



Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

zwischen

dem jeweiligen Kunden der DICIS AG, der die Leistungen der DICIS AG in Anspruch nimmt
(nachfolgend „Auftraggeber“ oder „Verantwortlicher“)

und

DICIS AG, Gerichtsweg 28, 04103 Leipzig, vertreten durch den Vorstand (nachfolgend „DICIS“ oder
„Auftragsverarbeiter“), Amtsgericht Leipzig HRB 38455

– gemeinsam auch „Parteien“ –

wird folgende Vereinbarung zur Auftragsverarbeitung geschlossen.

Präambel

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten durch DICIS im Auftrag des Auftraggebers. Sie gilt für alle Leistungen, bei deren Erbringung DICIS personenbezogene Daten im Auftrag des Auftraggebers verarbeitet.

Diese Vereinbarung ist Bestandteil der zwischen den Parteien geschlossenen Vereinbarung zur Zertifizierung von Managementsystemen (festgehalten im bestätigten Angebot mit Bezug auf die ABG). Soweit diese Vereinbarung wirksam in die Allgemeinen Geschäftsbedingungen oder den elektronischen Bestell- oder Registrierungsprozess von DICIS einbezogen wird, kommt sie mit Annahme der entsprechenden Vertragsbedingungen zustande.

Eine gesonderte Unterschrift ist nicht erforderlich, soweit die gesetzlichen Voraussetzungen für den Abschluss in elektronischer Form erfüllt sind.

§ 1 Gegenstand, Dauer, Art und Zweck der Verarbeitung

(1) DICIS verarbeitet personenbezogene Daten im Auftrag des Auftraggebers ausschließlich zur Erbringung der im Hauptvertrag vereinbarten Leistungen. Gegenstand der Verarbeitung ist insbesondere die Bereitstellung, der Betrieb, die Wartung, die Sicherung und der Support der von DICIS angebotenen Software und der damit verbundenen Funktionen.

(2) Die Dauer der Verarbeitung entspricht grundsätzlich der Laufzeit des Hauptvertrags. Einzelne Verarbeitungsvorgänge können darüber hinaus fortbestehen, soweit gesetzliche Aufbewahrungspflichten bestehen oder Daten in technisch erforderlichen Sicherungskopien bis zu deren turnusmäßiger Löschung enthalten sind.

(3) Art der Verarbeitung kann – abhängig von der Nutzung durch den Auftraggeber – insbesondere das Erheben, Erfassen, Ordnen, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Übermitteln, Bereitstellen, Abgleichen, Verknüpfen, Einschränken, Löschen und Vernichten personenbezogener Daten umfassen.

(4) Zweck der Verarbeitung ist die vertragsgemäße Bereitstellung des Zertifizierungstools einschließlich Benutzerverwaltung, Authentifizierung, Speicherung und Verarbeitung von vom Auftraggeber eingestellten Inhalten, Dokumentation, Auswertung, Support, Fehlerbehebung, Systemsicherheit, Datensicherung und Wiederherstellung.

(5) DICIS verarbeitet die personenbezogenen Daten nicht für eigene, mit den Zwecken des Auftraggebers unvereinbare Zwecke. Gesetzlich vorgeschriebene Verarbeitungen bleiben unberührt; DICIS informiert den Auftraggeber hierüber vor der Verarbeitung, soweit das betreffende Recht eine solche Information nicht aus wichtigen Gründen des öffentlichen Interesses verbietet.

§ 2 Kategorien betroffener Personen und Arten personenbezogener Daten

(1) Abhängig von der konkreten Nutzung der Leistungen können insbesondere folgende Kategorien betroffener Personen von der Verarbeitung umfasst sein:

- Beschäftigte, freie Mitarbeitende und sonstige für den Auftraggeber tätige Personen;
- Administratoren, Super User und sonstige registrierte Nutzer der Plattform;
- Geschäftsführer, Organmitglieder und Ansprechpartner des Auftraggebers;
- Kunden, Interessenten und Ansprechpartner von Kunden des Auftraggebers;
- Lieferanten, Dienstleister, Geschäftspartner und deren Ansprechpartner;
- sonstige betroffene Personen, deren personenbezogene Daten der Auftraggeber oder dessen Nutzer in die Software eingeben, hochladen, erzeugen oder anderweitig verarbeiten.

