Datenschutzvereinbarung zur Wartung und Support von INDICATION durch ET SOFTWARE Developments GmbH

- nachstehend „Vereinbarung“

zwischen

xxx - nachstehend „Auftraggeber“

und

ET Software Developments GmbH
Am Leimbachring 30
69207 Sandhausen

- nachstehend „Auftragnehmer“

Diese Datenschutzvereinbarung regelt den Schutz personenbezogener Daten bei der Datenverarbeitung durch den Auftragnehmer im Auftrag des Auftraggebers gemäß § 11 Bundesdatenschutzgesetz (BDSG).
Der Begriff der Verarbeitung schließt das Erheben, Verarbeiten, Verändern, Kopieren, Löschen und Nutzen von Daten sowie Wartungsaufgaben ein.

§ 1
Gegenstand und Dauer des Auftrags

1. Der Gegenstand des Auftrags zur Datenverarbeitung ist die Durchführung folgender Aufgaben durch den Auftragnehmer:
   - Fernwartung und Support für die Software INDICATION
   - Anwendersupport für die Software INDICATION

2. Der Auftrag ist unbefristet erteilt und kann von beiden Parteien schriftlich mit einer Kündigungsfrist von einer Woche gekündigt werden. Die Möglichkeit zur außerordentlichen fristlosen Kündigung bleibt hiervon unberührt.

§ 2
Umfang, Art, Zweck der vorgesehenen Verarbeitung; Art der Daten; Kreis der Betroffenen

1. Beschreibung des Auftragsgegenstandes im Hinblick auf Umfang, Art und Zweck der Erhebung, Verarbeitung und/oder Nutzung der personenbezogenen Daten durch den Auftragnehmer:
   - Visualisierung von der beim Auftraggeber installierten INDICATION Instanz und deren existierenden Auftraggeber-Daten durch ein Remote Desktop Tool (e.g. Teamviewer).

2. Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:
   - Auftraggeber Login und Profil-Daten
   - Patientenstammdaten
   - Patienten Abrechnungsdaten

- Medizinische Patientendaten

3. Kreis der Personen beim Auftragnehmer, die Zugriff auf Daten vom Auftraggeber bekommen:

   - Der Kreis, der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen, umfasst exklusiv die internen Mitarbeiter des Auftragnehmers. Diese Personen sind namentlich bekannt und sind zur Geheimhaltung Verpflichtet.

   - Der Auftragnehmer bekommt vom Auftraggeber für die Zeit der Remote-Wartung, bei Bedarf und auf der eigenen Initiative vom Auftraggeber, einen zeit-begrenzten Zugriff auf seinen in INDICATION gepflegten Daten.

   - Der Auftragsnehmer kann nicht auf die Daten vom Auftraggeber ohne seine aktive Zustimmung (Genehmigung am Bildschirm) am Anfang der Session zugreifen.

   - Beliebiger Zugang zu den Daten ist nach Beendigung der Remote-Wartung Session nicht mehr möglich. Ein neuer Zugrifft verlangt eine neue Remote-Wartung Session, und damit eine neue aktive Zustimmung vom Auftraggeber.

§ 3
Technische und organisatorische Maßnahmen nach § 9 BDSG

Der Auftragnehmer speichert in seinen Lokationen oder auf seiner Infrastruktur KEINE Daten vom Auftraggeber. Nicht desto trotz,

1. Der Auftragnehmer trifft die im Rahmen eines Sicherheitskonzeptes erforderlichen technischen und organisatorischen Datensicherheitsmaßnahmen, um den Datenschutz zu gewährleisten.

2. Das Sicherheitskonzept umfasst insbesondere folgende nach § 9 BDSG einschließlich Anlage erforderlichen technischen und organisatorischen Maßnahmen:

   a) Zutrittskontrolle zu technischen Anlagen,
   b) Zugangskontrolle (Passwort o.ä.),
   c) Zugriffskontrolle (autorisierte Personen erhalten Zugriff ausschließlich auf Daten, die erforderlich sind, um die ihnen übertragenen Aufgaben zu erfüllen),
   d) Weitergabe-/Transportkontrolle,
   e) Eingabekontrolle (wer führt welche Schritte aus),
   f) Auftragskontrolle,
   g) Verfügbarkeitskontrolle,
   h) Trennungsgebot (getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden).
   i) Maßnahmen im Hinblick auf die Art des Datenaustauschs / Bereitstellung von Daten, Art/Umstände der Verarbeitung/der Datenhaltung und Art/Umstände beim Output/Versand

Die erforderlichen Maßnahmen seitens Auftragnehmers ergeben sich aus den Datenschutz- und Sicherheitskonzept-Maßnahmen im Einsatz bei dem Auftragnehmer.

