/>	Es existieren keine Maßnahmen zur Zutrittskontrolle.	
<input checked="" type="checkbox"/>	Es existieren folgende Maßnahmen zur Zutrittskontrolle	
	Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/>	Alarmanlage	<input checked="" type="checkbox"/> Schlüsselregelung / Liste
<input type="checkbox"/>	Automatisches Zugangskontrollsystem	<input type="checkbox"/> Empfang / Rezeption / Pförtner
<input type="checkbox"/>	Videouberwachung der Eingänge	<input type="checkbox"/> Besucherbuch / Protokoll der Besucher
<input type="checkbox"/>	Chipkarten / Transpondersysteme	<input type="checkbox"/> Mitarbeiter- / Besucherausweise
<input checked="" type="checkbox"/>	Manuelles Schließsystem	<input checked="" type="checkbox"/> Besucher in Begleitung durch Mitarbeiter
<input checked="" type="checkbox"/>	Sicherheitsschlösser	<input type="checkbox"/> Sorgfalt bei Auswahl des Wachpersonals
<input type="checkbox"/>	Sicherheitsschloss am Serverraum	<input checked="" type="checkbox"/> Sorgfalt bei Auswahl Reinigungsdienste
<input type="checkbox"/>	Schließsystem mit Codesperre	
<input type="checkbox"/>	Absicherung der Gebäudeschächte	
<input checked="" type="checkbox"/>	Klingelanlage mit Kamera	
<input type="checkbox"/>	Klingelanlage ohne Kamera	
<input type="checkbox"/>	Serverräume sind nur durch bestimmte Schlüssel zu betreten	
<input checked="" type="checkbox"/>	Es existieren zusätzliche folgende Maßnahmen zur Zutrittskontrolle	
	<ul style="list-style-type: none"> ▪ Türsicherung (elektronischer Türöffner, etc.) 	

3.2 Zugangskontrolle

Zugangskontrolle

Keine unbefugte Systembenutzung, z. B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern.

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z. B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

<input type="checkbox"/>	Es sind keine Maßnahmen zur Zugangskontrolle erforderlich, weil ...	
<input type="checkbox"/>	Es existieren keine Maßnahmen zur Zugangskontrolle.	
<input checked="" type="checkbox"/>	Es existieren folgende Maßnahmen zur Zugangskontrolle	
	Technische Maßnahmen	Organisatorische Maßnahmen

<input checked="" type="checkbox"/>	Login mit Benutzername + Passwort	<input checked="" type="checkbox"/>	Verwalten von Benutzerberechtigungen
<input checked="" type="checkbox"/>	Login mit biometrischen Daten	<input checked="" type="checkbox"/>	Erstellen von Benutzerprofilen
<input checked="" type="checkbox"/>	Anti-Viren-Software Server	<input checked="" type="checkbox"/>	Zentrale Passwortvergabe
<input checked="" type="checkbox"/>	Anti-Virus-Software Clients	<input checked="" type="checkbox"/>	Richtlinie „Sicheres Passwort“
<input type="checkbox"/>	Anti-Virus-Software mobile Geräte	<input type="checkbox"/>	Richtlinie „Löschen / Vernichten“
<input checked="" type="checkbox"/>	Firewall	<input type="checkbox"/>	Richtlinie „Clean Desk“
<input type="checkbox"/>	Intrusion Detection Systeme	<input checked="" type="checkbox"/>	Allg. Richtlinie Datenschutz/Sicherheit
<input type="checkbox"/>	Mobile Device Management	<input type="checkbox"/>	Mobile Device Policy
<input checked="" type="checkbox"/>	Einsatz VPN bei Remote-Zugriffen	<input type="checkbox"/>	Anleitung „Manuelle Desktopsperre“
<input checked="" type="checkbox"/>	Verschlüsselung von Datenträgern		
<input checked="" type="checkbox"/>	Verschlüsselung Smartphones		
<input type="checkbox"/>	Gehäuseverriegelung		
<input type="checkbox"/>	BIOS Schutz (separates Passwort)		
<input type="checkbox"/>	Sperre externer Schnittstellen (USB)		
<input checked="" type="checkbox"/>	Automatische Desktopsperre		
<input checked="" type="checkbox"/>	Verschlüsselung von Notebooks/Tablet		
<input checked="" type="checkbox"/>	Es existieren zusätzliche folgende Maßnahmen zur Zugangskontrolle		
	<ul style="list-style-type: none"> ▪ Protokollierung der Anmeldeversuche und Abbruch des Anmeldevorgangs nach festgelegter Zahl von erfolglosen Versuchen ▪ Abkapselung von sensiblen Systemen durch getrennte Netzbereiche 		

3.3 Zugriffskontrolle

Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z. B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z. B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

- Es sind keine Maßnahmen zur Zugriffskontrolle erforderlich, weil ...
- Es existieren keine Maßnahmen zur Zugriffskontrolle.

