Remotezugriffsvereibarung

Als Anlage zum Hauptvertrag (Kauf, Lizenzierung und Wartung) und Nebenvertrag (Auftragsdatenverarbeitung inkl. Technisch-organisatorischer Maßnahmen TOMs) schließen die Vertragsparteien für ihre Nutzer eine Remotezugriffsvereinbarung

Zwischen

(# Anzeigen Stammdaten ärztlich und oder zahnärztlich)

_____

(im folgenden „Auftraggeber“)

und

Crosssoft GmbH

Knooper Weg 126/128

24105 Kiel

_____

(im folgenden Auftragnehmer)

Wird der Remotezugriff wie folgt beschrieben:

§1 Beschreibung Remotezugriff

1 Der Auftragnehmer liefert dem Auftraggeber in der Software eingegliedert eine Fernwartungs-Software die sie gemeinsam nutzen können.

2 Die Auswahl der Lösung liegt beim Auftragnehmer, der sich auf Grund der in Deutschland erstellten und auf Grundlage der ISO 27001 auditiertem Software für TeamViewer als Mitglied der Allianz für Cyber-Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entschieden hat. TeamViewer ist durch Ende-zu-Ende-256-Bit-AES-Verschlüsselung, Zwei-Faktor-Authentifizierung und andere branchenkonforme Sicherheitsfunktionen, wie Conditional Access, SSO und viele weitere, geschützt und gemäß KRITIS nutzbar. Die TeamViewer Sicherheitsbulletins sind für die Nutzer zugänglich: https://www.teamviewer.com/de/trust-center/sicherheitsbulletins/

3 Der Remotezugriff wird mit dem Ziel vereinbart, dem Auftragnehmer zu ermöglichen, von seinem Firmenstandort aus die mit dem Hauptvertrag vereinbarten Maßnahmen im gemeinsamen Interesse effizient durchführen und/ oder Systemstörungen bzw. Ausfälle unterschiedlicher Kritikalität zeitnah und im Rahmen der vereinbarten Service Level auf Basis der DSVGO beheben zu können.

4 Der Remotezugriff ermöglicht dem Auftragnehmer über die Remotelösung im Detail…

- …fachliche Verbesserungen und Erweiterungen der CROSSSOFT-Systeme ohne Zeitverlust aufzuspielen,

- …Leistungen aus den vertraglichen Regelungen zur Pflege und Aufrechterhaltung bzw. Wiederherstellung seiner Betriebsbereitschaft zu erbringen,
- …die Entstörung aller CROSSSOFT-Systeme durchzuführen
- …die Experten des Auftraggebers bei Fehleranalysen und Fehlerbehebungen zu unterstützen
- … die Administrationsaufgaben des Auftraggebers in den CROSSSOFT-Systemen zu unterstützen.

5 Jedwede Änderung des mit diesem Vertrag vereinbarten Verarbeitungsgegenstandes, von Verfahrensänderungen oder eingesetzter Verarbeitungsmethoden ist schriftlich zu vereinbaren.

6 Die Kosten des Remotezugriffs sind in den Vergütungs- und/oder Gewährleistungs-vereinbarungen werden im Hauptvertrages geregelt.

7 Sollte aus betriebsinternen Gründen des Auftragsgebers die Einrichtung nach §1 Abs 2 nicht gegeben sein, stellt der Auftraggeber einen VPN-Zugang zur Verfügung, so dass der Auftragnehmer gemäß RDP einen Zugriff realisieren kann.

§ 2 Ablauf der Kommunikation

1 Auftraggeber und Auftragnehmer klären vor einem beabsichtigten Remotezugriff des Auftragnehmers telefonisch Notwendigkeit und Zweck und Umfang der geplanten Maß-nahmen.

2 Die Zugriffsprotokollierung

Der Auftraggeber wird daraufhin den Zugriff freischalten, indem er eine Wartungssession zur Verfügung stellt, auf die sich der Auftragnehmer per Webmeeting aufschalten kann. Diese Zugriffe können vom Auftraggeber aufgezeichnet werden. Dadurch können alle Aktionen der Remotewartung nachvollzogen werden. Dies kann in Echtzeit erfolgen (Vieraugenprinzip).

3 Die Aufzeichnungsdaten werden durch den Auftraggeber für sechs Monate gespeichert und können innerhalb dieses Zeitraums überprüft werden.

4 Nach Beendigung der Aktivitäten wird die Verbindung vom Auftragnehmer wieder getrennt.

§ 3 Pflichten des Auftraggebers

1 Der Auftraggeber sorgt für die technische Einrichtung und Erreichbarkeit des Remotezugangs und trägt hierfür, sowie für die Remotezugriffe alle bei ihm entstehenden Kosten.