(2) Abhängig von der konkreten Nutzung können insbesondere folgende Datenkategorien verarbeitet werden:

- Stammdaten, insbesondere Name, Vorname, Benutzername, Funktion und organisatorische Zuordnung;
- Kontaktdaten, insbesondere E-Mail-Adresse, Telefonnummer und geschäftliche Kontaktdaten;
- Benutzer- und Authentifizierungsdaten einschließlich technisch gesicherter Authentifizierungsinformationen;

- Zugriffs-, Protokoll-, Nutzungs- und Verbindungsdaten, insbesondere Zeitpunkte von An- und Abmeldungen, IP-Adressen und technische Logdaten;
- Kommunikationsdaten;
- Dokumente, Dateien, Freitexte, Kommentare, Bewertungen, Maßnahmen, Nachweise und sonstige vom Auftraggeber oder dessen Nutzern bereitgestellte oder erzeugte Inhaltsdaten;
- organisations- und prozessbezogene Daten, soweit sie einen Personenbezug aufweisen;
- sonstige personenbezogene Daten, die der Auftraggeber im Rahmen der vertragsgemäßen Nutzung der Software verarbeitet.

(3) Der Auftraggeber entscheidet, welche personenbezogenen Daten er im Rahmen der Nutzung der Leistungen verarbeitet. DICIS hat grundsätzlich keinen Einfluss darauf, welche Inhalte der Auftraggeber in frei nutzbare Eingabe-, Upload- oder Dokumentationsfelder einstellt.

(4) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO ist nur zulässig, soweit dies vom Leistungsumfang gedeckt ist und der Auftraggeber die hierfür erforderlichen datenschutzrechtlichen Voraussetzungen sicherstellt.

§ 3 Weisungsgebundene Verarbeitung

(1) DICIS verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, soweit DICIS nicht durch das Recht der Europäischen Union oder eines Mitgliedstaats zu einer Verarbeitung verpflichtet ist.

(2) Die im Hauptvertrag und in dieser Vereinbarung festgelegten Leistungen gelten als dokumentierte Weisungen des Auftraggebers. Einzelweisungen können vom Auftraggeber in Textform, insbesondere per E-Mail oder über hierfür bereitgestellte elektronische Kommunikationswege, erteilt werden.

(3) DICIS informiert den Auftraggeber unverzüglich, wenn DICIS der Auffassung ist, dass eine Weisung gegen die DSGVO oder andere Datenschutzbestimmungen der Europäischen Union oder der Mitgliedstaaten verstößt. DICIS ist berechtigt, die Durchführung der betreffenden Weisung auszusetzen, bis sie vom Auftraggeber bestätigt, geändert oder zurückgenommen wurde.

(4) Änderungen des Verarbeitungsgegenstands oder wesentliche Verfahrensänderungen werden zwischen den Parteien abgestimmt und dokumentiert.

§ 4 Vertraulichkeit und Geheimhaltung

(1) DICIS verpflichtet sich, sämtliche Informationen, Unterlagen, Daten und sonstigen Inhalte, die DICIS oder ihren Beschäftigten im Zusammenhang mit der Anbahnung, Durchführung oder Betreuung der Geschäftsbeziehung vom Auftraggeber zugänglich gemacht oder bekannt werden, die nach ihrer Art oder den Umständen ihrer Offenlegung als vertraulich anzusehen sind, vertraulich zu behandeln. Dies gilt unabhängig davon, ob es sich um personenbezogene Daten handelt.

