LCE medical IT

IT for Healthcare

Vereinbarung zur Auftragsverarbeitungsvertrag nach Art. 28 DSGVO

zwischen dem/der

Firma:	……
Verantwortlicher:	……
Straße, Hausnr.:	……
PLZ, Ort:	……

- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der

Firma:	LCE Medical IT GmbH
Verantwortlicher:	Frau Madlen Vogt
Straße, Hausnr.:	Zwickauer Str. 16b
PLZ, Ort:	09112 Chemnitz

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

- Projektdienstleistungen für den Auftraggeber und ggf. für dessen Kunden,
- Auftragsabwicklung für den Auftraggeber und ggf. für dessen Kunden,
- Technischer Support, IT-Dienstleistungen,
- Kundenservice (Erklärung von Programmfunktion, Fehleranalyse der Systeme),
- Cloud-Services.

Da der Auftragnehmer in Erfüllung seiner Aufgaben, Daten im Auftrag, nach Weisung und im Interesse des Auftraggebers verarbeitet bzw. ein Zugriff auf personenbezogene Daten bei der Auftragserfüllung nicht ausgeschlossen werden kann, erfolgt die Dienstleistung als Auftragsverarbeitung nach den für den Auftraggeber einschlägigen deutschen und europäischen Datenschutzgesetzen.

(2) Dauer
Dieser Vertrag beginnt mit Unterzeichnung beider Vertragsparteien und gilt, solange der Auftragnehmer für den Auftraggeber personenbezogene Daten im Auftrag verarbeitet. Er endet jedoch nicht vor Erfüllung der Lösch- und Rückgabepflichten dieses Vertrages.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten
Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

- Abwicklung von IT-Service- und Wartungsleistungen

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Wird hergestellt durch verbindliche interne Datenschutzvorschriften
(Art. 46 Abs. 2 lit. b i.V.m. 47 DSGVO).

(2) Art der Daten
Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- Personen-/ Patientenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten
  (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kunden-/ Patientenhistorie
- Gesundheitsdaten
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- IP-Adresse

(3) Kategorien betroffener Personen
Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden/ Patienten
- Interessenten
- Abonnenten
- Beschäftigte
- Lieferanten
- Handelsvertreter

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen [Einzelheiten in Anlage I].

(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. Berichtigung, Einschränkung und Löschung von Daten

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

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

a) Der Auftragnehmer ist gemäß den geltenden datenschutzrechtlichen Bestimmungen, insbesondere der Datenschutz-Grundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG), nicht verpflichtet, einen Datenschutzbeauftragten zu bestellen, da die gesetzlichen Voraussetzungen hierfür nicht vorliegen.

Der Auftragnehmer verpflichtet sich dennoch, personenbezogene Daten ausschließlich im Rahmen der gesetzlichen Vorschriften zu verarbeiten und angemessene technische und organisatorische Maßnahmen zum Schutz der Daten zu treffen.

Sofern der Auftraggeber Fragen, Hinweise oder mögliche Datenschutzvorfälle feststellt, sind diese unverzüglich an den Auftragnehmer zu melden. Datenschutzbezogene Anfragen oder Hinweise können zentral an folgende Kontaktadresse gerichtet werden:

LCE Medical IT GmbH
E-Mail: info@lce-medical-it.de

Der Auftragnehmer wird eingehende datenschutzbezogene Anliegen prüfen und im Rahmen seiner Zuständigkeit angemessen bearbeiten bzw. – sofern erforderlich – an zuständige Stellen weiterleiten.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Anlage I].

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

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

f) Der Auftragnehmer unterstützt den Auftraggeber auch bei erforderlichen Datenschutz-Folgeabschätzungen.

g) Dem Auftragnehmer ist bekannt, dass der Auftraggeber Berufsgeheimnisträger ist und Verstöße dagegen nach § 203 StGB strafbewährt sind.

h) Der Auftragnehmer unterstützt den Auftraggeber bei allen gesetzlichen Informations- und Auskunftspflichten, die im Zusammenhang mit der Auftragsdatenverarbeitung stehen. Auskünfte an Betroffene oder Dritte darf der Auftragnehmer nur nach vorheriger Weisung des Auftraggebers erteilen. Soweit ein Betroffener seine Rechte nach den einschlägigen Datenschutzgesetzen unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten

i) Der Auftragnehmer sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der

Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

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

6. Unterauftragsverhältnisse

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

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.
Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

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

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

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

(6) Folgende Unterauftragnehmer wird zu diesem Vertrag benannt:
ptc premium technologies GmbH., Zwickauer Straße 16b, 09112 Chemnitz. Vertragliche Regelungen zum Datenschutz und Datensicherheit zwischen LCE Medical IT GmbH und Unterauftragnehmer sind vorhanden.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Der Auftraggeber hat das Recht, dem Auftragnehmer Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Grundsätzlich können Weisungen mündlich erteilt werden. Mündlich erteilte Weisungen sind zu dokumentieren. Weisungen sind schriftlich oder in Textform zu erteilen, wenn der Auftragnehmer dies verlangt.

(2) Der Auftragnehmer verarbeitet die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich nach den Weisungen des Auftraggebers und im Rahmen der getroffenen Vereinbarungen.