3. Der Auftragnehmer ist verpflichtet, die technischen und organisatorischen Maßnahmen zukünftig in der erforderlichen Art und Weise gemäß dem technischen Fortschritt sowie dem gesetzlichen Mindeststandard anzupassen und einzuhalten. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen sowie der gesetzlichen Mindestanforderungen nicht unterschritten werden. Der Auftragnehmer hat auf Anforderung die Angaben nach § 4g Abs. 2 S. 1 BDSG dem Auftraggeber zur Verfügung zu stellen.

§ 4
Berichtigung, Löschung und Sperrung von Daten

Der Auftragnehmer hat nur nach schriftlicher Weisung (auch per E-Mail) des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

Es ist sonst im Rahmen von einer Remote-Wartung Session NICHT vorgesehen, dass der Auftragnehmer Daten von dem Auftraggeber erfasst, verändert oder löscht.

§ 5
Pflichten, insbesondere Kontrollen des Auftragnehmers

Durch eine Remote-Wartung werden keine Daten vom Auftraggeber zu dem Auftragnehmer transferiert oder anders als Sicht per Remote-Bildschirm übertragen.
Nicht desto trotzt,

1. Eine Verwendung der Daten für andere Zwecke als in dieser Vereinbarung vorgesehen, einschließlich eigener Zwecke des Auftragnehmers, ist nicht gestattet. Der Auftragnehmer wird ohne Wissen des Auftraggebers keine Kopien oder Duplikate erstellen, es sei denn, es handelt sich um Sicherheitskopien oder Daten, deren Aufbewahrung gesetzlich vorgeschrieben ist.

2. Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags nach § 11 Abs. 4 BDSG folgende Pflichten:

   a) Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten, der seine Tätigkeit gemäß §§ 4f, 4g BDSG ausüben kann. Die Kontaktdaten dieses Datenschutzbeauftragten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.

   b) Die Wahrung des Datengeheimnisses gemäß § 5 BDSG. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.

   c) Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend § 9 BDSG und Anlage.

   d) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach § 38 BDSG . Dies gilt auch, soweit eine zuständige Behörde nach §§ 43, 44 BDSG beim Auftragnehmer ermittelt.

e) Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.

f) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) vorlegen.

§ 6
Unterauftragsverhältnisse

1. Unteraufträge dürfen vom Auftragnehmer (und Unterauftraggeber) an den Unterauftragnehmer nur mit vorheriger schriftlicher Einwilligung des Auftraggebers erteilt werden.

2. Die vertraglichen Vereinbarungen zwischen Auftragnehmer und Unterauftragnehmer sind so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen. Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrecht entsprechend dieser Vereinbarung und des § 11 BDSG i.V.m. Nr. 6 der Anlage zu § 9 BDSG beim Unterauftragnehmer einzuräumen.

3. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt (z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte). Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

§ 7
Kontrollrechte des Auftraggebers

1. Der Auftraggeber hat das Recht, die in Nr. 6 der Anlage zu § 9 BDSG vorgesehene Auftragskontrolle durchzuführen. Dabei ist der Auftragnehmer verpflichtet, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu geben oder entsprechende Nachweise verfügbar zu machen.

2. Der Auftraggeber wird sich vor Beginn der Datenverarbeitung und sodann in regelmäßigen Abständen von der Einhaltung der gemäß § 3 dieser Vereinbarung getroffenen Maßnahmen überzeugen und das Ergebnis dokumentieren. Der Auftragnehmer unterstützt die hierzu erforderlichen Maßnahmen des Auftraggebers, indem er ihm die Umsetzung dieser Maßnahmen nachweist.

§ 8
Mitteilung von Verstößen durch den Auftragnehmer

1. Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Regelungen vorgefallen sind.

2. Es ist bekannt, dass nach § 42a BDSG Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber Pflichten nach § 42a BDSG treffen, hat der Auftragnehmer ihn hierbei zu unterstützen.

§ 9
Umfang der Weisungsbefugnis des Auftraggebers

1. Der Auftragnehmer verpflichtet sich, die anvertrauten Informationen nur gemäß dieser Vereinbarung und entsprechend den Weisungen des Auftraggebers zu verarbeiten. Das Weisungsrecht des Auftraggebers über Art, Umfang und Verfahren der Datenverarbeitung ist im Rahmen dieser Vereinbarung umfassend.