<input checked="" type="checkbox"/>	Es existieren folgende Maßnahmen zur Zugriffskontrolle			
	Technische Maßnahmen		Organisatorische Maßnahmen	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Aktenschredder	<input checked="" type="checkbox"/>	Einsatz Berechtigungskonzepte
<input type="checkbox"/>	<input type="checkbox"/>	Externer Aktenvernichter (DIN 66399)	<input checked="" type="checkbox"/>	Minimale Anzahl an Administratoren
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Physische Löschung von Datenträgern	<input type="checkbox"/>	Datenschutztresor
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	<input checked="" type="checkbox"/>	Verwaltung Benutzerrechte
<input type="checkbox"/>	Es existieren zusätzliche folgende Maßnahmen zur Zugriffskontrolle			
	<ul style="list-style-type: none"> ▪ 			

3.4 Trennungskontrolle

Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z. B. Mandantenfähigkeit, Sandboxing.

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

<input type="checkbox"/>	Es sind keine Maßnahmen zur Trennungskontrolle erforderlich, weil ...			
<input type="checkbox"/>	Es existieren keine Maßnahmen zur Trennungskontrolle.			
<input checked="" type="checkbox"/>	Es existieren folgende Maßnahmen zur Trennungskontrolle			
	Technische Maßnahmen		Organisatorische Maßnahmen	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Trennung von Produktiv- und Testumgebung	<input checked="" type="checkbox"/>	Steuerung über Berechtigungskonzept
<input type="checkbox"/>	<input type="checkbox"/>	Physikalische Trennung (Systeme / Datenbanken / Datenträger)	<input checked="" type="checkbox"/>	Festlegung von Datenbankrechten
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Mandantenfähigkeit relevanter Anwendungen		
<input checked="" type="checkbox"/>	Es existieren zusätzliche folgende Maßnahmen zur Trennungskontrolle			
	<ul style="list-style-type: none"> ▪ Verschlüsselte Speicherung von personenbezogenen Daten 			

3.5 Pseudonymisierung

Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

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.

<input type="checkbox"/>	Es sind keine Maßnahmen zur Pseudonymisierung erforderlich, weil ...			
<input type="checkbox"/>	Es existieren keine Maßnahmen zur Pseudonymisierung.			

<input checked="" type="checkbox"/>	Es existieren folgende Maßnahmen zur Pseudonymisierung			
	Technische Maßnahmen		Organisatorische Maßnahmen	
	<input checked="" type="checkbox"/>	Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrennten und abgesicherten System (mögl. verschlüsselt)	<input checked="" type="checkbox"/>	Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu pseudonymisieren
<input checked="" type="checkbox"/>	Es existieren zusätzliche folgende Maßnahmen zur Pseudonymisierung			
	<ul style="list-style-type: none"> ▪ Hashwertverfahren (SHA-2; SHA-3) 			

4. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

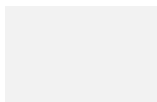
4.1 Weitergabekontrolle

Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z. B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen

Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z. B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

<input type="checkbox"/>	Es sind keine Maßnahmen zur Weitergabekontrolle erforderlich, weil ...			
<input type="checkbox"/>	Es existieren keine Maßnahmen zur Weitergabekontrolle.			
<input checked="" type="checkbox"/>	Es existieren folgende Maßnahmen zur Weitergabekontrolle			
	Technische Maßnahmen		Organisatorische Maßnahmen	
	<input checked="" type="checkbox"/>	E-Mail-Verschlüsselung	<input type="checkbox"/>	Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
	<input checked="" type="checkbox"/>	Einsatz von VPN	<input type="checkbox"/>	Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
	<input checked="" type="checkbox"/>	Protokollierung der Zugriffe und Abrufe	<input type="checkbox"/>	Datensätze sind mit Zweckattributen versehen
	<input type="checkbox"/>	Sichere Transportbehälter	<input checked="" type="checkbox"/>	Weitergabe in anonymisierter oder pseudonymisierter Form
	<input checked="" type="checkbox"/>	Bereitstellung über verschlüsselte Verbindungen wie sftp, https	<input checked="" type="checkbox"/>	Sorgfalt bei Auswahl von Transport- Personal und Fahrzeugen
	<input type="checkbox"/>	Nutzung von Signaturverfahren	<input type="checkbox"/>	Persönliche Übergabe mit Protokoll
<input checked="" type="checkbox"/>	Es existieren zusätzliche folgende Maßnahmen zur Weitergabekontrolle			
	<ul style="list-style-type: none"> ▪ Transportprozesse mit individueller Verantwortlichkeit 			



