Anwender-Informationen für den Betrieb der ALBIS Praxiscomputer der DOS GmbH

Stand: April 2016

Hinweis: Die „DOS GmbH“, im folgenen „DOS“ genannt, ist ein Vertriebs- und Servicepartner der CompuGroup Medical Deutschland AG (Geschäftsbereich ALBIS).

Impressum

Diese Information dient den Anwendern von Praxiscomputer-Anlagen, die durch die DOS GmbH Berlin installiert und betreut werden.

Herausgeber: DOS GmbH
Erbacher Straße 3 a
14193 Berlin-Grunewald
Telefon: 030 8099 710

Verantwortlich: Dipl.-Ing. Rainer Ludewig

für die Arzt-Praxis

Lieber Anwender,

als Betreiber eines Praxiscomputers können Sie zum kostengünstigen und reibungslosen Betrieb Ihrer Anlage viel beitragen. Die vorliegende Schrift soll Ihnen die notwendigen Informationen vermitteln. Bitte lesen Sie die Ausführungen sorgfältig durch und integrieren Sie geeignete Vorschläge in Ihren Praxisablauf und ggf. in Ihr Qualitätsmanagement.

Diese Anwender-Information wurde mit dem Betreiber der Anlage oder einem Vertreter besprochen, offene Fragen geklärt und ausgehändigt.

Berlin, den . . . . . Unterschrift Mitarbeiter DOS GmbH: . . . . . .

Abnahme der Anlage oder deren Erweiterung

Zunächst wünschen wir Ihnen viel Erfolg und Freude an der neuen Anlage oder deren Erweiterung. Bitte testen Sie die neuen Geräte und Installationen zusammen mit unserem Mitarbeiter und überzeugen Sie sich davon, dass alles nach Ihren Wünschen eingerichtet ist. Es gibt möglicherweise Details, die nur Sie wissen. Die folgende Checkliste soll Ihnen dabei helfen:

a) Sind alle Geräte laut Lieferschein vorhanden?

b) Sind Standorte und Positionierung in Ordnung?

c) Ist die gewünschte Software auf den Arbeitsplätzen installiert?

d) Liegen die Lizenzen (CD, Lizenzcode o.a.) zur Software vor?
Bitte bewahren Sie diese Lizenzen sorgfältig auf. Nur mit dem Besitz der Lizenz sind Sie rechtmäßiger Eigentümer der Software. Die Lizenz wird benötigt, wenn beispielsweise nach einer Festplattenreparatur, die Software erneut installiert werden soll.

e) Sind die Drucker bedarfsgerecht eingerichtet?

f) Werden außer den ALBIS-Daten alle weiteren notwendigen Daten gesichert?

g) Ist ein Virenschutz notwendig bzw. installiert?

h) Wissen Sie wie die Datensicherung funktioniert und kontrolliert wird?

i) Wissen Sie wie die USV funktioniert und kontrolliert wird?

j) Wissen Sie wie man die Anlage startet und herunterfährt?

k) Notieren Sie sich bitte die Standorte der Switches (Netzverteiler) und Router!

l) Bitte notieren Sie alle weiteren Wünsche zusammen mit dem Mitarbeiter.

m) Bitte unterzeichen Sie den Lieferschein und den Servicebericht.

Maßnahmen zur Betriebssicherheit

Ihre Anlage wird Sie in der täglichen Arbeit sehr unterstützen und Ihre Praxis wird in gewisser Weise von der einwandfreien Funktion abhängig sein. Bitte beachten Sie die folgenden Regeln:

a) Machen Sie täglich eine Datensicherung und prüfen Sie diese (siehe Seite 6)!

b) Achten Sie darauf, ob Kabelverbindungen in den Arbeitsbereich gelangen und Belastungen ausgesetzt sind. Häufig sind Kabel nach dem Einsatz der Reinigungskraft lose.

c) Achten Sie darauf, dass die Anlage ordnungsgemäß heruntergefahren wird.

d) Sorgen Sie für einen verantwortlichen Ansprechpartner für die EDV in der Praxis und klären Sie die Verantwortlichkeiten.

e) Sorgen Sie dafür, dass keine unsachgemäßen Änderungen an der Anlagenkonfiguration vorgenommen werden oder unkontrolliert Daten oder Programme installiert werden.

f) Nehmen Sie einmal jährlich den von uns angebotenen „Frühjahrsputz“ in Anspruch oder sorgen Sie für eine vergleichbare Leistung durch Ihren EDV-Betreuer.

g) Achten Sie auf eine einwandfreie Elektroinstallation. Vermeiden Sie mehrfach geschachtelte Steckdosenleisten und tauschen Sie defekte Anschlüsse aus.

h) Achten Sie darauf, dass die Geräte gut „durchatmen“ können. Ein freier Luftstrom ist bei den heutigen Computern überlebenswichtig.

i) Halten Sie einen „Plan B“ für einen plötzlichen Ausfall der EDV-Anlage bereit. Rechnen Sie damit, dass eine Reparatur einen Arbeitstag oder mehr dauern kann.

j) Halten Sie regelmäßig eine aktuelle Datensicherung außerhalb der Praxisräume bereit.

k) Halten Sie Ersatz-Tastaturen und Ersatz-Mäuse vor.

l) Um die Ausfallsicherheit zu erhöhen, können beispielsweise unterbrechungsfreie Stromversorgungen, Spiegelplatten-Systeme und Reserve-Systeme helfen. Denken Sie aber an eine Kosten/Nutzen Analyse. Wir beraten Sie gern!

m) Alle Daten die von außen ins System kommen können Viren enthalten. Datenträger (z.B. CD's, DVD's, USB-Sticks und USB-Festplatten) sollten vor dem Einsatz mit einem Virenscanner getestet werden.