(2) Die Verpflichtung zur Vertraulichkeit gilt insbesondere für Informationen, die der Auftraggeber Beschäftigten oder sonstigen für DICIS tätigen Personen im Rahmen von Vertriebsgesprächen, Beratung, Implementierung, Customer Support, Kundenbetreuung, Vorbereitung und Durchführung von Audits sowie sonstigen Leistungen zur Verfügung stellt oder offenlegt. Hierzu zählen insbesondere Geschäfts- und Betriebsinformationen, interne Prozesse und Verfahren, Dokumentationen, Managementsystemunterlagen, Auditnachweise, technische Informationen, Sicherheitsinformationen, Zugangsdaten, Vertrags- und Kundendaten sowie sonstige nicht öffentlich bekannte Informationen des Auftraggebers.

(3) DICIS verwendet vertrauliche Informationen ausschließlich zur Anbahnung, Durchführung und Erfüllung der Geschäftsbeziehung sowie zur Erbringung der vereinbarten Leistungen. Eine Verwendung für andere Zwecke ist ohne vorherige Zustimmung des Auftraggebers nicht zulässig.

(4) DICIS gibt vertrauliche Informationen ohne vorherige Zustimmung des Auftraggebers nicht an außenstehende Dritte weiter. Innerhalb von DICIS sowie gegenüber von DICIS zur Leistungserbringung eingesetzten Personen dürfen vertrauliche Informationen nur solchen Personen zugänglich gemacht werden, die diese Informationen zur Erfüllung ihrer jeweiligen Aufgaben benötigen. DICIS stellt sicher, dass diese Personen zur Vertraulichkeit verpflichtet sind oder einer entsprechenden gesetzlichen oder berufsrechtlichen Verschwiegenheitspflicht unterliegen.

(5) Soweit DICIS personenbezogene Daten im Auftrag des Auftraggebers verarbeitet, stellt DICIS sicher, dass Personen, die zur Verarbeitung dieser Daten befugt sind, sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Der Zugriff auf personenbezogene Daten wird auf diejenigen Personen beschränkt, die diesen zur Erfüllung ihrer jeweiligen Aufgaben benötigen.

(6) Nicht als vertrauliche Informationen im Sinne dieser Vereinbarung gelten die Tatsache der erfolgten Zertifizierung des Auftraggebers, die Bezeichnung der jeweils zertifizierten Norm oder Normen sowie die Laufzeit und Gültigkeitsdauer des jeweiligen Zertifikats. DICIS ist berechtigt, diese Angaben zum Zweck der Transparenz und Überprüfbarkeit von Zertifizierungen in ihrer öffentlich zugänglichen Zertifikatsdatenbank zu veröffentlichen und für die Dauer der Zertifizierung sowie im erforderlichen Umfang darüber hinaus vorzuhalten.

(7) Von der Verpflichtung zur Vertraulichkeit ausgenommen sind weiterhin Informationen, die

a) zum Zeitpunkt ihrer Offenlegung bereits öffentlich bekannt waren oder nachträglich ohne Verstoß gegen diese Vereinbarung öffentlich bekannt werden,

- b) DICIS nachweislich bereits vor ihrer Offenlegung rechtmäßig bekannt waren,
- c) DICIS von einem hierzu berechtigten Dritten rechtmäßig und ohne Vertraulichkeitsverpflichtung mitgeteilt wurden oder
- d) aufgrund gesetzlicher Vorschriften, behördlicher Anordnung oder vollziehbarer gerichtlicher Entscheidung offengelegt werden müssen.

Soweit rechtlich zulässig, informiert DICIS den Auftraggeber vor einer Offenlegung nach Buchstabe d) und beschränkt die Offenlegung auf den zwingend erforderlichen Umfang.

(8) DICIS trifft angemessene organisatorische Maßnahmen, um vertrauliche Informationen vor unbefugter Kenntnisnahme, Verwendung, Weitergabe, Veränderung oder Verlust zu schützen.