- Verschlüsselungsverfahren, die Datenveränderungen während des Transports aufdecken
- Sicherer Transportbehälter für Datenträger

4.2 Eingabekontrolle

Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z. B.: Protokollierung, Dokumentenmanagement.

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z. B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Es sind keine Maßnahmen zur Eingabekontrolle erforderlich, weil ...

Es existieren keine Maßnahmen zur Eingabekontrolle.

Es existieren folgende Maßnahmen zur Eingabekontrolle

Technische Maßnahmen		Organisatorische Maßnahmen	
<input checked="" type="checkbox"/>	Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	<input type="checkbox"/>	Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
<input checked="" type="checkbox"/>	Manuelle oder automatisierte Kontrolle der Protokolle	<input checked="" type="checkbox"/>	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
		<input checked="" type="checkbox"/>	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
		<input type="checkbox"/>	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
		<input type="checkbox"/>	Klare Zuständigkeiten für Löschungen

Es existieren zusätzliche folgende Maßnahmen zur Eingabekontrolle

-

5. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

5.1 Verfügbarkeitskontrolle

Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z. B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlage, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidssysteme, Plattenspiegelungen etc.

Es sind keine Maßnahmen zur Verfügbarkeitskontrolle erforderlich, weil ...

Es existieren keine Maßnahmen zur Verfügbarkeitskontrolle.

Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle

Technische Maßnahmen		Organisatorische Maßnahmen	
<input type="checkbox"/>	Feuer- und Rauchmeldeanlagen	<input checked="" type="checkbox"/>	Backup & Recovery-Konzept (ausformuliert)
<input type="checkbox"/>	Feuerlöscher Serverraum	<input checked="" type="checkbox"/>	Kontrolle des Sicherungsvorgangs
<input type="checkbox"/>	Serverraumüberwachung Temperatur und Feuchtigkeit	<input checked="" type="checkbox"/>	Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
<input type="checkbox"/>	Serverraum klimatisiert	<input type="checkbox"/>	Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
<input checked="" type="checkbox"/>	USV	<input checked="" type="checkbox"/>	Keine sanitären Anschlüsse im oder oberhalb des Serverraums
<input type="checkbox"/>	Schutzsteckdosenleisten Serverraum	<input checked="" type="checkbox"/>	Existenz eines Notfallplans (z. B. BSI IT Grundschutz 100-4)
<input type="checkbox"/>	Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.)	<input checked="" type="checkbox"/>	Getrennte Partitionen* für Betriebssysteme und Daten
<input type="checkbox"/>	RAID System / Festplattenspiegelung		
<input type="checkbox"/>	Videoüberwachung Serverraum		
<input type="checkbox"/>	Alarmmeldung bei unberechtigtem Zutritt zu Serverraum		

Es existieren zusätzliche folgende Maßnahmen zur Verfügbarkeitskontrolle

5.2 Rasche Wiederherstellung (Art. 32 Abs. 1 lit. c) DSGVO)

Rasche Wiederherstellung (Art. 32 Abs. 1 lit. c) DSGVO

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z. B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne

Es sind keine Maßnahmen zur raschen Wiederherstellung erforderlich, weil ...

Es existieren keine Maßnahmen zur raschen Wiederherstellung.

