Auftragsverarbeitungsvertrag nach Artikel 28 DSGVO

zwischen

(kurz: „**Auftraggeber**" / „Verantwortlicher")

und

ABACUS Informationssysteme GmbH,

Schießhausstrasse 2, 72275 Alpirsbach

(kurz: „**Auftragnehmer**" / "Auftragsverarbeiter")

Präambel

P.1. Auftraggeber und Auftragnehmer sehen sich den hohen Standards verpflichtet, die im Hinblick auf den Datenschutz gelten.

P.2. Der vorliegende **A**uftrags**v**erarbeitungs**v**ertrag (kurz: „**AVV**") konkretisiert für alle Verarbeitungen die Rechte und Pflichten der Parteien auf dem Gebiet des Datenschutzes, welche sich aus den zwischen den Parteien bereits oder künftig bestehenden rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnissen (kurz: „**Hauptvertrag**") ergeben.

P.3. Der Auftraggeber erhält Zugriff auf die im Rahmen der Zusammenarbeit in seinem Verbreitungsgebiet beim Auftragnehmer anfallenden Daten. Bei der Verwendung dieser Daten wird er sämtliche Datenschutzrechtlichen Bestimmungen beachten. Insbesondere ist dem Auftraggeber bewusst, dass eine Verarbeitung personenbezogener Daten nur nach ausdrücklicher Zustimmung der Nutzer zulässig ist.

§ 1 Auftrag und Spezifika der Verarbeitung

1.1. Der AVV kommt mit all seinen Teilen zur Anwendung, sofern und soweit der Auftraggeber den Auftragnehmer zur Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO (kurz: „**Daten**") verpflichtet hat.

1.2. Der AVV bildet den Rahmen für eine Vielzahl unterschiedlicher Vorgänge der Auftragsverarbeitung.

1.3. Die für einzelne Verarbeitungen geltenden spezifischen datenschutzrechtlichen Festlegungen (kurz: „**Spezifika**") werden vor Beginn der Verarbeitung in Anlagen zum AVV geregelt. Dies sind insbesondere Gegenstand und Dauer sowie Art und Zweck der Verarbeitung, die Kategorie der Daten und die Kategorien betroffener Personen sowie die technischen und organisatorischen Maßnahmen („**TOM**").

1.4. Die Anlagen sind Teil des AVV. Bei etwaigen Widersprüchen gehen die Regelungen der ANLAGEN der allgemeineren Regelung im AVV vor. Wird im Folgenden oder in den ANLAGEN auf den AVV Bezug genommen, so ist der AVV mit allen seinen Teilen gemeint.

§ 2 Verantwortlichkeit und Verarbeitung auf Weisung

2.1. Der Auftraggeber ist im Rahmen dieses AVV für die Einhaltung der anwendbaren gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Offenlegung gegenüber dem Auftragnehmer sowie für die Rechtmäßigkeit der Verarbeitung allein verantwortlich („Verantwortlicher" im Sinne des Art. 4 Nr. 7 DSGVO).

2.2. Der Auftragnehmer handelt ausschließlich weisungsgebunden, außer es liegt ein Ausnahmefall im Sinne des Art. 28 Abs. 3 a DSGVO vor (anderweitige gesetzliche Verarbeitungspflicht). Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

2.3. Der Auftragnehmer verändert oder löscht die vertragsgegenständlichen Daten oder schränkt deren Verarbeitung ein (kurz: „**Sperrung**"), wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist.

2.4. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Vorschriften über den Datenschutz verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis diese vom Auftraggeber in Textform bestätigt oder abgeändert wurde. Die Ausführung offensichtlich datenschutzrechtswidriger Weisungen darf der Auftragnehmer jederzeit ablehnen.

2.5. Der Auftraggeber benennt in Textform einen oder mehrere Ansprechpartner in datenschutzrechtlichen Angelegenheiten, einschließlich der bestellten Datenschutzbeauftragten. Ergeben sich bei den Ansprechpartnern Änderungen, haben sich die Parteien hierüber in Textform zu informieren.