n) Treffen Sie Maßnahmen zum Schutz gegen Diebstahl und Einbruch, sowie Wasser- und Brandschäden. Prüfen Sie ihre entsprechenden Versicherungen auf ausreichende Deckung.

o) Um Sie über die in den Wartungsverträgen der CompuGroup Medical Deutschland AG vereinbarten Leistungen hinaus unterstützen zu können, bieten wir seit 2014 unseren **DOS BASIS-Wartungsvertrag** für nur 12€ monatlich (incl. MwSt.) an. Bitte vereinbaren Sie mit uns diese für Sie wichtige und wirtschaftliche Unterstützung. Sie sparen damit Gebühren für Einwahlen und Beratungen. Wir beraten Sie gern über diesen Wartungsvertrag.

p) In unserem **DOS PREMIUM-Wartungsvertrag** sind neben dem „Frühjahrsputz" eine Vielzahl von Leistungen enthalten, die der Betriebssicherheit auf wirtschaftliche Weise dienen. Lassen Sie sich für Ihre Anlage ein Angebot machen!
Für eine Dreiplatzanlage kostet die PREMIUM-Wartung nur 63€ monatlich zzgl. MwSt.!

Die Datensicherung

Die in Ihrer Anlage gespeicherten Daten stellen einen großen Wert dar, der bei Verlust existenzbedrohend sein kann. Datensicherung und Aufbewahrung ist Chefsache! Folgende Regeln sollten Sie beachten:

a) Machen Sie unbedingt täglich eine Datensicherung, für jeden Wochentag auf einen anderen Datenträger (Generationenprinzip).

b) Machen Sie nach jeder Quartalsabrechnung vor der Archivierung eine Sicherung, die Sie an einem sicheren Ort (nicht in der Praxis) aufbewahren. Die KV geht von einer Aufbewahrungsdauer von 10 Jahren aus. Achten Sie bei Innovationen darauf, dass die Datenträger noch verarbeitet werden können.

c) Achten Sie auf qualitativ hochwertige Datenträger. Die Haltbarkeit ist begrenzt. Auskünfte erhalten Sie beim Hersteller. Gehen Sie bei CD und DVD von ca. 3 Jahren aus. Die Hersteller geben oft nur eine Lebensdauer für das Material und nicht für die Daten an. Langzeithaltbarkeiten sind bisher nicht erwiesen!

d) Lesen Sie regelmäßig die Protokolle des Sicherungsprogrammes! Nur so können Sie bemerken, wenn die Daten nicht oder nur fehlerhaft gesichert werden.

e) Lassen Sie ca. einmal im Jahr den Datenträger auf Lesbarkeit und Vollständigkeit prüfen. Wir machen dies im Rahmen des „Frühjahrsputzes“.

f) Bewahren Sie die Sicherung getrennt von der Anlage auf. Bei Einbruch, Feuer, Wasserschäden usw. ist die Datensicherung oft die einzige Möglichkeit den Praxisbetrieb wiederherzustellen.

g) In den meisten Fällen funktioniert die Datensicherung nur dann korrekt, wenn alle die Programme verlassen haben. Besprechen Sie dies mit Ihrem Betreuer und stellen Sie sicher, dass Ihr Personal damit vertraut ist.

h) Achten Sie darauf, dass auch alle wichtigen Daten außerhalb der ALBIS (Texte, Tabellen u.a.) gesichert werden! Denken Sie bei Erweiterungen (LZ-EKG, LZ-RR, Spiro usw.) an die Sicherung der aufgezeichneten Daten.

i) Wenn Sie viele Programme auf Ihrem Server installiert haben, ist eine Image-Sicherung der Serverfestplatte, zur schnellen Wiederherstellung bei Ausfall, sehr ratsam.

j) Machen Sie die Datensicherung zum Bestandteil Ihres Qualitäts-Managements und formulieren Sie entsprechende Arbeitsanweisungen!

Datenschutz

Der Schutz von personenbezogenen Daten vor fremdem Zugriff ist gesetzlich geregelt. Eine Orientierungshilfe bieten die „Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der Bundesärztekammer und der KBV.

Ihre EDV betreffend beachten Sie bitte u.a. folgende Hinweise:

a) Weisen Sie Ihre Mitarbeiter auf den Datenschutz hin und lassen Sie sich eine Erklärung zum Datenschutz unterschreiben. Beispiel im Anhang.

b) Beachten Sie die Diskretion bei der Position der Bildschirme und natürlich auch der anderen schutzwürdigen Dinge wie Karteikarten, Rezepte, Befunde oder Gespräche.

c) Wenn Patienten allein mit dem System sind, sollten auf dem Bildschirm keine Daten sichtbar sein. Vor allem darf keine Arbeit am System möglich sein.

d) Es sollte eine schriftliche Erklärung zur Schweigepflicht externer Dienstleister vorliegen. Alle Mitarbeiter von **DOS** haben eine solche Erklärung abgegeben.

e) Datenträger mit Patientendaten dürfen praxisfremden Personen nicht zugänglich sein.

f) Achten Sie bei der Entsorgung von Datenmaterial darauf, dass es keine verwertbaren Daten enthält oder beauftragen Sie eine geeignete Entsorgungsfirma.
Bei **DOS** werden Datenträger mit schutzwürdigen Daten sicher entsorgt.

g) Bestellen Sie ggf. einen betrieblichen Datenschutzbeauftragten, der Sie bei der Aufsicht unterstützt. Ab 5 Mitarbeitern, die schutzwürdige Daten ständig bearbeiten, ist die Bestellung laut BDSG (Bundesdatenschutzgesetz) Pflicht.