(3) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Vorschriften verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(4) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

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

(4) Dieser Vertrag zur Auftragsdatenverarbeitung ist vom Bestand des zugrundeliegenden Dienstleistungsvertrages abhängig. Endet der Dienstleistungsvertrag, so endet auch dieser darauf beruhende Vertrag zur Auftragsdatenverarbeitung, ohne dass es einer gesonderten Kündigung bedarf.

(5) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse über Personen, Geschäftsgeheimnisse und Datensicherheitsmaßnahmen auch nach Beendigung des Vertrages vertraulich zu behandeln.

11. Haftung/ Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vertragsregelung und all ihrer Bestandteile, einschließlich etwaiger Zusicherungen des Auftragsverarbeiters, bedürfen einer Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Vertragsregelung handelt.

(2) Sollten einzelne Teile dieser Vertragsregelung unwirksam sein, so berührt dies die Wirksamkeit der Vertragsregelung im Übrigen nicht. An Stelle der unwirksamen Bestimmung soll eine Bestimmung vereinbart werden, die dem von den Partnern hiermit verfolgten wirtschaftlichen Zweck möglichst nahekommt. Entsprechendes gilt im Falle einer Regelungslücke.

(3) Diese Vertragsregelung unterliegt ausschließlich dem formellen und materiellen Recht der Bundesrepublik Deutschland.

(4) Wird auf Art. 82 des aktuellen DSGVO wir verweisen.

(5) Die Vertragsparteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Vertragspartei vertraulich zu behandeln. Geschäftsgeheimnisse sind alle auf ein Unternehmen bezogene Tatsachen, Umstände und Vorgänge, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung der Geheimnisträger ein berechtigtes Interesse hat. Datensicherheitsmaßnahmen sind alle technischen und organisatorischen Sicherheitsmaßnahmen, die eine Partei nach den für den Auftraggeber einschlägigen Datenschutzgesetzen getroffen hat.
Diese Geheimhaltungspflicht besteht nach Beendigung dieses Vertrags fort.

(6) Sofern eine Vertragspartei weiteren Geheimnisschutzregeln unterliegt und sie dies der anderen Vertragspartei zu Vertragsbeginn schriftlich mitteilt, ist auch diese Vertragspartei verpflichtet, die Geheimnisschutzregeln zu beachten.

(7) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände des Auftraggebers ausgeschlossen.

12. Abschlusserklärung

……

……

……

……	……
Ort, Datum	Ort, Datum
……	……
Unterschrift/ Stempel Auftraggeber	Unterschrift/ Stempel Auftragnehmer

Anlagen:
Anlage I – Technisch organisatorische Maßnahmen (2 Seiten)

Anlage I – Technisch-organisatorische Maßnahmen

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

- **Zutrittskontrolle**

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen
- Schlüsselregelung/ Transpondersystem/ Schlüssel- / Sicherheitsschließanlage
- elektrische Türöffner (Haustür) / Tür mit Knauf an der Außenseite
- Alarmanlagen
- Absicherung von IT-Netzen durch Firewalls, Netzwerksegmetierung
- Backup
- Datentresor / Safe/Tresor

- **Zugangskontrolle**

Keine unbefugte Systembenutzung
- (sichere) Kennwörter /Log-in mit Benutzername und Passwort
- Verschlüsselung von Datenträgern (Backup, Serverdatenträger)

- **Zugriffskontrolle**

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems
- Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte
- Fernzugriff über TeamViewer die IP Adressen werden dazu verwendet
- Akten Schredder
- Verschließbarer Stahlschrank

- **Trennungskontrolle**

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden
- Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantennummern)

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

- **Weitergabekontrolle**

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport:
- Verschlüsselung von Übermittlungsgegenstand und Verbindung
- Virtual Private Networks (VPN)
- Applikationsmanagement (keine Adminrechte für Benutzer)
- Speichermedieneinsatz (HDD in Kopieren, Plottern)

- **Eingabekontrolle**

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind
- Protokollierung
- Dokumentenmanagement
- Verpflichtung auf das Datengeheimnis

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

- **Verfügbarkeitskontrolle**

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust:
- Backup-Strategie (online/offline; on-site/off-site)
- unterbrechungsfreie Stromversorgung (USV)
- Virenschutz
- Firewall
- Festplattenspiegelung
- Intrusion Detection System (IDS)
- Datensicherung (Räumliche Trennung von der Sicherungsquelle)
- CO2 Feuerlöscher in Serverräumlichkeiten

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

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

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);
- Auftragskontrolle

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.:
- o Eindeutige Vertragsgestaltung,
- o formalisiertes Auftragsmanagement,
- o strenge Auswahl des Dienstleisters,
- o Vorabüberzeugungspflicht,
- o Nachkontrollen

5. Organisatorische Maßnahmen

die durch Handlungsanweisung, Verfahrens- und Vorgehensweisen umgesetzten Maßnahmen des Datenschutzes

- Arbeitsanweisung zum Umgang mit fehlerhaften Druckerzeugnissen
- Verpflichtung auf das Datengeheimnis
- Meldewege und Notfallpläne
- Schlüsselregelung
- Schulungsplan
- Spamabwehr