Es existieren folgende Maßnahmen zur raschen Wiederherstellung

Technische Maßnahmen

Organisatorische Maßnahmen

Bereitstellung des Server Systemdienstes VSS (Volume Shadow Copy Service) um gelöschte Daten auf dem Fileserver zeitnah wiederherzustellen

Backupkonzept mit Datenvorhaltung vor Ort und redundant an einem weiteren Standort

Notfallhandbuch

Es existieren zusätzliche folgende Maßnahmen zur raschen Wiederherstellung

▪

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

6.1 Datenschutz-Management

Datenschutz-Management			
<input type="checkbox"/>	Es sind keine Maßnahmen zum Datenschutzmanagement erforderlich, weil ...		
<input type="checkbox"/>	Es existieren keine Maßnahmen zum Datenschutzmanagement		
<input checked="" type="checkbox"/>	Es existieren folgende Maßnahmen zum Datenschutzmanagement		
	Technische Maßnahmen		Organisatorische Maßnahmen
<input type="checkbox"/>	Software-Lösungen für Datenschutz-Management im Einsatz	<input checked="" type="checkbox"/>	externer Datenschutzbeauftragter
<input checked="" type="checkbox"/>	Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z. B. Wiki, Intranet ...)	<input checked="" type="checkbox"/>	Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
<input type="checkbox"/>	Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12	<input checked="" type="checkbox"/>	Regelmäßige Sensibilisierung der Mitarbeiter, mindestens jährlich
<input type="checkbox"/>	Anderweitiges dokumentiertes Sicherheitskonzept	<input checked="" type="checkbox"/>	Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
<input checked="" type="checkbox"/>	Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	<input checked="" type="checkbox"/>	Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
		<input checked="" type="checkbox"/>	Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
<input type="checkbox"/>	Es existieren zusätzliche folgende Maßnahmen zum Datenschutzmanagement		
	▪		

6.2 Incident-Response-Management

Incident-Response-Management			
<input type="checkbox"/>	Es sind keine Maßnahmen zum Incident-Response-Management erforderlich, weil ...		
<input type="checkbox"/>	Es existieren keine Maßnahmen zum Incident-Response-Management.		
<input checked="" type="checkbox"/>	Es existieren folgende Maßnahmen zum Incident-Response-Management		
	Technische Maßnahmen		Organisatorische Maßnahmen
<input checked="" type="checkbox"/>	Einsatz von Firewall und regelmäßige Aktualisierung	<input type="checkbox"/>	Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
<input checked="" type="checkbox"/>	Einsatz von Spamfilter und regelmäßige Aktualisierung	<input type="checkbox"/>	Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
<input checked="" type="checkbox"/>	Einsatz von Virens Scanner und regelmäßige Aktualisierung	<input checked="" type="checkbox"/>	Einbindung von <input checked="" type="checkbox"/> DSB und <input checked="" type="checkbox"/> ISB in

				Sicherheitsvorfälle und Datenpannen
	<input type="checkbox"/>	Intrusion Detection System (IDS)	<input type="checkbox"/>	Dokumentation von Sicherheitsvorfällen und Datenpannen z. B. via Ticketsystem
	<input type="checkbox"/>	Intrusion Prevention System (IPS)	<input checked="" type="checkbox"/>	Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen
<input type="checkbox"/>	Es existieren zusätzliche folgende Maßnahmen zum Incident-Response-Management			
	▪			

6.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Datenschutzfreundliche Voreinstellung				
<input type="checkbox"/>	Es sind keine Maßnahmen zur Datenschutzfreundliche Voreinstellung erforderlich, weil ...			
<input type="checkbox"/>	Es existieren keine Maßnahmen zur Datenschutzfreundliche Voreinstellung.			
<input checked="" type="checkbox"/>	Es existieren folgende Maßnahmen zur Datenschutzfreundliche Voreinstellung			
	Technische Maßnahmen		Organisatorische Maßnahmen	
	<input checked="" type="checkbox"/>	Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen	<input checked="" type="checkbox"/>	Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
<input type="checkbox"/>	Es existieren zusätzliche folgende Maßnahmen zur Datenschutzfreundliche Voreinstellung			
	▪			

6.4 Auftragskontrolle

Auftragskontrolle				
Keine Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z. B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.				
Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.				
<input type="checkbox"/>	Es sind keine Maßnahmen zur Auftragskontrolle erforderlich, weil ...			
<input type="checkbox"/>	Es existieren keine Maßnahmen zur Auftragskontrolle.			
<input checked="" type="checkbox"/>	Es existieren folgende Maßnahmen zur Auftragskontrolle			
	Technische Maßnahmen		Organisatorische Maßnahmen	
	<input type="checkbox"/>		<input checked="" type="checkbox"/>	Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	<input type="checkbox"/>		<input checked="" type="checkbox"/>	Auswahl des Auftragnehmers unter