h) In Praxisgemeinschaften muss der Patient explizit über die Verfügbarkeit der Daten entscheiden. Siehe auch: „Für die Praxis – Praxiskooperation“ auf der Home-Page der KV-Berlin.
https://www.kvberlin.de/20praxis/10zulassung/40praxiskooperation/10pg/index.html

i) Gibt es eine Online-Verbindung zur Außenwelt muss das EDV-System durch Virenschutz und Firewall vor fremden Zugriff geschützt werden. Siehe „Sichere Nutzung von Online-Diensten“.

j) Bei Diebstahl können Daten in falsche Hände gelangen. Zur Abhilfe können z.B. der Datenserver und die Datensicherung in einem besonders gesicherten Raum untergebracht werden.

k) Beachten Sie auch die „Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der KBV und Bundesärztekammer.

l) Weitere Infos auch unter *„Datenschutz in der KV Berlin: Leitlinie Datensicherheit und Datenschutz“* (PDF) auf der Home-Page der KV-Berlin.
https://www.kvberlin.de/20praxis/70themen/datenschutz/10teaser_blickpunkt.html

m) Machen Sie den Datenschutz zum Bestandteil Ihres Qualitäts-Managements!

Sichere Nutzung von Online-Diensten

Online-Dienste sind unverzichtbare Bestandteile der modernen Kommunikation. Um diese Dienste sicher nutzen zu können, empfehlen wir Ihnen folgendes zu beachten:

a) Wenn einer Ihrer Praxiscomputer einen online-Zugang zum Internet hat, sind auf jeden Fall Sicherheitsvorkehrungen zu treffen.

b) Eine 100%ige Sicherheit kann niemand garantieren.

c) Das Sicherheitskonzept ist abhängig von Ihrer Anlage. Auf jeden Fall muss auf jedem Arbeitsplatz, der Zugriff auf das Internet hat, ein aktueller Virenscanner installiert sein.

d) Das Netzwerk darf nur über einen Router mit aktiver Firewall „online“-Zugang haben.

e) Von Zeit zu Zeit sollten die neuesten Betriebs-System-Updates (Service-Packs) installiert werden (zum Beispiel im Rahmen des Frühjahrsputzes). Hinweis: Wenn Sie ein Windows-Update selbst herunterladen und installieren, kann es durch die dazugekommenen Schutzmaßnahmen zu Funktionsbeeinträchtigungen einzelner Programme kommen. Die Schutzmaßnahmen müssen dann erst wieder mit Ihrem System abgestimmt werden.

f) Nur aus zuverlässigen Quellen dürfen Daten und Programme herunter geladen werden.

g) Wenn der Virenscanner meldet, dass die Lizenz abgelaufen ist, werden keine aktuellen Updates mehr geladen. Die Lizenz muss dann umgehend verlängert werden (geht meist per Telefon und eMail). Informieren Sie Ihr Praxispersonal über die Möglichkeit dieser Meldung.

h) Vereinbaren Sie mit Ihrem Praxispersonal, dass Veränderungen an Systemeinstellungen nie ohne Rücksprache erfolgen dürfen (Es kommt beispielsweise vor, dass lästige Meldungen eines Virenscanners einfach abgeschaltet werden).

i) Stellen Sie sicher, dass nur vertrauenswürdige Datenträger (CD’s, DVD’s, Wechselplatten, USB-Sticks, externe Festplatten usw.) an Ihrem System benutzt werden.

j) Vermeiden Sie nach Möglichkeit den Einsatz des WLAN; auch aus Gründen der Betriebssicherheit.

k) Melden Sie sich nach Praxis-Schluss ordnungsgemäß an allen Arbeitsplätzen und am Server ab.

l) Bewahren Sie Ihre Zugangsdaten sorgfältig auf. Denken Sie daran bei Personalwechsel Konten zu deaktivieren und ev. Passwörter zu ändern.

m) Machen Sie die Online-Sicherheit zum Bestandteil Ihres Qualitäts-Managements!

Begriffe zur Online-Sicherheit

Viren bzw. Computerviren verbreiten sich selbständig über Datenträger, Internet, eMails, Downloads, USB-Sticks u.v.m. Sie sind in der Regel gemacht, um irgendeinen Schaden anzurichten, im harmlosesten Fall als Spaß, in ernsten Fällen als Zerstörer von System und Daten oder auch als Spione. Gegenmaßnahme: Virenscanner.

Hackerangriffe finden statt, um in Ihr System einzudringen und dort unbemerkt tätig zu werden. Hierbei können Daten gestohlen oder zerstört werden, die Systemkonfiguration kann manipuliert oder unbrauchbar gemacht werden oder ihr System wird einfach für fremde Zwecke benutzt (z.B. als Datenserver für urheberrechtlich geschützte Daten, Filme, Musik o.a.). Gegenmaßnahme: Firewall, Windows-Update, Schließen von Ports, Trennung der Verbindung, Verwendung sinnvoller Passwörter.

Virenscanner sind Programme die auf dem Arbeitsplatz jederzeit aktiv sind und alle über die Verbindung ankommenden Daten auf Viren überprüfen. Gleichzeitig können Datenträger, Speicher, eMails usw. auf Virenbefall untersucht werden. Die meisten Virenscanner bringen sich selbst, in kurzen Abständen, online auf den neusten Stand (Online-Update Signaturen).

Firewall nennt man eine Einrichtung im Router (Verbindung des Praxis-Netzes mit der Online-Welt) oder im Computer mit Online-Anschluß, die Angriffe von außen unterbindet. Am wirkungsvollsten sind Router mit Firewall. Damit ist die IP-Adresse des angeschlossenen Computers nicht von außen sichtbar.