2.6. Die Datenschutzbeauftragte des Auftragsnehmers ist:
Doris Senger, Forlenweg 13, 78166 Donaueschingen, email ds@ub-senger.de

2.7. Der Auftragnehmer gewährleistet, dass die zur Verarbeitung der Daten befugten Personen die Weisungen des Auftraggebers kennen und diese beachten.

2.8. Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben und einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits- und Verschwiegenheitspflicht besteht auch nach Beendigung der Verarbeitung fort.

§ 3 Sicherheit der Verarbeitung

3.1. Die Parteien vereinbaren TOM gemäß Art. 32 DSGVO zum angemessenen Schutz der Daten (kurz: „**Anhang TOM**").

3.2. Änderung der vereinbarten TOM bleiben dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau insgesamt nicht unterschritten wird. Wesentliche Änderungen sind dem Auftraggeber in Textform mitzuteilen.

3.3. Eigene technische und organisatorische Maßnahmen des Auftraggebers für eine auf den Auftragnehmer übertragene Datenverarbeitung trifft der Auftraggeber im Benehmen mit dem Auftragnehmer.

§ 4 Unterrichtung bei Datenschutzverletzungen und Fehlern der Verarbeitung

4.1. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes von Daten im Sinne des Art. 4 Nr. 12 DSGVO in seinem Organisationsbereich bekannt werden oder ein konkreter Verdacht einer solchen Datenschutzverletzung beim Auftragnehmer besteht. Mündliche Unterrichtungen sind in Textform nachzureichen. Der Auftragnehmer stimmt sich zur Behandlung solcher Verletzungen mit dem Auftraggeber ab. Die Parteien treffen die erforderlichen Maßnahmen, einschließlich der Maßnahmen zur Minderung möglicher nachteiliger Folgen.

4.2. Stellt der Auftraggeber Fehler bei der Verarbeitung fest, hat er den Auftragnehmer unverzüglich hierüber zu informieren und das weitere Vorgehen mit ihm abzustimmen. Mündliche Unterrichtungen sind unverzüglich in Textform nachzureichen.

§ 5 Übermittlung von Daten an einen Empfänger in einem Drittland

Die Übermittlung von Daten an einen Empfänger in einem Drittland außerhalb von EU und EWR ist unter den in Art. 44 ff. DSGVO geschriebenen Bedingungen zulässig. Einzelheiten werden in einer oder mehreren ANLAGEN geregelt.

§ 6 Unterbeauftragung weiterer Auftragsverarbeiter

6.1. Der Auftragnehmer darf die Verarbeitung personenbezogener Daten ganz oder teilweise durch weitere Auftragsverarbeiter (kurz: „**Unterauftragnehmer**") erbringen lassen.

6.2. Der Auftragnehmer informiert den Auftraggeber rechtzeitig vorab über die Beauftragung von Unterauftragnehmern oder Änderungen in der Unterbeauftragung. Der Auftraggeber kann bei Vorliegen eines wichtigen Grundes der Unterbeauftragung innerhalb von vier Wochen nach Kenntnisnahme in Textform widersprechen. Ein wichtiger Grund liegt insbesondere vor, wenn ein begründeter Anlass zu Zweifeln besteht, dass der Unterauftragnehmer die vereinbarte Leistung entsprechend den anwendbaren gesetzlichen Bestimmungen zum Datenschutz oder gemäß dieser AVV erbringt.

6.3. Der Auftragnehmer wird mit dem Unterauftragnehmer die in diesem AVV getroffenen Regelungen inhaltsgleich vereinbaren. Insbesondere müssen die mit dem Unterauftragnehmer zu vereinbarenden technischen und organisatorischen Maßnahmen mindestens dasselbe Schutzniveau aufweisen.

6.4. Keine Unterbeauftragungen im Sinne dieser Regelung sind Leistungen, die der Auftragnehmer als reine Nebenleistung zur Unterstützung seiner geschäftlichen Tätigkeit außerhalb der Auftragsverarbeitung in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes der Daten auch für solche Nebenleistungen angemessene Vorkehrungen zu ergreifen.