<input type="checkbox"/>		<input checked="" type="checkbox"/>	Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit
<input type="checkbox"/>		<input checked="" type="checkbox"/>	Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard Vertragsklauseln
<input type="checkbox"/>		<input checked="" type="checkbox"/>	Schriftliche Weisungen an den Auftragnehmer
<input type="checkbox"/>		<input checked="" type="checkbox"/>	Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
<input type="checkbox"/>		<input checked="" type="checkbox"/>	Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
<input type="checkbox"/>		<input checked="" type="checkbox"/>	Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
<input type="checkbox"/>		<input checked="" type="checkbox"/>	Regelung zum Einsatz weiterer Subunternehmer
<input type="checkbox"/>		<input checked="" type="checkbox"/>	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
<input type="checkbox"/>		<input checked="" type="checkbox"/>	Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus
<input type="checkbox"/>	Es existieren zusätzliche folgende Maßnahmen zur Auftragskontrolle		
	▪		

7. Schlussbemerkung

Ich versichere, dass ich die vorstehenden Angaben wahrheitsgemäß nach bestem Wissen und Gewissen gemacht habe.

Datum, Unterschrift

Kontakt:
ics cloud services GmbH
Möckernsche Str. 3
04155 Leipzig
E-Mail: kontakt@ics-cloud.services
www.ics-cloud.services

Anlage 3 zur AVV: Unterauftragnehmer

Folgende Unterauftragnehmer sind mit Zustimmung des Auftraggebers tätig:

- Unternehmen:** IONOS SE
Elgendorfer Straße 57
56410 Montabaur
Amtsgericht Montabaur / HRB 24498
- Zweck:** Hosting der Projektmanagement-, ERP- und CRM-Plattformen der ics cloud services GmbH, Cloud-Plattform für Entwicklungs-, Test- und Produktivsysteme von und für Kunden der ics cloud services GmbH, sofern dies Bestandteil der vereinbarten Leistungserbringung für den Kunden ist
-
- Unternehmen:** STRATO GmbH, Otto-Ostrowski-Straße 7
10249 Berlin,
Registergericht Berlin-Charlottenburg, HRB 270570 B
- Zweck:** Hosting der Projektmanagement-, ERP- und CRM-Plattformen der ics cloud services GmbH, Cloud-Plattform für Entwicklungs-, Test- und Produktivsysteme von und für Kunden der ics cloud services GmbH, sofern dies Bestandteil der vereinbarten Leistungserbringung für den Kunden ist
-
- Unternehmen:** ic-solution GmbH
Möckernsche Str. 3
04155 Leipzig
Amtsgericht Leipzig HRB 26422
- Zweck:** Erbringung von Dienstleistungen zur Einrichtung und Anpassung von kundenspezifischen Anforderungen, Customizing der Systeme und Softwareentwicklungen, die dem Auftraggeber bereitgestellt werden.

Für Auftraggeber, für die wir die Software des Herstellers **ABBYY** (unter anderem „Flexi-Capture“, „Finereader“, „Vantage“) einsetzen:

Unternehmen: ABBYY Europe GmbH, Friedensstr. 22b, 81671 München
Amtsgericht München, HRB 131467

Zweck: 2nd-Level-Support bei Softwarefehlern

Für Auftraggeber, für die wir die Software des Herstellers des Herstellers **Tungsten Automation Deutschland GmbH (ehemals KOFAX)** (unter anderem „Tungsten Capture“, „Total Agility“) einsetzen:

Unternehmen: Tungsten Automation Deutschland GmbH, Engelbergerstr.
19, 79106 Freiburg
Amtsgericht Freiburg HRB 725671

Zweck: 2nd-Level-Support bei Softwarefehlern

Für Auftraggeber, für die wir die Software der **ic-solution Gruppe** (unter anderem „SPICE“, „LAERA“) einsetzen:

Unternehmen: Skilja GmbH,
Kartäuserstraße 49
79102 Freiburg
Amtsgericht Freiburg, HRB 707966

Zweck: 2nd-Level-Support bei Softwarefehlern

Anlage 4: Anonymisiertes Training

Vorbemerkung:

Im Zuge der technologischen Weiterentwicklung ermöglichen KI-gestützte Systeme die gemeinschaftliche Nutzung von Trainings- bzw. Lernmengen (nachfolgend „Lernmenge“ genannt) in Klassifikations- und Extraktionsprojekten.