VPN – Arbeiten von Ferne (Remote)

VPN (Virtual Private Network) ist eine Software, die unter modernen Betriebssystemen läuft und zwei Netze über einen sogenannten Tunnel (VPN-Protokoll) verbindet. Über diese Verbindung kann ein Arbeitsplatz in einem anderen Netz ferngesteuert werden (Remote Desktop). Dies ergibt eine Lösung, um vom Heimarbeitsplatz oder von einem entfernten Standort aus mit dem Praxiscomputer zu arbeiten. D.h. mit einem Computer wird, über ein Netzwerk, ein zweiter eingeschalteter Computer ferngesteuert.

Voraussetzungen: An beiden Standorten muss ein Online-Zugang, am besten ein DSL-Anschluß mit möglichst hoher Geschwindigkeit (ab 3.000MBit/Sek), vorhanden sein. Betriebssysteme ab Windows 2012 Server oder Windows 7 sind nötig, ebenso sollte an beiden Standorten für Virenschutz und Hackerschutz (Router mit Firewall) gesorgt sein.

Risiken: Wenn keine Standleitung vorhanden ist, muss der Praxiscomputer zur Namensauflösung bei einem DNS-Server angemeldet sein. Diese Server stehen im Internet auch kostenfrei zur Verfügung, können aber manchmal Ursache für Verbindungsprobleme sein. Z.B. wenn dieser Server ausfällt, gewartet wird oder einfach aus dem Netz genommen wird. Wenn die Verbindung eine Zeit nicht benutzt wird, löschen diese Server den Account und der Fernarbeitsplatz findet die Praxis (Host) nicht mehr. Ein DSL-Zugang mit eigener IP-Adresse ist im Unterhalt teurer, braucht aber so einen DNS-Server nicht. Feste IP-Adressen werden allerdings häufiger angegriffen.
Der Tunnel und die Verschlüsselung der Übertragung bietet eine gewisse Sicherheit, trotzdem müssen alle Möglichkeiten des Schutzes wie oben beschrieben (Online-Sicherheit) genutzt werden.

Wichtig: Melden Sie sich nach der Arbeit ordnungsgemäß ab. Melden Sie sich auch in Arbeitspausen oder wenn Sie Ihren Platz verlassen ab. Verwenden Sie unübliche Kennworte, die nicht aus Ihren persönlichen Daten ableitbar sind. Achten Sie auf Ihr Kennwort!
Nachdem Sie sich abgemeldet haben, müssen Sie noch die VPN-Verbindung zum Praxisnetz trennen.
Hinweis: Wenn Sie nur die Verbindung trennen, sind Sie auf Ihrem Praxisrechner noch angemeldet!

Durch die modernen, leistungsfähigen Datenverbindungen ist die Arbeit per Fernsteuerung fast genauso schnell und angenehm, als wenn Sie vor Ort arbeiten. Für eine Vernetzung von Praxen mit mehreren Standorten bietet sich diese Lösung besonders an.

Bevor der Techniker kommt

Bevor ein Techniker kommt, um Ihre Anlage zu reparieren, zu warten oder zu erweitern, sind einige Vorbereitungen ratsam:

a) Machen Sie eine Datensicherung! Dies spart teure Technikerzeit, denn unsere Techniker sind angehalten bei relevanten Arbeiten am System die Daten vorher zu sichern.

b) Sorgen Sie für Zugang zu den entsprechenden Räumen und verlagern Sie die Behandlung ggf. in andere Räume. Auch Wartezeit wird berechnet.

c) Achten Sie darauf, dass ein Mitarbeiter zugegen ist, der mit der Anlage vertraut ist und weiß was gemacht werden soll. Dieser muss die Arbeit anschließend auch abnehmen und eventuell eingewiesen werden.

d) Beachten Sie bitte, dass wir viele Praxen betreuen und die Standorte mancher Komponenten nicht dokumentiert haben. Halten Sie die Dokumentation Ihrer Praxiscomputer-Anlage bereit.

e) Wenn Sie einen **Leih-Arbeitsplatz** bekommen, machen Sie bitte eine Liste der wirklich notwendigen Programme, die Sie außer der ALBIS, an diesem Arbeitsplatz für die Zeit bis zum Rücktausch brauchen (Kosten). Legen Sie die entsprechenden Datenträger, Zugangsdokumente und Lizenzen bereit. Wir gehen bei der Stellung eines Leih-Arbeitsplatzes zunächst davon aus, dass nur ALBIS genutzt wird.

f) Wenn Sie einen **neuen Arbeitsplatz** als Ersatz für einen bestehenden bekommen, machen Sie bitte eine Liste der notwendigen Programme, die Sie außer der ALBIS, an diesem Arbeitsplatz brauchen. Legen Sie die entsprechenden Datenträger, Zugangsdokumente und Lizenzen bereit. Wir gehen bei der Einrichtung eines neuen Arbeitsplatzes zunächst davon aus, dass nur ALBIS genutzt wird.

g) Rechnen Sie damit, dass der Techniker sich verspäten kann. Vor allem nachmittags können sich Verlängerungen der Einsatz-Zeiten addieren. Der Techniker möchte in jeder Praxis alles wirklich fertig machen. Auch in Ihrer Praxis kann der Einsatz mal länger dauern.

h) Bitte besprechen Sie mit uns alle Ihre Wünsche vor dem Einsatz-Termin, damit die Einsatz-Dauer für beide Seiten abschätzbar ist.

i) Geben Sie uns eine Rufnummer unter der ein Praxismitarbeiter auf jeden Fall erreicht werden kann. Möglicherweise kommt der Techniker nicht ins Haus oder möchte seine Verspätung mitteilen.

Umgang mit der Hotline

Unsere Hotline ist von Montag bis Freitag von 7:30 Uhr bis 20:00 Uhr besetzt.
In den abrechnungsrelevanten Phasen gibt es darüber hinaus zusätzliche Hotline-Zeiten.
Diese finden Sie auf unserer Homepage:
www.albis.berlin oder **www.albis-berlin.de** unter „Service“ – „Ihre ALBIS-Hotline“.