§ 7 Unterstützung des Auftraggebers bei der Geltendmachung von Betroffenenrechten

Macht eine betroffene Person Ansprüche gemäß Kapitel 3 der DSGVO bei einer der Parteien geltend, so informiert sie die jeweils andere Partei darüber unverzüglich. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Bearbeitung solcher Anträge sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

§ 8 Kontroll- und Informationsrechte des Auftraggebers

8.1. Der Auftragnehmer weist dem Auftraggeber die Einhaltung seiner Pflichten mit geeigneten Mitteln nach. Der Auftraggeber überprüft die Geeignetheit.

8.2. Der Auftraggeber ist berechtigt, zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs, regelmäßig nach vorheriger Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit, Inspektionen beim Auftragnehmer zur Prüfung der Einhaltung der datenschutzrechtlichen Bestimmungen durchzuführen. Der Auftragnehmer darf die Inspektion von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der von ihm getroffenen technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen die Beauftragung dieses Prüfers ein Einspruchsrecht.

8.3. Zur Behebung der bei einer Inspektion getroffenen Feststellungen stimmen die Parteien umzusetzende Maßnahmen ab.

8.4. Macht eine Aufsichtsbehörde von Befugnissen nach Art. 58 DSGVO Gebrauch, so informieren sich die Parteien hierüber unverzüglich. Sie unterstützen sich in ihrem jeweiligen Verantwortungsbereich, bei Erfüllung der gegenüber der jeweiligen Aufsichtsbehörde bestehenden Verpflichtungen.

§ 9 Haftung und Schadenersatz

9.1. Macht ein Betroffener gegenüber einer Partei Schadenersatzansprüche wegen Verstoßes gegen datenschutzrechtliche Bestimmungen geltend, so hat die beanspruchte Partei die andere Partei hierüber unverzüglich zu informieren.

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

9.3. Die Parteien unterstützen sich wechselseitig bei der Abwehr von Schadenersatzansprüchen betroffener Personen, es sei denn, dies würde die Rechtsposition der einen Partei im Verhältnis zur anderen Partei oder zur Aufsichtsbehörde gefährden.

§ 10 Laufzeit

10.1. Der AVV wird auf unbestimmte Zeit geschlossen. Die Laufzeit seiner ANLAGEN wird in den ANLAGEN selbst geregelt; ohne eine solche Regelung entspricht die Laufzeit einer ANLAGE derjenigen des AVV.

10.2. Der AVV kann mit einer Frist von drei Monaten zum Monatsende gekündigt werden, wenn gleichzeitig oder zuvor alle ANLAGEN beendet wurden.

10.3. Eine ANLAGE endet mit Beendigung des zugehörigen AVV, ohne dass es einer gesonderten Kündigung dieser ANLAGE bedarf. Der Auftragnehmer hat in diesem Fall nach Wahl des Auftraggebers unverzüglich die nach der ANLAGE verarbeiteten Daten herauszugeben oder datenschutzkonform zu löschen und dies dem Auftraggeber in Textform (z. B. durch ein Löschprotokoll) zu bestätigen. Sofern der Auftragnehmer eine eigene gesetzliche Pflicht zur Speicherung dieser Daten hat, hat er dies dem Auftraggeber in Textform anzuzeigen.

§ 11 Fortgeltung und Überleitung von Altverträgen

Der AVV ersetzt mit Wirkung ab dem 25.05.2018 die bestehenden Verträge nach § 11 BDSG. Haben die Parteien vor Abschluss dieses AVV Spezifka im Sinne von § 1 vereinbart, so gelten diese sinngemäß unter dem AVV fort, es sei denn sie werden durch ANLAGEN ersetzt, denen derselbe Verarbeitungsgegenstand zu Grunde liegt.

§ 12 Schlussbestimmungen

12.1. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber in Textform zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich in Textform darüber informieren, dass die Verantwortung für die Daten ausschließlich beim Auftraggeber liegt.

