

Auf Wolke Sicher

Cloud-Computing und Datenschutz im Netz

Jeder selbständige Therapeut kennt das Dilemma: Das gute alte Telefon hat zwar nicht wirklich ausgedient, jedoch sind viele weitere Werkzeuge und Wege hinzugekommen, die mittlerweile selbstverständlich zum Alltag der Praxisorganisation gehören. So ist man – auch als nicht Technik-affiner Mensch – gezwungen, sich mit den zahlreichen Anwendungsmöglichkeiten der neuen mobilen Hilfsmittel auseinanderzusetzen.

Die rasende Entwicklung der IT-Branche bringt zum Glück nicht nur neue Herausforderungen mit sich, sondern auch eine Menge Erleichterungen: Das Internet ermöglicht Datenkommunikation in nie geahnten Ausmaßen und dank mobiler Lösungen fand es den Weg in unsere Hosentaschen. Ihrem erklärten Ziel – mobile, allgegenwärtige, robuste und benutzerfreundliche Hard- und Software anzubieten – ist die IT-Branche in den letzten fünf Jahren ein gewaltiges Stück nähergekommen. Mit dem Einzug mobiler Geräte (Handys, Tablets usw.) und dem schier unerschöpflichen Angebot an Fertiglösungen hat die Digitalisierung von Prozessen unser Privatleben erobert. Unter tausenden von Apps findet man fast immer etwas Passendes.

Das, was große Unternehmen unter dem Begriff „IT-gestützter Prozessoptimierung“ kennen, ist inzwischen bis in die kleinsten Wohn- und Lebensgemeinschaften vorgedrungen. Paradebeispiele sind hier die vielen Anwendungen im Bereich Aufgabenverwaltung. Mit diesen Programmen werden, quasi unbemerkt, Wege optimiert,

Ressourceneinkäufe effizient organisiert und diese auf Personen verteilt und durchgeführt.

Übersetzt auf die Welt des Therapeuten heißt das: „Wir sind zwar gezwungen, uns ganz neuen Herausforderungen zu stellen, aber diese bieten uns auch jede Menge neuer Chancen!“

IT so leicht wie nie

Google, Facebook und andere erfolgreiche Anbieter von EDV-Produkten zeigen: Software kann durchaus bedienbar, stabil und sinnvoll auf unterschiedlichen Geräten laufen. Bei diesen Anwendungen handelt es sich meist um sogenannte Web-Anwendungen (weil es Anwendungen sind, die in einem Browser, wie Firefox, Safari, Google Chrome, Internet Explorer usw. angezeigt werden).

Die Seiten, die auf unserem Rechner im Browser angezeigt werden, stammen von einem Web-Server. Auf dem Web-Server wird dann entsprechend ein Programm ausgeführt, das die notwendigen Seiten erzeugt. Über das Internet werden diese Seiten an unseren Browser übertragen. Keine Installation, einfach so. Weder die Google-Suche noch das soziale Netzwerk Facebook müssen auf dem heimischen PC installiert werden – man gibt einfach die Adresse ein (oder sucht diese bei Google) – und schon kann man im Browser loslegen.

Der Nutzer wird nicht mehr mit technischen Details konfrontiert, wie Updates,



Papick G. Taboada
Geschäftsführer von
pgt technology scouting
GmbH und Betreiber von
der online Praxisverwaltung
LEMNISCUS

Betrieb von Server und Backups. Noch nie war IT so einfach, so massentauglich, so unglaublich effizient.

Gewonnene Bequemlichkeit

Die derzeit heranwachsende Generation kennt eine ganze andere IT, als wir sie noch zur Jahrtausendwende erlebt haben. Es ist heute selbstverständlich, dass die Daten auf mehreren Geräten verfügbar sind. Vernetzung ist kein Bonus mehr, sondern Pflicht. Ganze Betriebssysteme werden inzwischen über das Internet installiert. Keine CDs, keine Insellösungen mehr. Ein Rechner ohne Internet ist ein Rechner ohne Updates, ein Rechner ohne Mail, ohne Kommunikation, abgeschottet und eingeschränkt.