2 Er sorgt durch technische Maßnahmen oder entsprechende Zugangsrechte und -sicherungen für eine ausreichende Abschottung des Remotegriffs auf die Service-relevanten Bereiche und Rechner.

3 Er bleibt verantwortlich für die Beurteilung der Zulässigkeit des Remotezugriffs und die Wahrung der Rechte etwaiger Betroffener.

4 Er sorgt für die Einhaltung der ihn treffenden Verpflichtungen zum Datenschutz und holt vor dem Remotezugriff eventuell erforderliche Zustimmungen ein.

5 Insbesondere zur Wahrung des Datenschutzes hat er das Recht, Weisungen über Art, Umfang und Ablauf der Remotewartung zu erteilen. Der Auftraggeber benennt zu diesem Zweck gegenüber dem Auftragnehmer weisungsbefugte Personen (KEY-USER).

Im Falle von Wechseln oder länger andauernder Verhinderung der genannten Person(en) sind seitens des Auftraggebers umgehend Nachfolger oder Vertreter zu benennen.

§ 4 Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich,

1 für die Remotewartung aufgrund der Sensibilität der beim Auftraggeber ggf. vorzufindenden Daten ausschließlich festangestellte und entsprechend geschulte Mitarbeiter einzusetzen,

2 die Remotewartung nur zu den unter § 1 beschriebenen Zwecken aus eigenen Betriebsstätten heraus zu betreiben und dabei den unter § 2 beschriebenen Ablauf einzuhalten,

3 den Remotezugriff nach dem aktuellen Stand der Wissenschaft und Technik gegen Einsichtnahme oder Angriffe Dritter zu schützen, insbesondere die Datenübertragung zu verschlüsseln und die zugriffsberechtigten Mitarbeiter zu authentisieren,

4 für die Sicherheit verarbeiteter Daten relevante Entscheidungen zur Organisation der Datenverarbeitung und hierzu angewandten Verfahren im Vorfeld mit dem Auftraggeber abzustimmen,

5 Weisungen des Auftraggebers zum Umgang mit Daten sowie zu technischen und organisatorischen Maßnahmen umgehend und vollständig zu befolgen, soweit diese mit Rücksicht auf die besondere Sensibilität verarbeiteter Daten in einem angemessenen Verhältnis zu dem hieraus resultierenden Aufwand stehen,

6 den Auftraggeber im Falle zu Tage tretender Unregelmäßigkeiten oder anderer Sachverhalte, die Vorschriften des Datenschutzes verletzen, insbesondere über solche, die einen Datenzugriff durch hierzu unbefugte Dritte ermöglichen können, unverzüglich zu informieren,

7 die Remotewartung so weit wie möglich ohne gleichzeitige Speicherung der am Diagnose-System sichtbaren Daten vorzunehmen; diese Daten bei entsprechender Notwendigkeit nur temporär und für die Dauer ihrer Notwendigkeit zu speichern,

8 nach Abschluss der vertraglich geschuldeten Arbeiten gespeicherte Daten, erstellte Verarbeitungs- und/oder Nutzungsergebnisse und über die Vertragsdurchführung erlangte Ergebnisse dem Auftraggeber mitzuteilen. Datenträger des Auftragnehmers sind nach vorangegangener Zustimmung des Auftraggebers in Datenschutz gerechterweise zu löschen bzw. zu vernichten,

9 beim Auftragnehmer gespeicherte Daten des Auftraggebers gesondert und physisch getrennt von anderen Datenbeständen des Auftragnehmers oder Dritter aufzubewahren,

10 alle im Rahmen der Vertragsdurchführung erlangten Kenntnisse von vertraulichen Informationen, Geschäftsgeheimnisse, Datensicherheitsmaßnahmen sowie gespeicherte Daten des Auftraggebers geheim zu halten und in keinem Fall an Dritte weiterzugeben,

11 alle beteiligten Mitarbeiter zur Einhaltung der vorstehenden Geheimhaltung zu verpflichten;

12 Ohne schriftliche Genehmigung des Auftraggebers keine Unterauftragnehmer für den Gegenstand dieser Vereinbarung einzusetzen.

§ 6 Datengeheimnis

1 Der Auftragnehmer verpflichtet sich, das Datengeheimnis zu wahren, die im Rahmen dieses Vertrages eingesetzten Mitarbeiter zuvor mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut zu machen und auf das Datengeheimnis gemäß Art. 28 Abs. 3 Satz 2 DSGVO schriftlich zu verpflichten.

2 Sollte der Auftraggeber unter den Schutz des Kirchendatenrechts fallen, unterwirft sich der Auftragnehmer zur Auftragsverarbeitung gemäß Art 28 EU-DSVGO der kirchlichen Datenschutzaufsicht gemäß §30 Abs. 5 Kirchengesetz der entsprechenden Regelungen.