Hierzu werden Dokumente, E-Mails oder sonstige Transaktionen (nachfolgend „Transaktionen“ genannt) des Auftraggebers dem Auftragnehmer übermittelt, damit dieser in Dienstleistung eine zentrale Lernmenge trainiert.

Als Ergebnis ist diese Lernmenge in der Lage, dann auch neue unbekannte Transaktionen des Auftraggebers besser zu erkennen und mit höherer Präzision zu verarbeiten.

Die hierbei vom Auftragnehmer erstellte Lernmenge wird softwareseitig um kundenspezifische Informationen bereinigt. Dies umfasst üblicherweise personenbezogene Daten oder Wirtschaftsdaten wie Einkaufspreise etc.

Um alle Auftraggeber kollektiv an dieser Leistung teilhaben zu lassen, und auch, um ihn von individuellen Trainingskosten zu befreien, stellt der Auftragnehmer auch anderen Auftraggebern diese Lernmenge zur Verfügung.

Mit dieser Anlage, welche gesondert freizugeben ist, erteilt der Auftraggeber die Freigabe, die Transaktionen mit den darin enthaltenen Daten zu verarbeiten.

Abhängigkeit zum Auftragsverarbeitungsvertrag:

Diese Anlage wird auf Grundlage eines Auftragsverarbeitungsvertrags (nachfolgend „AVV“ genannt) erteilt. Die Freigabe der Datennutzung sowie der Nutzung der Lernmenge gilt jedoch auch weiter, wenn die AVV beendet wird. Wird die AVV beendet und diese Anlage nicht gekündigt und keine gesonderte Regelung getroffen, tritt sie stillschweigend an Stelle eines eigenständigen Vertrags auf Basis der AGB des Auftragnehmers.

Art- und Umfang der zu verarbeitenden Daten:

Die Freigabe umfasst alle Daten, die im System des Kunden oder auf den Systemen des Auftraggebers mit der vertragsgegenständlichen Softwarelösung verarbeitet werden oder die der Softwarelösung (nachfolgend „Lösung“ genannt) zur Verfügung gestellt werden. Da der Auftragnehmer keinen Einfluss auf die ihm überlassenen Transaktionen und Daten hat, gilt die Freigabe auf die Art der Daten ohne Einschränkung auf Personen- oder Datenkreise auch dann, wenn in einem geltenden Auftragsverarbeitungsvertrag ggfs. eine Einschränkung vereinbart wurde.

Als vertragsgegenständliche Lösung gelten die Lösungen, die im Kauf-, Miet- oder Nutzungsvertrag benannt sind, und für die in diesen Verträgen das anonymisierte Training als Vertragsbestandteil ausgewiesen ist. Die Nutzung von marketingtechnischen Namen für diese Leistung ist zulässig.

Zurverfügungstellung:

Die Gewährung der Transaktionen und damit verbundenen Daten erfolgt bei vom Auftraggeber betriebenen Lösungen durch regelmäßige Übermittlung, für die er die notwendigen Systemvoraussetzungen gemäß Weisung des Auftragnehmers schafft. Der Auftragnehmer übermittelt die Lernmengen wiederum ebenfalls regelmäßig über den gleichen Weg.

Bei vom Auftragnehmer für den Auftraggeber betriebenen Lösungen auf den Systemen des Auftragnehmers sorgt der Auftragnehmer für die Übermittlung von Transaktionen, Daten und Lernmengen.

Zeitraum der Datennutzung:

Der Auftraggeber erteilt dem Auftragnehmer das Recht, die Daten zur Erstellung dieser Lernmenge zu nutzen. Es beginnt mit der Unterzeichnung dieser Anlage. Da die Ergebnisse des Trainings unwiderruflich in die Lernmenge einfließen, ist das Nutzungsrecht für die Daten der Transaktionen, die der Auftragnehmer erhalten hat, unbefristet und unwiderruflich.

Kündigung:

Die Auftragsverarbeitung infolge dieser Anlage kann von beiden Seiten mit einer Frist von 3 Monaten zum Ende eines Kalenderjahres gekündigt werden. Sie beendet das Recht der Nutzung der Transaktionen zur Verbesserung der Lernmenge zum Vertragsende. Der Auftraggeber wiederum verpflichtet sich, die erhaltene Lernmenge aus seinem System auf seine Kosten zum Vertragsende zu entfernen und nicht weiter zu nutzen. Auf die Einhaltung des Datenschutzes gemäß DSGVO wird an dieser Stelle nochmals hingewiesen.