12.2. Mündliche Nebenabreden wurden nicht getroffen. Änderungen und Ergänzungen des AVV bedürfen zu ihrer Wirksamkeit der Textform und der ausdrücklichen Bezugnahme auf die AVV. Abweichende mündliche Abreden der Parteien sind unwirksam. Dies gilt auch für Änderungen dieser Klausel.

12.3. Sollte auch nur eine Bestimmung dieser Vereinbarung ganz oder teilweise rechtsunwirksam oder nichtig sein oder werden, bleibt dieser AVV im Übrigen gleichwohl aufrechterhalten und gültig. An Stelle der rechtsunwirksamen oder nichtigen Bestimmung gilt das Gesetz, sofern die hierdurch entstandene Lücke nicht durch ergänzende Vertragsauslegung gemäß §§ 133, 157 BGB geschlossen werden kann. Beide Parteien sind jedoch insoweit verpflichtet, unverzüglich eine rechtswirksame und datenschutzkonforme Vertragsergänzung abzustimmen und zu erstellen.

12.4. Anwendbares Recht ist das Recht der Bundesrepublik Deutschland.
Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen des Artikel 44 ff. DSGVO erfüllt sind.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift	Unterschrift
_____	_____
Name, Funktion Unterzeichner (in Druckbuchstaben) Auftraggeber	Name, Funktion Unterzeichner (in Druckbuchstaben) Auftragnehmer

AVV Anlage 1

Gegenstand der Verarbeitung (des Auftrags)

Gegenstand des Auftrags ist:

Betreuung div. IT-Systeme des Auftraggebers
ggf. Benutzerservice

_____

_____

In diesem System ist ersichtlich:

- Benutzer und Berechtigungen
- Ggf. Dateien
- Ggf. Datenbanken
- Ggf. emails
- Ggf. ergänzen:

Dauer des Auftrags

Der Auftrag beginnt mit Unterzeichnung dieses Vertrags und wird auf unbestimmte Zeit geschlossen. Er ist mit einer Frist von **3 Monaten zum Monatsende** kündbar. Die Möglichkeit zur fristlosen Kündigung aus besonderem Grund bleibt hiervon unberührt.

Zweck der Verarbeitung

Die Tätigkeit des Auftragnehmers dient folgenden vereinbarten Zwecken:

☐ Lieferung und Betreuung von IT-Systemen in Räumen des Auftragsgebers oder per Fernwartung
☐ Lieferung von Waren
☐ Beratung zum IT-Einsatz und zur Geschäftsprozessunterstützung durch IT-Systeme
☐ Aufbau und Wartung Dokumentenmanagement
☐ Aufbau und Wartung email-Archivierung
☐ Aufbau und Wartung der Unternehmensfirewall und/oder des Netzwerkes (LAN)
☐ Hosting von Internetdiensten wie email (smtp, pop3, imap), Webserver (http, https) und Datenübertragung (ftp, sftp)
☐ Bereitstellung von Zugängen zum Internet mittels einer Benutzerkennung
☐ Kommunikation mittels elektronischer Medien
☐ Ermöglichung der Kontaktierung von Nutzern
☐ Dokumentation von Aktivitäten aufgrund dieses Vertrages
☐ Zugangsverwaltung hinsichtlich IuK-Technik und Unternehmensnetzwerk
☐ Verwaltung von Berechtigungen
☐ Verwaltung von Softwarelizenzen
☐ Abrechnung der erbrachten Dienstleistungen und Warenlieferungen
☐ Support, Wartung- und Updatetätigkeiten
☐ **Weitere** –siehe ggf. gesonderte Anlage