3 Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind und er sie im Rahmen dieses Vertrages geflissentlich befolgen wird. Er wird die Einhaltung der datenschutzrechtlichen Vorschriften durch seine Mitarbeiter in geeigneter Form und Frequenz überwachen.

4 Der Auftragnehmer darf gegenüber Dritten keinerlei Auskünfte über Umfang und Zweck dieser Vereinbarung sowie hiermit in Zusammenhang erlangte Kenntnisse erteilen. Gegenüber dem Auftraggeber dürfen seitens des Auftragnehmers Auskünfte nur den hier-zu seitens des Auftraggebers benannten und autorisierten Personen erteilt werden (§ 4 Abs. 4 dieser Vereinbarung).

§ 7 Kontrollrechte

1 Der Auftraggeber hat das Recht, einen laufenden Remotezugriff zu jedem Zeitpunkt zu unterbrechen, wenn er den Eindruck gewinnt, dass unbefugt auf Daten, Dateien oder Systeme zugegriffen wird.

2 Der Auftraggeber kann sich zu Prüfzwecken in den Betriebsstätten des Auftragnehmers zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Vertragsdurchführung einschlägigen Datenschutzgesetze überzeugen. Dem Auftraggeber ist ferner auf Verlangen Einsicht in sämtliche Unterlagen und Dateien des Auftragnehmers zu gewähren, die mit der Durchführung der auf Grundlage dieser Vereinbarung erfolgenden Fernwartung in Zusammenhang stehen.

§ 8 Technische und organisatorische Maßnahmen

Um die Sicherheit der Datenübertragung zu gewährleisten und unbefugte Zugriffe auf Datenbestände des Auftraggebers im Rahmen des Remotezugriffs zu verhindern, wer-den seitens des Auftraggebers die folgenden - weiter unten beschriebenen - technischen und organisatorischen Maßnahmen verbindlich festgelegt.

Die innerbetriebliche Organisation ist so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dies wird durch die folgenden Maßnahmen sichergestellt:

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

- Zutrittskontrolle:

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

Dies wird durch die folgenden Maßnahmen sichergestellt:

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene, Sozial- und Gesundheitsdaten verarbeitet werden, verwehrt. Dies wird durch eine Zugangskontrolle und Videoüberwachung der Innen und Außenbereiche sichergestellt.

Die Fa. CROSSSOFT. setzt eine elektronische Zugangskontrolle der Fa. Simons Voss, Unterföhring, ein. Das Zugangskontrollsystem verhindert, dass Unbefugte Zutritt zu Räumen, Unterlagen und Datenverarbeitungsanlagen erhalten und Zugriff auf Daten erlangen können. Der digitale Schließzylinder 3061 protokolliert neben Öffnen und Schließen eine Vielzahl intelligenter Funktionen wie Zutrittskontrolle mit Protokollierung, Zeitzonensteuerung, Event-Management und Türüberwa-chung. Der digitale Schließzylinder 3061 wird mit aktiven Identifikationsmedien (Transpondern), welche jedem Mitarbeiter persönlich ausgehändigt wurden, betrieben.

Zu den Serverräumen haben nur Administratoren und Geschäftsführer über einen Token Zugang. Zu- und Austritt werden protokolliert.

- Zugangskontrolle

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

Dies wird durch die folgenden Maßnahmen sichergestellt:

Die Zugangs-Autorisierung passiert über Abfragen von Benutzerkennungen gegen das Aktive Directory via LDAP.

- Zugriffskontrolle:

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

Dies wird durch die folgenden Maßnahmen sichergestellt:

Die Benutzung von Datenverarbeitungsanlagen der CROSSSOFT. wird durch ein Rechte- und Rollenkonzept sichergestellt. Unterschieden werden Rechte für Administratoren, Entwickler, Autoren, Support- und Vertriebs-Mitarbeiter.

Es wird überwacht, dass Berechtigte ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass Daten bei der Verarbeitung, Nutzung und nach einer etwaigen Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Die Administration erfolgt im Vier-Augenprinzip durch die Geschäftsführung. Die Rolle des Administrators hat keinen Zugriff auf die Daten sondern nur auf die Administration.

- Trennungskontrolle

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

Dies wird durch die folgenden Maßnahmen sichergestellt:

Auf einem Unix-System jeweils in Kiel und in Zapfendorf passiert die Datenhaltung geclustert. Mandantenfähigkeit und Sandboxen wird gewährleistet bzw. ist vor-handen. Jeder Mandant wird in einem getrennten System verwaltet. Alle Mandantenprojekte werden regelmäßig gesichert.

- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen;

Dies wird durch die folgenden Maßnahmen sichergestellt:

Es findet keine weitere Pseudonymisierung von Testdaten der KVB statt.