Bitte beachten Sie auch:

a) Zwischen 7:30 Uhr und 9:00 Uhr, sowie zwischen 18:00 Uhr und 20:00 Uhr ist der Notdienst geschaltet. Bitte rufen Sie zu diesen Zeiten nur bei wirklichen Notfällen an. Uns stehen dann nicht alle Möglichkeiten zur Verfügung, um Ihnen zu helfen.

b) Erfahrungsgemäß kommt es morgens ab 9:00 Uhr und mittags ab 13:00 Uhr zu erhöhtem Anrufaufkommen, was trotz entsprechendem Personaleinsatz zu Wartezeiten führen kann. Wir bitten dafür um Verständnis. Vielleicht können Sie diese Information bei Ihren Anfragen berücksichtigen.

c) Bitte nutzen Sie für Ihre Anfragen auch unsere eMail-Adresse: **hotline@albis.berlin** oder **FAX 030 8099 7130**. Nutzen Sie diese Möglichkeit auch in dringenden Fällen!

d) Die Hotline kann und soll keine Schulung oder Einweisung ersetzen. Wir haben umfangreiche und kostengünstige Seminarprogramme entwickelt, die Ihnen und Ihren Mitarbeitern die Möglichkeit geben ALBIS optimal kennen zu lernen.
Auf unserer Homepage **www.albis.berlin** finden Sie unter „Seminare“ alle entsprechenden Informationen und Termine.

e) Kennwörter für die Benutzer werden von der Hotline grundsätzlich nicht vermittelt. Zum einen kennen wir die Kennwörter nicht, zum anderen ist es nicht möglich den Anrufer zweifelsfrei zu identifizieren. Wir bitten für diese Maßnahme, in Ihrem Interesse, um Verständnis. Bitte verwahren Sie die Kennwörter sorgfältig und weisen Sie Ihr Personal entsprechend an.

f) Das Tageskennwort (z.B. zum Zusammenführen von Patienten) nennen wir an der Hotline gegen Nennung des Mitarbeiter-Namens.

g) Das Administratorenkennwort nennen wir nur nach vorherigem schriftlichen Auftrag durch den Praxisbetreiber und seinem persönlichen zeitnahen Anruf.

h) Bitte beachten Sie die Update- und Installationsanweisungen! Möglicherweise finden Sie hier bereits Antworten auf viele Fragen.

i) Häufige Fragen an der Hotline haben wir auf unserer Homepage **www.albis.berlin** gesammelt und mit hilfreichen Antworten versehen. Bitte schauen Sie ev. dort nach.

j) Kostengünstige und schnelle Hilfe bietet oft die Einwahl auf dem Arbeitsplatz. Berechnet werden in diesem Fall nur die geleisteten AWs und die Einwahl-Pauschale.
Der Zugriff auf Ihre EDV-Anlage über eine Fernwartungs-Software berührt die Regelungen des Bundesdatenschutzgesetzes und der Datenschutzregelungen der Länder. Wir unterliegen der Aufsicht der Datenaufsichtsbehörden für den nicht öffentlichen Bereich.
Deshalb ist es notwendig vorher eine Einwahl-Vereinbarung zu treffen. Sie finden die entsprechenden Formulare auf unserer Homepage **www.albis.berlin** unter „Service“. Wenn Sie einen BASIS- oder PREMIUM-Wartungsvertrag haben, gibt es eine entsprechende Vereinbarung bereits. Sollte eine Einwahl oder ein Zugriff auf die Praxisdaten seitens der CGM Deutschland AG notwendig sein, muß zusätzlich ein sogenannter **ADV-Vertrag** (Vertrag zur Auftragsdatenverarbeitung) geschlossen werden. Dieser regelt im Sinne des BDSG (§11) Rechte, Pflichten und Maßnahmen zwischen Auftraggeber (Praxis) und Auftragnehmer (CGM).

Einspielen der Updates

Updates enthalten Verbesserungen und notwendige Änderungen in der Software für Ihren Praxiscomputer. Meistens werden Updates über das Internet heruntergeladen und anschließend eingespielt. In manchen Fällen liegt das Update auf einem Datenträger vor (CD, DVD o.a.).

Bitte beachten Sie beim ALBIS-Update:

a) Online Update: Laden Sie das Update möglichst bald nach der Ankündigung herunter. Sie brauchen das Update nicht sofort einzuspielen! Während des Herunterladens kann mit ALBIS gearbeitet werden!

b) Vor dem Einspielen des Updates empfehlen wir eine Datensicherung zu machen. Siehe auch Seite 6.

c) Beim Einspielen des Updates müssen alle anderen Arbeitsplätze das ALBIS-Programm beendet haben. Bitte stellen Sie auch sicher, dass während des Update-Vorganges ALBIS an keinem Platz gestartet wird. In großen, unübersichtlichen Praxen empfehlen wir die Anlage vor dem Update herunterzufahren und den Server neu zu starten.

d) Lesen Sie bitte die Update-Dokumentation und informieren Sie Ihr Personal über relevante Änderungen. (Online über: „?“ – „Infoseiten“ – „Update-Info“ - …).

e) Vergessen Sie bitte nicht ggf. die Gebührenordnungen zu aktualisieren. Während dieses Vorganges sollte ebenfalls an keinem anderen Platz mit ALBIS gearbeitet werden.

Updates des Betriebssystems (Windows) sind hauptsächlich empfehlenswert um Sicherheitslücken zu schließen (siehe oben „Sichere Nutzung von Online-Diensten“).
Achtung: Das Einspielen von Updates oder so genannten Patches kann zu Funktionsbeeinträchtigungen führen, die eine Änderung der Konfiguration notwendig machen.