(9) Die Verpflichtungen aus diesem § 4 bestehen auch nach Beendigung der Geschäftsbeziehung und dieser Vereinbarung fort, solange und soweit die betreffenden Informationen ihrem Wesen nach vertraulich sind oder ein berechtigtes Geheimhaltungsinteresse des Auftraggebers besteht.

§ 5 Technische und organisatorische Maßnahmen

(1) DICIS trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO.

(2) Die zum Zeitpunkt des Vertragsschlusses geltenden technischen und organisatorischen Maßnahmen sind in Anlage 1 beschrieben. Sie sind Bestandteil dieser Vereinbarung.

(3) Da technische und organisatorische Maßnahmen dem technischen Fortschritt und der Weiterentwicklung der Systeme unterliegen, ist DICIS berechtigt, gleichwertige oder bessere Maßnahmen einzuführen. Das vereinbarte Schutzniveau darf dadurch nicht unterschritten werden.

(4) DICIS überprüft die Wirksamkeit der getroffenen Maßnahmen regelmäßig und passt diese bei Bedarf an die Risikolage und den Stand der Technik an.

§ 6 Unterstützung bei Betroffenenrechten

(1) DICIS unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und soweit dies möglich ist durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung seiner Pflichten zur Beantwortung von Anträgen betroffener Personen nach Kapitel III der DSGVO.

(2) Dies betrifft insbesondere Anträge auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Datenübertragbarkeit sowie – soweit einschlägig – Widersprüche gegen Verarbeitungen.

(3) Geht bei DICIS unmittelbar eine Anfrage einer betroffenen Person ein, die erkennbar eine Verarbeitung im Verantwortungsbereich des Auftraggebers betrifft, leitet DICIS diese Anfrage ohne schuldhaftes Zögern an den Auftraggeber weiter. DICIS beantwortet die Anfrage nicht eigenständig, sofern keine entsprechende Weisung des Auftraggebers oder gesetzliche Verpflichtung besteht.

(4) Soweit die Funktionalität der Software dies ermöglicht, kann die Unterstützung insbesondere darin bestehen, dem Auftraggeber den Zugriff auf, den Export, die Berichtigung oder die Löschung der betreffenden Daten zu ermöglichen.

§ 7 Unterstützung bei Pflichten nach Art. 32 bis 36 DSGVO

(1) DICIS unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der DICIS zur Verfügung stehenden Informationen in angemessenem Umfang bei der Einhaltung seiner Pflichten nach Art. 32 bis 36 DSGVO.

(2) Die Unterstützung umfasst insbesondere die Bereitstellung relevanter Informationen über die technischen und organisatorischen Maßnahmen und die Verarbeitung, soweit diese Informationen für die Bewertung der Sicherheit der Verarbeitung, eine Datenschutz-Folgenabschätzung oder eine gegebenenfalls erforderliche vorherige Konsultation der Aufsichtsbehörde benötigt werden.

(3) Soweit eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO für eine vom Auftraggeber verantwortete Verarbeitung erforderlich ist, stellt DICIS auf Anfrage die in ihrem Verantwortungsbereich vorhandenen und für die Bewertung erforderlichen Informationen zur Verfügung.

(4) Soweit eine vorherige Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO erforderlich ist, unterstützt DICIS den Auftraggeber hinsichtlich der von DICIS durchgeführten Verarbeitung durch die Bereitstellung der hierfür verfügbaren Informationen.

§ 8 Verletzungen des Schutzes personenbezogener Daten

(1) DICIS informiert den Auftraggeber unverzüglich, nachdem DICIS eine Verletzung des Schutzes personenbezogener Daten festgestellt hat, soweit personenbezogene Daten betroffen sind, die DICIS im Auftrag des Auftraggebers verarbeitet.

(2) Die Mitteilung enthält, soweit die Informationen DICIS zu diesem Zeitpunkt vorliegen, insbesondere eine Beschreibung der Art des Vorfalls, die betroffenen Daten und Personengruppen, die

voraussichtlichen Folgen sowie die von DICIS ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung oder Begrenzung des Vorfalles.