Wir alle haben uns an Google Suche, Google Maps, Google Mail, Facebook, WhatsApp und Dropbox gewöhnt. Hervorragende Produkte, die im privaten Bereich gerne genutzt werden und für eine hohe Erwartungshaltung sorgen. Die Software von heute soll mobil, vernetzt, stabil, einfach und bedienbar sein. Jedoch stehen diese Anwendungen allesamt nicht im Einklang mit unserem Datenschutzgesetz. Dabei ist insbesondere bei der elektronischen Datenerfassung von Personendaten Vorsicht geboten.

Elektronische Datenerfassung von Personendaten

Der Betrieb einer Praxis hat einige organisatorische Aspekte, die für die elektronische Datenverarbeitung sehr interessant sind. Bereits die Terminplanung und Rechnungsstellung beinhalten – auch wenn unter Umständen nur indirekt – Angaben zu besonderen Personendaten. Wie mit Personendaten umzugehen ist, wurde umfassend im Bundesdatenschutzgesetz (kurz BDSG) festgehalten.

Besondere Personendaten sind laut dem BDSG § 3 Abs. 9:

- Ethnische Herkunft
- Politische Meinungen
- Religiöse oder philosophische Überzeugungen
- Gewerkschaftszugehörigkeit
- Angaben über die Gesundheit
- Sexualleben.

Beispiele für Angaben über die Gesundheit [1]:

- einzelne Krankheiten, Diagnose, Verlauf, Schwere, Dauer
- Ablauf und Inhalt medizinischer Behandlungen durch Ärzte, Krankenhäuser und medizinische Hilfsdienste
- verordnete oder eingenommene Medikamente
- Alkohol- oder sonstige Drogensucht.

Es sind selbst Angaben betroffen, die lediglich indirekt Informationen über besondere Daten vermitteln. Beispiel: Der Vermerk „Max Mustermann, Rückengymnastik“ im Terminkalender eines Physiotherapeuten vermittelt indirekt Informationen über die Gesundheit.

Der Therapeut darf im Rahmen seiner Tätigkeit zweckgebunden besondere Personendaten erfassen, und es ist prinzipiell davon auszugehen, dass sämtliche erfassten Daten direkt oder indirekt zu den besonderen Personendaten gehören. Da diese zweckgebundene Erfassung von Personendaten für die Tätigkeit des Therapeuten unablässig ist, wird keine explizite Zustimmung des Patienten benötigt, § 28 BDSG. Eine Zustimmung wird erst dann notwendig, wenn Daten an Dritte übermittelt werden. Übermitteln von Daten ist die Bekanntgabe personenbezogener Daten an Dritte, § 3 Abs. 4 Nr. 3 BDSG. Dritter ist gemäß § 8 Abs. 2 BDSG jeder andere, mit Ausnahme des eigentlichen Betroffenen, meist der Patient, und derjenigen, die die personenbezogenen Daten nur für den

Therapeuten im Auftrag erheben, verarbeiten oder nutzen.

Es kommt somit darauf an, ob der Therapeut noch selbst die „Herrschaft über die personenbezogenen Daten“ behält oder ob andere die personenbezogenen Daten eigenverantwortlich und weisungsfrei verwenden können und damit selbst „Herr der personenbezogenen Daten“ werden. **Beispiel:** Ein Therapeut speichert Abrechnungsinformationen auf einen USB Stick. Dieser wird von einem Fahrrad-Kurier zu einem Abrechnungsdienstleister auf der anderen Seite der Stadt transportiert.

- Der Fahrrad-Kurier transportiert lediglich die Daten. Hier findet keine Datenverarbeitung statt.
- Der Abrechnungsdienstleister muss die Daten aus dem Stick auslesen und für seine Tätigkeit auch übernehmen. Rechnungen werden nicht im Namen des Therapeuten, sondern im Namen der Abrechnungsstelle gestellt. Hier findet ein Wechsel der Herrschaft über die personenbezogenen Daten statt.