Manche Anwendungen benötigen den Internet Explorer oder Java (KBV-Prüfprogramm). Ggf. sind die entsprechenden Updates durchzuführen, damit diese Programme korrekt laufen.

Updates von Virenprogrammen sind unbedingt durchzuführen. In den meisten Fällen geschehen diese Updates automatisch über das Internet. Achten Sie darauf die Update-Lizenzen rechtzeitig zu verlängern.

Beachten Sie bei sonstigen Updates die Dokumentation der Hersteller.

Bei unserem jährlichen „Frühjahrsputz“ werden notwendige Updates der Betriebssysteme durchgeführt.

Garantie und Gewährleistung

Durch unsere langjährige Erfahrung im Markt der Praxiscomputer haben wir uns besonders zuverlässige Lieferanten mit qualitativ hochwertigen Produkten ausgesucht. Trotzdem kommt es zuweilen zu Defekten. Dies ist bedauerlicherweise bei technischen Produkten nicht zu vermeiden.

Es gibt Defekte, die schon bei der Lieferung in der Anlage schlummern. Für diese haben Sie die Sicherheit unserer Vollgarantie, die nicht nur für den Austausch des defekten Teiles sorgt, sondern darüber hinaus An- und Abfahrt des Technikers und alle Installations- und Konfigurationsarbeiten an Ihrem System abdeckt. Diese Vollgarantie können Sie 1 Jahr in Anspruch nehmen. Sie müssen in diesem Fall auch nicht den Nachweis führen, dass der Fehler schon bei Lieferung vorhanden war, wie es das Gewährleistungsrecht vorsieht.

Sicher haben Sie Verständnis dafür, dass Verschleißteile, gebrauchsbedingter Verschleiß und Verbrauchsmaterial von der Gewährleistung ausgeschlossen sind.

Zu den Verschleißteilen gehören beispielsweise Computer-Komponenten mit mechanisch bewegten Teilen mit offenem Zugang wie Floppy- und CD/DVD-Laufwerke, Wechselmedien- Laufwerke, Streamer und Lüfter.

Bei Druckern sind die Nadel-Druckköpfe, Tonertrommeln und Tinten-Druckköpfe Verschleißteile.

Der Gesetzgeber sieht eine Gewährleistung für private Verbraucher von 2 Jahren, für Unternehmer von einem Jahr, vor. Der Mangel muss bei Übergabe des Kaufgegenstandes vorgelegen haben und darf nicht durch Eigenverschulden des Kunden entstanden sein.

Wir hoffen Ihnen mit diesen Ausführungen gedient zu haben. Im Falle eines Defektes stehen Ihnen unsere Techniker gern zu Verfügung.

Anhang: Telefonnummern, Adressen u.a.

DOS GmbH ● ALBIS.Berlin
Erbacher Straße 3 a
14193 Berlin-Grunewald
www.albis.berlin
Zentrale: 030 8099 710
Hotline: 030 8099 7125
Beschwerden 030 8099 7126
info@albis.berlin

CGM Deutschalnd AG - Geschäftsbereich ALBIS
Maria Trost 23
56070 Koblenz
www.albis.de
Telefon: 0261 80 00-1600
Fax: 0261 80 00-1650
info@albis.de

Kassenärztliche Vereinigung Berlin
Masurenallee 6 a
14057 Berlin
www.kvberlin.de
Telefon: 030 3100 30
Fax: 030 3100 3380
Service: 030 3100 3999
kvbe@kvberlin.de

Kassenärztliche Vereinigung Brandenburg
Pappelallee 5
14469 Potsdam
www.kvbb.de
Telefon: 0331 2309 – 0
Fax: 0331 2309 – 175
info@kvbb.de

Kassenärztliche Bundesvereinigung
Herbert-Lewin-Platz 2, 10623 Berlin
Postfach 12 02 64, 10592 Berlin
www.kbv.de
Telefon: 030 40 05 – 0
Fax: 030 40 05 – 15 90
info@kbv.de

Ärztekammer Berlin
Friedrichstraße 16
10969 Berlin
www.aerztekammer-berlin.de
Telefon: 030 40806 – 0
Fax: 030 40806 – 3499
kammer@aekb.de

Privadis c/o CGM Deutschland AG
Maria Trost 23
56070 Koblenz
www.privadis.de
Telefon: 0261 8000 2025
Fax: 0261 8000 2675
info@privadis.de

german-telematics
Rankestraße 26
10789 Berlin
www.german-telematics.de
Telefon: 030 – 3180 5455
Fax: 030 – 3180 5454
info@german-telematics.de

Anhang: Beispiel zur Datenschutzerklärung (ohne Gewähr)

Präambel zur „Verpflichtung zur Wahrung des Datengeheimnisses“

Mitarbeiter der Praxis und deren Beauftragte, die Umgang mit Daten über Einzelpersonen haben oder von diesen Daten Kenntnis erlangen, sind nach § 5 Datenschutzgesetz sowie nach § 8 Landesdatenschutzgesetz zur Einhaltung des Datengeheimnisses verpflichtet. Diese Verpflichtung erfolgt für jede/n Mitarbeiter/in bei Aufnahme ihrer/seiner Tätigkeit und setzt sich nach deren Beendigung fort.

Das Datengeheimnis gilt auch für Personen, die als temporäre Mitarbeiter, wie Wartungskräfte, Leihpersonal, Studenten, Doktoranden o. ä. beschäftigt werden.

Die Wahrung des Datengeheimnisses bezieht sich auf jede Form der Datenverarbeitung bis hin zur Weitergabe von Computerlisten. Geschützt sind alle in Dateien gespeicherten Daten, die sich auf Personen bzw. bestimmbare Personen beziehen.