(3) Können nicht alle Informationen gleichzeitig bereitgestellt werden, darf DICIS diese ohne unangemessene weitere Verzögerung schrittweise ergänzen.

(4) DICIS unterstützt den Auftraggeber im angemessenen Umfang bei der Erfüllung etwaiger Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO.

§ 9 Unterauftragsverarbeiter

(1) Der Auftraggeber erteilt DICIS die allgemeine Genehmigung, weitere Auftragsverarbeiter („Unterauftragsverarbeiter“) einzusetzen, soweit dies für die Erbringung der vertraglich vereinbarten Leistungen erforderlich ist.

(2) Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter ergeben sich aus den Angaben in der öffentlich einsehbaren Datenschutzerklärung unter <https://www.dicisgroup.com/de/datenschutz/>.

(3) Die von DICIS eingesetzten Unterauftragsverarbeiter ergeben sich aus der jeweils aktuellen Übersicht der Unterauftragsverarbeiter, die Bestandteil der Datenschutzbestimmungen von DICIS ist und auf der Website von DICIS dauerhaft elektronisch abrufbar ist. Der Auftraggeber stimmt dem Einsatz der dort aufgeführten Unterauftragsverarbeiter allgemein zu.

(3) DICIS ist berechtigt, die Liste der Unterauftragsverarbeiter zu aktualisieren und bestehende Unterauftragsverarbeiter zu ersetzen oder weitere Unterauftragsverarbeiter hinzuzuziehen. DICIS informiert den Auftraggeber über eine solche beabsichtigte Änderung in elektronischer Form. Die Information kann insbesondere durch einen automatisierten Hinweis im Kundenkonto, innerhalb der von DICIS bereitgestellten Software oder durch eine andere dem Auftraggeber elektronisch zugehende Mitteilung erfolgen. Einer gesonderten Zustimmung des Auftraggebers zu der Änderung bedarf es nicht.

(4) Der Auftraggeber kann innerhalb von 14 Kalendertagen nach Bereitstellung der Änderungsinformation aus nachweisbaren datenschutzrechtlichen Gründen gegen die Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters Einspruch erheben. Erfolgt innerhalb dieser Frist kein Einspruch, gilt die Änderung im Rahmen der erteilten allgemeinen Genehmigung als akzeptiert.

(5) Im Fall eines berechtigten Einspruchs bemühen sich die Parteien um eine angemessene Lösung. Ist eine solche Lösung nicht möglich und kann DICIS die Leistung ohne den betreffenden Unterauftragsverarbeiter nicht oder nur mit unverhältnismäßigem Aufwand erbringen, bleiben die vertraglichen Rechte der Parteien nach dem Hauptvertrag unberührt.

(6) DICIS verpflichtet jeden Unterauftragsverarbeiter vertraglich zu Datenschutzpflichten, die im Wesentlichen den für DICIS aus dieser Vereinbarung geltenden Pflichten entsprechen, soweit diese Pflichten auf die jeweilige Unterauftragsverarbeitung anwendbar sind.

(7) DICIS bleibt gegenüber dem Auftraggeber für die Erfüllung der Datenschutzpflichten der eingesetzten Unterauftragsverarbeiter nach Maßgabe der gesetzlichen Bestimmungen verantwortlich.

§ 10 Datenübermittlungen in Drittländer

- (1) Eine Übermittlung personenbezogener Daten in ein Drittland außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums oder an eine internationale Organisation erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind und die Übermittlung vom Leistungsumfang und den dokumentierten Weisungen des Auftraggebers gedeckt ist.
- (2) Soweit erforderlich, stellt DICIS sicher, dass für die jeweilige Übermittlung ein zulässiger Übermittlungsmechanismus besteht, insbesondere ein Angemessenheitsbeschluss oder geeignete Garantien nach Art. 46 DSGVO.
- (3) DICIS stellt dem Auftraggeber auf Anfrage Informationen über die für die jeweilige Übermittlung maßgeblichen Garantien zur Verfügung, soweit dem keine gesetzlichen oder vertraglich zulässigen Geheimhaltungspflichten entgegenstehen.