AVV Anlage 1

Datenarten / -kategorien

Folgende Datenarten sind Gegenstand dieses Auftrags:		
☐ Adressdaten	☐ Gesundheitsdaten	☐ Personal- und Identifikationsnummern
☐ Alter	☐ Kreditkartendaten	☐ Reisebuchungs- und -abrechnungsdaten
☐ Arbeitszeitdaten	☐ Gerätenamen MAC-Adressen	☐ Telekommunikations-abrechnungsdaten
☐ Audiodaten	☐ Lohn- und Gehaltsdaten	☐ IP-Verbindungsdaten
☐ Bankverbindungsdaten inkl. Zahlungsverkehrsdaten	☐ IP-Adressen	☐ Telefonnummern
☐ Bewerberdaten	☐ Mitarbeiter-qualifikation und eigenschaften	☐ Vertragsdaten
☐ Bilddaten	☐ Namen	☐ Videodaten
☐ Passwörter	☐ Nutzerkennungen	☐ Zahlungsdaten
☐ E-Mails	☐ sonst. Zugangsdaten	☐
☐ sonstige:		

AVV Anlage 1

Kreis der Betroffenen

Folgende Kategorien von Betroffenen sind Gegenstand des Auftrags:

- ☐ Beschäftigte
- ☐ Auszubildende und Praktikanten
- ☐ Bewerber
- ☐ ehemalige Arbeitnehmer
- ☐ freie Mitarbeiter
- ☐ Gesellschafter
- ☐ Angehörige von Beschäftigten
- ☐ Kunden
- ☐ Interessenten
- ☐ Lieferanten und Dienstleister
- ☐ Mieter
- ☐ Geschäftspartner
- ☐ externe Berater
- ☐ Besucher
- ☐ Pressevertreter
- ☐ sonstige: [Bitte ergänzen]

Besondere technische und organisatorische Maßnahmen

- ☐ Besonders abgegrenzte oder geschützte Gebäudeteile
- ☐ Besonders restriktiver Zugriff (restriktive Rollenvergabe, VAP, …)
- ☐ Spezielle Protokolle
- ☐ Besondere Maßnahmen der Verschlüsselung
- ☐ Trusted Employee-Bereich
- ☐ Besondere Kameraüberwachung
- ☐ Zusätzliche Backups / Ausfallrechenzentrum im Salzstock / …
- ☐ Leckage-System
- ☐ Sonstiges: [Bitte ergänzen]

Technisch-organisatorische Maßnahmen nach Art. 32 DSGVO

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

a) Zutrittskontrolle || Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen haben:

- ☐ Zutrittskontrollsystem, Ausweisleser (Magnet-/Chipkarte)
- ☒ Türsicherungen (Sicherheitsschloß, etc.)
- ☒ Sicherheitstüren / -fenster
- ☒ Gitter vor Fenstern/Türen
- ☐ Zaunanlagen
- ☐ Schlüsselverwaltung/Dokumentation der Schlüsselvergabe
- ☐ Werkschutz, Pförtner
- ☐ Alarmanlage
- ☐ Videoüberwachung
- ☐ Spezielle Schutzvorkehrungen des Serverraums
- ☐ Spezielle Schutzvorkehrungen für die Aufbewahrung von Back-Ups und/oder sonstigen Datenträgern
- ☐ Nicht-reversible Vernichtung von Datenträgern
- ☐ Mitarbeiter- und Berechtigungsausweise
- ☐ Sperrbereiche
- ☐ Besucherregelung (Bspw. Abholung am Empfang, Dokumentation von Besuchszeiten, Besucherausweis, Begleitung nach dem Besuch bis zum Ausgang)
- ☐ Ggf. sonstiges:

b) Zugangskontrolle || Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zugang zu den Datenverarbeitungssystemen haben.

- ☒ Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk
- ☐ Autorisierungsprozess für Zugangsberechtigungen
- ☐ Begrenzung der befugten Benutzer
- ☐ Single Sign-On
- ☐ BIOS-Passwörter
- ☒ Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall)
- ☒ Elektronische Dokumentation von Passwörtern und Schutz dieser Dokumentation vor unbefugtem Zugriff
- ☐ Personalisierte Chipkarten, Token, PIN-/TAN, etc.

- ☒ Protokollierung des Zugangs
- ☐ Zusätzlicher System-Log-In für bestimmte Anwendungen
- ☐ Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)
- ☒ Firewall
- ☐ sonstiges: [**Bitte ggf. ergänzen**]

c) Zugriffskontrolle || Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben.