Datenschutz:

In Bezug auf Datenschutz gelten die Bestimmungen einer geltenden AVV. Der Auftragnehmer sichert zu, mit größter Sorgfalt die Bestimmungen der AVV einzuhalten und die erhaltenen Transaktionen softwarebasiert automatisch zu anonymisieren. Die erhaltenen Transaktionen an sich werden zudem nur zum Zeitpunkt des Lernens verarbeitet und nicht dauerhaft gespeichert. Da der Wesenszweck dieser Vereinbarung jedoch der anonymisierte Austausch der Lernmenge innerhalb eines Kundenkreises ist, wird die Lernmenge auch Dritten zum Zwecke der verbesserten Nutzung der Klassifikation und Extraktion von Daten zur Verfügung gestellt. Diesem Austausch stimmt der Auftraggeber zu.

Unterauftragnehmer:

Der Auftragnehmer hat das Recht, den in einer geltenden AVV benannten Unterauftragnehmern sowohl Transaktionen als auch Daten zum Zwecke der Verbesserung der Lernmenge zu überlassen, sofern er diesen die sinngemäßen Bestimmungen der AVV ebenfalls auferlegt. Dieses Recht und die Liste der Unterauftragnehmer behalten auch Gültigkeit, falls die AVV beendet wurde, sofern nichts Abweichendes vereinbart wird.

Haftung, Verjährung von Ansprüchen:

Soweit sich aus dieser Anlage zur AVV, der AVV selbst und dem Auftragsverarbeitungsvertrag nebst aller Anlagen bzw. Vertragsbestandteile sowie der nachfolgenden Bestimmungen nichts

anderes ergibt, haftet der Auftragnehmer bei einer Verletzung von vertraglichen und außervertraglichen Pflichten nach den einschlägigen gesetzlichen Vorschriften.

Auf Schadensersatz haftet der Auftragnehmer – gleich aus welchem Rechtsgrund – bei Vorsatz und grober Fahrlässigkeit. Bei einfacher Fahrlässigkeit haftet der Auftragnehmer nur

- für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit,
- für Schäden aus der Verletzung einer wesentlichen Vertragspflicht (Verpflichtung, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung der Vertragspartner regelmäßig vertraut und vertrauen darf); in diesem Fall ist die Haftung des Auftragnehmers jedoch auf den Ersatz des vorhersehbaren, typischerweise eintretenden Schadens begrenzt.

Dies gilt auch für eine versehentliche ungeplante und/oder unzulässige Weiterreichung von in der Lernmenge enthaltenen Daten.

Die sich aus vorstehendem Absatz ergebenden Haftungsbeschränkungen gelten nicht, soweit der Auftragnehmer einen Mangel arglistig verschwiegen oder eine Garantie für die Funktionsfähigkeit oder Mangelfreiheit übernommen hat. Das gleiche gilt für Ansprüche des Auftraggebers nach dem Produkthaftungsgesetz oder etwaigen sonstigen Rechtsgrundlagen, die eine verschuldensunabhängige Haftung vorsehen.

Gewährleistungsrechtliche Ansprüche des Auftraggebers hinsichtlich unserer Leistungen verjähren innerhalb eines Jahres ab Leistungserbringung. Dies gilt nicht, wenn der Auftragnehmer eine längerfristige Garantie für die Funktionsfähigkeit oder Mangelfreiheit übernommen hat, es sich um einen Mangel handelt, der vom Auftragnehmer arglistig verschwiegen wurde, oder um solche wegen der Verletzung des Lebens, des Körpers oder der Gesundheit handelt. Insofern gelten die gesetzlichen Verjährungsfristen.

Salvatorische Klausel:

Sollten eine oder mehrere Bestimmungen dieser Vereinbarung ganz oder teilweise rechtsunwirksam sein oder werden, oder eine Lücke aufweisen, verpflichten sich die Parteien eine Regelung zu treffen, die dem entspricht, was die Parteien wirtschaftlich gewollt haben. Die Gültigkeit der übrigen geltenden Bestimmungen wird hierdurch nicht berührt.