§ 11 Informations-, Nachweis- und Kontrollrechte

- (1) DICIS stellt dem Auftraggeber alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten nachzuweisen.
- (2) Zum Nachweis können insbesondere geeignete Zertifizierungen und Beschreibungen der technischen und organisatorischen Maßnahmen herangezogen werden.
- (3) DICIS ermöglicht und unterstützt die gesetzlich erforderlichen Überprüfungen und Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer.

§ 12 Löschung und Rückgabe personenbezogener Daten

- (1) Nach Beendigung der Auftragsverarbeitung löscht oder gibt DICIS nach Wahl des Auftraggebers die im Auftrag verarbeiteten personenbezogenen Daten zurück und löscht vorhandene Kopien, soweit nicht nach dem Recht der Europäischen Union oder eines Mitgliedstaats eine Verpflichtung zur weiteren Speicherung besteht.
- (2) Soweit im Hauptvertrag oder in den Funktionen der Software ein Verfahren zum Export oder zur Rückgabe von Daten vorgesehen ist, kann die Rückgabe über dieses Verfahren erfolgen.
- (3) Daten in Sicherungskopien werden im Rahmen der regulären Sicherungs- und Löschzyklen gelöscht oder überschrieben, sofern eine sofortige selektive Löschung technisch nicht möglich oder nur mit unverhältnismäßigem Aufwand durchführbar ist. Bis zur endgültigen Löschung bleiben die Daten den Schutzpflichten dieser Vereinbarung unterworfen und dürfen nicht für andere Zwecke verarbeitet werden.
- (4) Dokumentationen, die DICIS zum Nachweis einer ordnungsgemäßen Auftragsverarbeitung oder aufgrund gesetzlicher Aufbewahrungspflichten benötigt, dürfen über das Vertragsende hinaus im erforderlichen Umfang aufbewahrt werden.

§ 13 Pflichten und Verantwortlichkeit des Auftraggebers

- (1) Der Auftraggeber ist im Verhältnis zu DICIS für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten, die Zulässigkeit der Datenübermittlung an DICIS und die Wahrung der Rechte der betroffenen Personen verantwortlich.
- (2) Der Auftraggeber stellt sicher, dass seine Weisungen mit den anwendbaren Datenschutzvorschriften vereinbar sind.
- (3) Der Auftraggeber informiert DICIS unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch DICIS feststellt.
- (4) Der Auftraggeber benennt DICIS auf Anfrage die für Datenschutzfragen und Weisungen zuständigen Ansprechpartner.

§ 14 Kosten besonderer Unterstützungsleistungen

- (1) Die gewöhnlichen Leistungen von DICIS zur Erfüllung der gesetzlichen Pflichten aus dieser Vereinbarung sind mit der Vergütung des Hauptvertrags abgegolten.
- (2) Verlangt der Auftraggeber darüber hinausgehende individuelle Unterstützungs-, Prüfungs- oder Umsetzungsleistungen, die nicht durch einen Verstoß von DICIS verursacht wurden und den üblichen Leistungsumfang erheblich überschreiten, können diese nach vorheriger Abstimmung nach Aufwand vergütet werden. Gesetzlich zwingende Rechte des Auftraggebers und Pflichten von DICIS bleiben unberührt.