2. Weisungen sind schriftlich (auch per E-Mail) zu erteilen.

3. Ist der Auftragnehmer der Ansicht, eine Weisung des Auftraggebers verstoße gegen datenschutzrechtliche Vorschriften, so hat er den Auftraggeber unverzüglich hierauf hinzuweisen. Die Ausführung der entsprechenden Weisung ist solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

§ 10
Löschung von Daten und Rückgabe von Datenträgern

Der Auftragnehmer speichert bei sich KEINE Auftraggeber Daten. Nicht desto trotz:

1. Unverzüglich nach Beendigung des Auftrags gemäß § 1 Abs. 2 oder früher nach Aufforderung durch den Auftraggeber hat der Auftragnehmer alle in seinen Besitz gelangten Unterlagen, überlassenes Datenmaterial und erstellte Verarbeitungsergebnisse einschließlich möglicher Zwischenergebnisse unaufgefordert dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten.

2. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

3. Dem Auftragnehmer steht kein Zurückbehaltungsrecht an den vorgenannten Unterlagen, Informationen und Ergebnissen zu.

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

§ 11
Anwendbares Recht, Gerichtsstand und Schlussbestimmungen

1. Auf diese Vereinbarung findet das Recht der Bundesrepublik Deutschland Anwendung (mit Ausnahme der internationalen Kollisionsregeln und des UN-Kaufrechts). Soweit gesetzlich zulässig, vereinbaren die Parteien Frankfurt am Main als Gerichtsstand für alle Streitigkeiten aus dieser Vereinbarung.

2. Der Auftragnehmer kann Rechte und Ansprüche aus dieser Vereinbarung nicht – auch nicht teilweise – abtreten, ohne die vorherige schriftliche Zustimmung des Auftraggebers zu erhalten.

3. Dies stellt den vollständigen Text der Datenschutzvereinbarung dar. Mündliche Nebenabreden sind nicht geschlossen. Änderungen dieser Datenschutzvereinbarung bedürfen der Schriftform; dies gilt auch für die Änderung des Schriftformerfordernisses.

4. Im Falle der Unwirksamkeit einzelner Klauseln des vorliegenden Vertrages verpflichten sich die Parteien, eine dem Verwendungszweck angemessene und interessengerechte Ersatzbestimmung auszuhandeln.

5. Soweit nicht anders in dieser Vereinbarung vorgesehen, bleiben andere vertragliche Beziehungen zwischen den Parteien unberührt.

Unterschriften:

Für Auftraggeber	**Für Auftragnehmer**
_____, _____	_____, _____
(Ort) (Datum)	(Ort) (Datum)
_____	_____
……..	……
_____	_____
……..	……..

Hinweise zu den allgemeinen technischen und organisatorischen Maßnahmen nach § 3 der Datenschutzvereinbarung

1. Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

Beispiele

- ⇨ Zutrittskontrollsystem,
  Ausweisleser, Magnetkarte, Chipkarte → zu beachten: § 6c BDSG
- ⇨ Schlüssel / Schlüsselvergabe
- ⇨ Türsicherung (elektrische Türöffner usw.)
- ⇨ Werkschutz, Pförtner
- ⇨ Überwachungseinrichtung
  Alarmanlage, Video- / Fernsehmonitor

2. Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.

Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

Beispiele

- ⇨ Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- ⇨ Automatische Sperrung (z.B. Kennwort oder Pausenschaltung)
- ⇨ Einrichtung eines Benutzerstammsatzes pro User
- ⇨ Verschlüsselung von Datenträgern

3. Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

Beispiele

⇨ Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)

⇨ Auswertungen

⇨ Kenntnisnahme

⇨ Veränderung

⇨ Löschung

4. Weitergabekontrolle

Aspekte der Weitergabe personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle ...

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

Beispiele

⇨ Verschlüsselung / Tunnelverbindung (VPN = Virtual Private Network)

⇨ Elektronische Signatur

⇨ Protokollierung

⇨ Transportsicherung

5. Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

Beispiel

⇨ Protokollierungs- und Protokollauswertungssysteme

6. Auftragskontrolle

Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten.

Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:

Beispiele

⇨ Eindeutige Vertragsgestaltung

⇨ Formalisierte Auftragserteilung (Auftragsformular)

⇨ Kriterien zur Auswahl des Auftragnehmers

⇨ Kontrolle der Vertragsausführung

7. Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Maßnahmen zur Datensicherung (physikalisch / logisch):

Beispiele

- ⇨ Backup-Verfahren
- ⇨ Spiegeln von Festplatten, z.B. RAID-Verfahren
- ⇨ Unterbrechungsfreie Stromversorgung (USV)
- ⇨ Getrennte Aufbewahrung
- ⇨ Virenschutz / Firewall
- ⇨ Notfallplan

8. Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

Beispiele

- ⇨ "Interne Mandantenfähigkeit" / Zweckbindung
- ⇨ Funktionstrennung /Produktion / Test)