- ☒ Verwaltung und Dokumentation von differenzierten Berechtigungen
- ☒ Abschluss von Verträgen zur Auftragsdatenverarbeitung für die externe Pflege, Wartung und Reparatur von Datenverarbeitungs-Anlagen, sofern bei der Fernwartung die Verarbeitung von personenbezogenen Daten Gegenstand der Dienstleistung ist.
- ☐ Auswertungen/Protokollierungen von Datenverarbeitungen
- ☐ Autorisierungsprozess für Berechtigungen
- ☐ Genehmigungsroutinen
- ☐ Profile/Rollen
- ☐ Verschlüsselung von CD/DVD- ROM, externen Festplatten und/oder Laptops (etwa per Betriebssystem, TrueCrypt, Safe Guard Easy, WinZip, PGP)
- ☐ Maßnahmen zur Verhinderung unbefugten Überspielens von Daten auf extern verwendbare Datenträger (z.B. Kopierschutz, Sperrung von USB-Ports, „Data Loss Prevention (DLP)-System")
- ☐ „Mobile Device Management-System"
- ☐ Vier-Augen-Prinzip
- ☐ Funktionstrennung „Segregation of Duties"
- ☐ Fachkundige Akten- und Datenträgervernichtung gemäß DIN 66399
- ☐ Nicht-reversible Löschung von Datenträgern
- ☐ Sichtschutzfolien für mobile Datenverarbeitungssysteme
- ☐ sonstiges: [**Bitte ggf. ergänzen**]

d) Trennungskontrolle || Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden.

- ☐ Speicherung der Datensätze in physikalisch getrennten Datenbanken
- ☐ Verarbeitung auf getrennten Systemen
- ☒ Zugriffsberechtigungen nach funktioneller Zuständigkeit
- ☐ Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen

- ☐ Mandantenfähigkeit von IT-Systemen
- ☐ Verwendung von Testdaten
- ☐ Trennung von Entwicklungs- und Produktionsumgebung

e) Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) || Die Verarbeitung personenbezogener Daten erfolgt 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.

☐ Sämtliche zum Einloggen erhobenen MAC Adress Daten werden mittels hash werden pseuodonymisiert.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

a) Weitergabekontrolle || Es ist sichergestellt, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

- ☒ Verschlüsselung von Email bzw.- Email-Anhängen (z.B. WinZip)
- ☐ Verschlüsselung des Speichermediums von Laptops
- ☒ Gesicherter File Transfer (z.B. sftp)
- ☒ Gesicherter Datentransport (z.B. SSL, ftp, ftps, TLS)
- ☐ Verschlüsselung von CD/DVD- ROM, externen Festplatten oder USB-Sticks (z.B. True Crypt, Safe Guard Easy, PGP)
- ☐ Physikalische Transportsicherung
- ☐ Verpackungs- und Versandvorschriften
- ☐ Elektronische Signatur
- ☒ Gesichertes WLAN
- ☐ Fernwartungskonzept (z.B. Verschlüsselung, Ereignisauslösung durch Auftraggeber, Challenge-Response, Rückrufautomatik, Einmal-Passwort)
- ☐ „Mobile Device Management-System"
- ☐ „Data Loss Prevention (DLP)-System"
- ☐ Regelung zum Umgang mit mobilen Speichermedien (z.B. Laptop, USB-Stick, Mobiltelefon)
- ☐ Protokollierung von Datenübertragung oder Datentransport
- ☐ Protokollierung von lesenden Zugriffen

- ☐ Protokollierung des Kopierens, Veränderns oder Entfernens von Daten
- ☒ Getunnelte Datenfernverbindungen (VPN = Virtuelles Privates Netzwerk)
- ☐ sonstiges: [**Bitte ggf. ergänzen**]

b) Eingabekontrolle || Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat.

- ☒ Zugriffsrechte
- ☐ Systemseitige Protokollierungen
- ☐ Dokumenten Management System (DMS) mit Änderungshistorie
- ☐ Sicherheits-/Protokollierungssoftware
- ☒ Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten
- ☐ Mehraugenprinzip
- ☐ „Data Loss Prevention (DLP)-System"
- ☐ sonstiges: [**Bitte ggf. ergänzen**]

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle und Belastbarkeitskontrolle || Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind.