§ 15 Laufzeit und Schlussbestimmungen

- (1) Diese Vereinbarung tritt gleichzeitig mit dem Hauptvertrag oder mit ihrer wirksamen Einbeziehung in das bestehende Vertragsverhältnis in Kraft und gilt für die Dauer der Auftragsverarbeitung.
- (2) Soweit Bestimmungen des Hauptvertrags und dieser Vereinbarung datenschutzrechtliche Fragen der Auftragsverarbeitung unterschiedlich regeln, gehen die Bestimmungen dieser Vereinbarung vor.
- (3) Änderungen und Ergänzungen dieser Vereinbarung können in elektronischer Form oder Textform vereinbart werden, soweit nicht zwingendes Recht eine strengere Form verlangt.
- (4) Sollte eine Bestimmung dieser Vereinbarung ganz oder teilweise unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.
- (5) Im Übrigen gelten die Bestimmungen des Hauptvertrags.

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Die nachfolgend aufgeführten technischen und organisatorischen Maßnahmen (TOM) beschreiben die von DICIS getroffenen Maßnahmen zum Schutz personenbezogener Daten gemäß Art. 32 DSGVO. Sie dienen insbesondere der Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der zur Verarbeitung personenbezogener Daten eingesetzten Systeme und Dienste.

1. Vertraulichkeit

- Zutrittskontrolle zu Betriebs- und Rechenzentrumsbereichen;
- Zugangskontrolle durch individuelle Benutzerkonten und geeignete Authentifizierungsverfahren;
- rollen- und berechtigungsbasierte Zugriffskontrolle nach dem Need-to-know-Prinzip;
- regelmäßige Überprüfung und Anpassung von Berechtigungen;
- Verschlüsselung geeigneter Übertragungswege nach dem Stand der Technik;
- Verpflichtung zugriffsberechtigter Personen auf Vertraulichkeit;
- Mandantentrennung und Trennung von Entwicklungs-, Test- und Produktivumgebungen, soweit technisch vorgesehen.

2. Integrität

- Schutz der Datenübertragung gegen unbefugte Kenntnisnahme und Veränderung;
- Protokollierung sicherheitsrelevanter System- und Administrationsvorgänge;
- geregelte Änderungs-, Freigabe- und Berechtigungsprozesse;
- Schutz vor Schadsoftware und unberechtigten Systemzugriffen;
- geeignete Verfahren zur sicheren Softwareentwicklung, Wartung und Aktualisierung.

3. Verfügbarkeit und Belastbarkeit

- regelmäßige Datensicherungen nach einem definierten Backup-Konzept;
- geeignete Wiederherstellungsverfahren;
- redundante oder ausfallsichere Infrastruktur, soweit für die vereinbarte Leistung erforderlich;
- Monitoring wesentlicher Systeme und Behandlung technischer Störungen;
- geregeltes Patch- und Schwachstellenmanagement;
- Notfall- und Wiederanlaufverfahren entsprechend der Risikolage.

4. Verfahren zur regelmäßigen Überprüfung

- regelmäßige Überprüfung der Wirksamkeit technischer und organisatorischer Maßnahmen;
- Informationssicherheits- und Datenschutzrichtlinien;
- Schulung und Sensibilisierung der Beschäftigten;
- Incident-Response- und Meldeprozesse;
- regelmäßige Überprüfung von Berechtigungen, Risiken und Sicherheitsmaßnahmen;
- interne oder externe Audits und Prüfungen entsprechend dem eingesetzten Managementsystem.

5. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

- Berücksichtigung von Datenminimierung, Zweckbindung und Berechtigungskonzepten bei der Systemgestaltung;
- datenschutzfreundliche Voreinstellungen, soweit dies durch DICIS beeinflussbar ist;
- Möglichkeiten zur Löschung, Berichtigung oder zum Export von Daten, soweit funktional vorgesehen.

6. Auftragskontrolle

- dokumentierte Vereinbarungen zur Auftragsverarbeitung;
- geregelte Prozesse zur Erteilung und Befolgung von Weisungen;
- Auswahl und Kontrolle von Unterauftragsverarbeitern;
- festgelegte Zuständigkeiten und Ansprechpartner;
- Kontrolle der weisungsgebundenen Verarbeitung.