Keine der genannten Personen darf geschützte personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen vertraglichen Aufgabenerfüllung gehörenden Zweck verarbeiten, bekannt geben, anderen Personen oder Personenkreisen zugänglich machen. Verstöße gegen das Datengeheimnis sind strafbar.

Verpflichtungserklärung

Gemäß § 5 Bundesdatenschutzgesetz (BDSG) und § 8 Landesdatenschutzgesetz wird

Frau / Herr _____

durch die folgenden Hinweise auf das Datengeheimnis verpflichtet:

1. Personenbezogene Daten sind alle Einzelangaben über persönliche und sachliche Verhältnisse einer Person. Personenbezogene Daten dürfen zu keinem anderen Zweck als demjenigen der jeweiligen rechtsmäßigen Aufgabenerfüllung verarbeitet, bekannt gegeben, zugänglich gemacht oder sonst genutzt werden. Eine Verletzung dieses Verbotes ist strafbar (nach § 41 BDSG) und disziplinarisch als Verletzung des Arbeitsvertrages zu ahnden. Die Verpflichtung auf das Datengeheimnis besteht auch nach Ende des Beschäftigungsverhältnisses fort.
2. Personenbezogene Daten und damit zusammenhängende Informationen sind nicht einzusehen, solange dies nicht zwingend zu der ordnungsgemäßen Auftragserfüllung erforderlich ist.
3. Alle angefertigten Kopien, Teilkopien und weiterverarbeitete Formen der Daten sind nach Abschluss des Auftrages zu löschen oder zu vernichten. Überlassene Datenträger sind an den Eigentümer zurückzugeben.
4. Die Weitergabe von Benutzerkennungen oder Passwörtern ist **nicht** erlaubt.
5. Nicht mehr benötigte Ausdrucke, die im Computer erstellt wurden, müssen in den entsprechend gekennzeichneten Behältern gesammelt werden.
6. Beim Verlassen des Bildschirmarbeitsplatzes darf ein unbefugter Zugriff zu vertraulichen Kundendaten nicht möglich sein (zurück in die Eingangsmaske).
7. Nicht mehr benötigte Datenträger müssen vor der Entsorgung sorgfältig gelöscht oder auf andere Art unlesbar gemacht werden.

Berlin, den _____ _____

Unterschrift der/s Mitarbeiter/in

Anhang: Checkliste zur Praxiscomputeranlage

Vielleicht hilft es Ihnen diese Checkliste von Zeit zu Zeit durchzugehen, um die Sicherheit Ihrer Praxiscomputeranlage zu erhöhen.

- ☐ Datensicherung wird ordnungsgemäß durchgeführt, kontrolliert und gelagert.
- ☐ Letzte Updates sind eingespielt und die Gebührenordnungen sind aktualisiert.
- ☐ Im Patienten ALBIS häufen sich keine verdächtigen Eintragungen.
- ☐ Kabelverlegung ist für Praxiscomputer und Personal betriebssicher.
- ☐ „Frühjahrsputz“ wurde vor weniger als einem Jahr durchgeführt.
- ☐ Wir sind auf einen Ausfall der Anlage vorbereitet.
- ☐ Hochwertige Datenträger zur Sicherung, Farbbänder, Toner u.a. sind vorrätig.
- ☐ Datenschutz wird beachtet (Diskretion, Datenschutzerkl. der MA, Entsorgung).
- ☐ Virenscanner sind aktiv und aktuell, Firewall ist scharf.
- ☐ Report-Dateien des Virenscanners durchgesehen und unauffällig.
- ☐ Die Datensicherung wurde an neue Erweiterungen angepasst.
- ☐ Die Dokumentation über die Anlage im Patienten „ALBIS“ ist aktuell.
- ☐ Die Dokumentation der Standorte aller Komponenten ist aktuell.
- ☐ Das Praxispersonal ist zu den notwendigen ALBIS-Schulungen angemeldet.
- ☐ Die Abarbeitung der Checkliste wurde im Patienten ALBIS dokumentiert.
- ☐
- ☐
- ☐
- ☐
- ☐

Ein letztes Wort

Diese Informationen sollen Ihnen einen reibungslosen Betrieb Ihres Praxiscomputers ermöglichen. Wir haben unsere mehr als 35jährige Erfahrung in diese Dokumentation einfließen lassen. Trotzdem wird es immer wieder Fälle geben, die hier nicht erwähnt sind. Obwohl wir mit aller Sorgfalt gearbeitet haben kann es auch passieren, dass der eine oder andere Sachverhalt missverständlich ist oder nicht mehr stimmt.

Letztlich tragen Sie als Unternehmer die volle Verantwortung für den Betrieb einer technischen Anlage. Wir beraten und helfen Ihnen gern.

Anregungen zur Verbesserung dieser Schrift nehmen wir gern entgegen.

Noch ein Tipp: Legen Sie in der ALBIS einen Patienten „ALBIS“ an und dokumentieren Sie dort alle Ereignisse (Anschaffungen, Reparaturen, Änderungen, Störungen usw.) rund um Ihren Praxiscomputer. Dies hilft Ihnen bei der objektiven Beurteilung Ihrer Anlage und der Technik oft bei der Fehlersuche.

Bitte beachten Sie unseren beiliegenden **BASIS-Wartungsvertrag**!

Berlin-Grunewald, im April 2016

Erklärung der DOS GmbH / ALBIS.Berlin zum Datenschutz

Präambel zur „Verpflichtung zur Wahrung des Datengeheimnisses“

Mitarbeiter der DOS GmbH und deren Beauftragte, die Umgang mit Daten über Einzelpersonen haben oder von diesen Daten Kenntnis erlangen, sind nach § 5 Datenschutzgesetz sowie nach § 8 Landesdatenschutzgesetz zur Einhaltung des Datengeheimnisses verpflichtet. Diese Verpflichtung erfolgt für jede/n Mitarbeiter/in bei Aufnahme ihrer/seiner Tätigkeit und setzt sich nach deren Beendigung fort.