- ☒ Sicherheitskonzept für Software- und IT-Anwendungen
- ☒ Back-Up Verfahren
- ☒ Aufbewahrungsprozess für Back-Ups (brandgeschützter Safe, getrennter Brandabschnitt, etc.)
- ☐ Gewährleistung der Datenspeicherung im gesicherten Netzwerk
- ☒ Bedarfsgerechtes Einspielen von Sicherheits-Updates
- ☒ Spiegeln von Festplatten
- ☒ Einrichtung einer unterbrechungsfreien Stromversorgung (USV)
- ☐ Geeignete Archivierungsräumlichkeiten für Papierdokumente
- ☐ Brand- und/oder Löschwasserschutz des Serverraums
- ☐ Brand- und/oder Löschwasserschutz der Archivierungsräumlichkeiten
- ☐ Klimatisierter Serverraum
- ☒ Virenschutz
- ☒ Firewall
- ☐ Notfallplan
- ☐ Erfolgreiche Notfallübungen

☒ Redundante, örtlich getrennte Datenaufbewahrung (Offsite Storage)
☐ sonstige: [**Bitte ggf. ausführen**]

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

a) Datenschutz-Management || Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

☒ Richtlinien/Anweisungen zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Datensicherheit
☒ Bestellung eines Datenschutzbeauftragten
☒ Verpflichtung der Mitarbeiter auf das Datengeheimnis und Bankgeheimnis
☒ Hinreichende Schulungen der Mitarbeiter in Datenschutzangelegenheiten
☒ Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO)
☒ Durchführung von Datenschutzfolgenabschätzungen, soweit erforderlich (Art. 35 DSGVO)
☐ Ext. Prüfung/Auditierung der Informationssicherheit (etwa im Rahmen von ISO-Zertifizierung, SOX-Compliance)
☐ sonstige: [**Bitte ggf. ausführen**]

b) Incident-Response-Management ||Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

☒ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)
☒ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO)
☐ sonstige: [Bitte ggf. ausführen]

c) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO) ||

Die default Einstellungen sind sowohl bei den standardisierten Voreinstellungen von Systemen und Apps als auch bei der Einrichtung der Datenverarbeitungsverfahren zu berücksichtigen. In dieser Phase werden Funktionen und Rechte konkret konfiguriert, wird im Hinblick auf Datenminimierung die Zulässigkeit bzw. Unzulässigkeit bestimmter Eingaben

bzw. von Eingabemöglichkeiten (z. B. von Freitexten) festgelegt und über die Verfügbarkeit von Nutzungsfunktionen entschieden (z. B. hinsichtlich des Umfangs der Verarbeitung). Ebenso werden die Art und der Umfang des Personenbezugs bzw. der Anonymisierung (z. B. bei Selektions-, Export- und Auswertungsfunktionen, die festgelegt und voreingestellt oder frei gestaltbar zur Verfügung gestellt werden können) oder die Verfügbarkeit von bestimmten Verarbeitungsfunktionen, Protokollierungen etc. festgelegt.

d) Auftragskontrolle || Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten nur entsprechend der Weisungen verarbeitet werden können.

- ☒ Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers
- ☐ Prozess zur Erteilung und/oder Befolgung von Weisungen
- ☒ Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
- ☐ Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
- ☐ Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragnehmer
- ☐ Unabhängige Auditierung der Weisungsgebundenheit
- ☒ Verpflichtung der Mitarbeiter auf das Datengeheimnis
- ☐ Vereinbarung von Konventionalstrafen für Verstöße gegen Weisungen
- ☐ formalisiertes Auftragsmanagement
- ☐ dokumentiertes Verfahren zur Auswahl des Dienstleisters
- ☐ standardisiertes Vertragsmanagement zur Vor- und Nachkontrolle der Dienstleister
- ☐ sonstiges: [**Bitte ggf. ergänzen**]