Siehe auch Auftragsdatenvereinbarung zwischen Fa. Crosssoft und KVB zur bestehenden Leistungsvereinbarung.

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

- Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

Dies wird durch folgende Maßnahmen sichergestellt:

Datenbewegungen werden überprüft durch das verpflichtende Ein- und Aus-checken von Daten mit entsprechender Protokollierung.

Transportverschlüsselung wird über HTTPS sichergestellt.

Daten-Verschlüsselung in der Sandbox wird auf Wunsch des Auftraggebers über Public-Key-Verfahren eingesetzt.

- Eingabekontrolle

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

Dies wird durch folgende Maßnahmen sichergestellt:

Es ist gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme ein-gegeben, verändert oder entfernt worden sind.

Check-IN jeglicher Daten (Software, Konzepte, Testdaten), die in den mandantenfähigen Jail-Systemen dauerhaft zur Verfügung gestellt werden. Das Vorgehen entspricht einer impliziten Protokollierung.

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

- Verfügbarkeitskontrolle

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

Dies wird durch folgende Maßnahmen sichergestellt:

Es findet eine redundante Datenhaltung an den Standorten Kiel und Zapfendorf statt. Die beiden Systeme synchronisieren sich gegenseitig.

Ein Wartungssystem analysiert automatisch und gibt Meldung welche System-Bausteine in welchen Intervallen ausgetauscht werden müssen.

Eine Datenhaltung findet nicht in einer Cloud oder bei einem Internet-Provider statt. Es gibt feste IP-Adressen zu Cloud-Servern, die Clouds sind aber leer. Die IP-Adressen werden nur als Zugang zur Sandbox benötigt.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Datenschutz-Management;
- Incident-Response-Management;

- Auftragskontrolle

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

Dies wird durch folgende Maßnahmen sichergestellt:

Es ist sichergestellt, dass von diesem Vertrag betroffene Daten nur entsprechend der Weisungen des Auftraggebers verarbeitet werden können. Dies wird durch technische Maßnahmen wie das Ein- und Aus-Checken von Daten und organisatorische Maßnahmen wie eine Einweisung durch den Daten-schutzbeauftragten sichergestellt.

Mitarbeiter unterschreiben mit dem Arbeitsvertrag eine Verpflichtung zum Datengeheimnis und die Zustimmung zur Überwachung und Protokollierung. Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen (Datengeheimnis). Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

Siehe auch Auftragsdatenvereinbarung zwischen Fa. Crosssoft und KVB,

Die technischen und organisatorischen Maßnahmen können seitens des Auftraggebers einseitig im Laufe des Vertragsverhältnisses an die technische und/oder organisatorische Weiterentwicklung angepasst werden. Wesentliche Änderungen sind schriftlich zu vereinbaren.

Soweit die beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen den Anforderungen des Auftraggebers nicht genügen oder unvorhergesehen vom vereinbarten Standard abweichen sollen, hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

§ 9 Ende der Vereinbarung

Die Parteien können diese Vereinbarung jederzeit widerrufen, sofern dieses im Haupt-vertrag nicht anders vereinbart wurde. Im Übrigen endet diese Vereinbarung jeweils mit der Beendigung des Hauptvertrages. Die Verpflichtung des Auftragnehmers zur Einhaltung des mit diesem Vertrag vereinbarten Datengeheimnisses bleibt vom Ende dieser Vereinbarung unberührt und gilt unbeschränkt fort.

§ 10 Haftung

(1) Diese Vereinbarung dient allein dazu, dem Auftragnehmer den Remotezugriff auf Systeme des Auftraggebers zu gestatten. Die Haftung für eine durch Remotezugriff er-brachte Dienstleistung richtet sich nach den Bedingungen des jeweiligen Hauptvertrages. Soweit der Auftraggeber einen Schaden aufgrund eines Remotezugriffs geltend macht, trägt er die Beweislast für dessen Verursachung im Rahmen des Remotezugriffs.

§ 11 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrages bedürfen zu ihrer Wirksamkeit der Schriftform. Die Schriftform ist durch die Verwendung von E-Mails nicht gewahrt.

(2) Sollte eine Bestimmung dieses Vertrages ganz oder teilweise unwirksam sein, so wird dadurch die Wirksamkeit des übrigen Vertrages nicht berührt. Die Vertragspartner wer-den in diesem Fall eine Vereinbarung treffen, die dem wirtschaftlichen Zweck der Bestimmung in rechtlich zulässiger Weise am nächsten kommt.

(3) Gerichtsstand ist München. Für die vertraglichen Beziehungen gilt deutsches Recht.

(4) Im Übrigen gelten die Regelungen des jeweiligen Hauptvertrages.