Das Datengeheimnis gilt auch für Personen, die als temporäre Mitarbeiter, wie Wartungskräfte, Leihpersonal, Studenten, Doktoranden o. ä. beschäftigt werden.

Die Wahrung des Datengeheimnisses bezieht sich auf jede Form der Datenverarbeitung bis hin zur Weitergabe von Computerlisten. Geschützt sind alle in Dateien gespeicherten Daten, die sich auf Personen bzw. bestimmbare Personen beziehen.

Keine der genannten Personen darf geschützte personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen vertraglichen Aufgabenerfüllung gehörenden Zweck verarbeiten, bekannt geben, anderen Personen oder Personenkreisen zugänglich machen. Verstöße gegen das Datengeheimnis sind strafbar.

Jeder Mitarbeiter und Beauftragter der DOS GmbH haben die folgende Verpflichtungserklärung unterzeichnet. Die DOS GmbH bietet dem Auftraggeber damit die in §5 BDSG (Bundesdatenschutzgesetz) geforderte Sicherheit.

Verpflichtungserklärung

Gemäß § 5 Bundesdatenschutzgesetz (BDSG) und § 8 Landesdatenschutzgesetz werden die Mitarbeiter der DOS GmbH durch die folgenden Hinweise auf das Datengeheimnis verpflichtet:

1. Personenbezogene Daten sind alle Einzelangaben über persönliche und sachliche Verhältnisse einer Person. Personenbezogene Daten dürfen zu keinem anderen Zweck als demjenigen der jeweiligen rechtsmäßigen Aufgabenerfüllung verarbeitet, bekannt gegeben, zugänglich gemacht oder sonst genutzt werden. Eine Verletzung dieses Verbotes ist strafbar (nach § 41 BDSG) und disziplinarisch als Verletzung des Arbeitsvertrages zu ahnden. Die Verpflichtung auf das Datengeheimnis besteht auch nach Ende des Beschäftigungsverhältnisses fort.
2. Personenbezogene Daten und damit zusammenhängende Informationen sind nicht einzusehen, solange dies nicht zwingend zu der ordnungsgemäßen Auftragserfüllung erforderlich ist.
3. Alle angefertigten Kopien, Teilkopien und weiterverarbeitete Formen der Daten sind nach Abschluss des Auftrages zu löschen oder zu vernichten. Überlassene Datenträger sind an den Eigentümer zurückzugeben.
4. Die Weitergabe von Benutzerkennungen oder Passwörtern ist **nicht** erlaubt.
5. Nicht mehr benötigte Ausdrucke, die im Computer erstellt wurden, müssen in den entsprechend gekennzeichneten Behältern gesammelt werden.
6. Beim Verlassen des Bildschirmarbeitsplatzes darf ein unbefugter Zugriff zu vertraulichen Kundendaten nicht möglich sein (zurück in die Eingangsmaske).
7. Nicht mehr benötigte Datenträger müssen vor der Entsorgung sorgfältig gelöscht oder auf andere Art unlesbar gemacht werden.

Diese Erklärung ist Bestandteil des Qualitäts-Management der DOS GmbH und ohne Unterschrift gültig.

Berlin, den 11. April 2016

Ihre Partner und Ihre Software:

Die **DOS GmbH** wurde 1979 gegründet und hat ihren Sitz in Berlin-Grunewald. Anfangs waren wir als Softwarehaus erfolgreich. Später konzentrierten wir uns zunehmend auf den Vertrieb und die Kundenbetreuung. Exklusiv sind wir seit 1990 mit den ALBIS Produkten in Berlin und Teilen von Brandenburg am Markt.

ALBIS.Berlin ist seit 1991 der Vertriebspartner der „**CGM Deutschland AG** – Geschäftsbereich **ALBIS“** und die größte Abteilung der **DOS GmbH**.
Die Markteinführung von ALBIS durch uns war von 1990 bis heute sehr erfolgreich. Inzwischen betreuen wir über 750 Anwender in Berlin und Umgebung. Somit zählen wir zu den führenden Anbietern im KV - Bereich. Unser Konzept, durch faire und zuverlässige Zusammenarbeit mit dem Kunden, getragen von Sympathie und gegenseitiger Wertschätzung, erfolgreich zu sein hat sich bis heute gewährt und überzeugt unsere Kunden.

CompuGroup Medical Deutschland AG ist eines der führenden eHealth-Unternehmen weltweit und erwirtschaftet einen Jahresumsatz von über 500 Mio. Euro. Seine Softwareprodukte zur Unterstützung aller ärztlichen und organisatorischen Tätigkeiten in Arztpraxen und Krankenhäusern, seine Informationsdienstleistungen für alle Beteiligten im Gesundheitswesen und seine webbasierten persönlichen Gesundheitsakten dienen einem sichereren und effizienteren Gesundheitswesen.

ALBIS ist aus der Praxis für die Praxis entwickelt worden und macht Ihnen bereits den Einstieg denkbar leicht. Die Installation erfolgt ohne technische Hürden und ist, dank einer hochwertigen Konvertierung mit allen vorhandenen Praxisdaten, auch im laufenden Quartal möglich.

ALBIS-Zusatzprodukte bieten Ihnen idealen Mehrwert. Wählen Sie nach Ihrem Praxis-Bedarf wertvolle Zusatz-Module aus und stellen Sie sich Ihr persönliches ALBIS-Leistungspaket zusammen.