Das Beispiel soll verdeutlichen, warum ein Abrechnungszentrum die Zustimmung der Patienten benötigt. Schließlich wechselt hier die Herrschaft, und damit die Kontrolle, über besondere Personendaten. Ein solcher Herrschaftswechsel ist für die eigentliche Durchführung der Therapie nicht mehr wirklich erforderlich. Daher bedarf es der Einwilligung des Patienten.

Jede Verarbeitung personenbezogener Daten bedarf besonderen Schutz. Dieser Schutz wird durch technische oder organisatorische Maßnahmen ermöglicht. Aus der Anlage zu § 9 Satz 1 ist folgender Absatz zu entnehmen:

„Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind“.

Auf den Punkt gebracht, muss der Therapeut besondere Maßnahmen in Bezug auf die Daten seiner Patienten ergreifen. Diese sind:

- Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen perso-

nenbezogene Daten verarbeitet oder genutzt werden, verwehren (**Zutrittskontrolle**).

- Verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**).
- Gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**).
- Gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (**Weitergabekontrolle**).
- Gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**).
- Gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**).
- Gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**).
- Gewährleisten, dass zu unterschiedlichen **Zwecken** erhobene Daten getrennt verarbeitet werden können.

Eine beispielhafte Aufstellung der praktischen Maßnahmen, die zu ergreifen sind, können aus dem online Artikel des Helmholtz-Zentrums Dresden-Rossendorf (HZDR) entnommen werden [2].

Beispiel: Zutrittskontrolle

Unbefugte sollen keinen Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, erhalten. Mögliche Maßnahmen könnten sein:

- Festlegung von Sicherungsbereichen
- Festlegung von befugten Personen (Mitarbeiter, Fremdbehörden, Fremdfirmen, Wartungsdienste, Anwendungsbetreuung)

- Festlegung von Besucherregelungen
- Sicherung von Gebäuden und Räumen
- Anwesenheitsaufzeichnungen.

Die aufgeführten Maßnahmen müssen ergriffen werden, unabhängig von der Größe der Praxis – selbst Solisten (also selbständige Therapeuten die Termine und Abrechnung selbst machen) müssen sich mit den einzelnen Punkten auseinandersetzen.

Outsourcing

Viele Tätigkeiten im Bereich der EDV können sehr ökonomisch und effizient ausgelagert werden. In der IT-Branche wird gerne in diesem Zusammenhang der Begriff „Outsourcing“ verwendet. Möchte der Therapeut nicht zum IT-Experten ausgebildet werden, so kann er Teile dieser Aufgaben an andere Experten auslagern.

Mögliche Szenarien:

- **Beratung:** Der Therapeut wird in die Lage versetzt, die technisch organisatorischen Maßnahmen selbst umzusetzen.
- **Umsetzung:** Der Therapeut beauftragt einen EDV- und Datenschutz-Experten, der die technisch organisatorischen Maßnahmen umsetzen soll.
- **Wartung und Betrieb:** Der Therapeut beauftragt einen EDV-Experten, der sich um den Betrieb der Infrastruktur kümmern soll.

Externe Dienstleister unterliegen nicht der ärztlichen Schweigepflicht, sodass diese nicht ohne weiteres damit beauftragt werden können, sich um Anlagen zu kümmern, die den Zugriff auf besondere Personendaten ermöglichen würden. So ist bereits die Reparatur des Praxis-Rechners durch eine Werkstatt eine knifflige Angelegenheit. Schließlich muss der Techniker Zutritt, Zugang und Zugriff auf das entsprechende System bekommen. Findet die Reparatur in Anwesenheit des Therapeuten statt, so kann der Therapeut sicherstellen, dass kein unerlaubter Zugriff stattfindet. Wird der Rechner eingeschickt, kann nicht mehr sichergestellt werden, dass ein unerlaubter Zugriff stattfindet.

Für diese und weitere Fälle in Sinne eines „Outsourcings“ wurde im Zuge der Novellierung im Jahr 2009 in § 11 BDSG ein Zehn-Punkte-Katalog definiert, die sogenannte Auftragsdatenverarbeitung oder kurz die ADV. In der Auftragsdatenverarbeitung wird ein Vertrag zwischen Therapeut und Dienstleister abgeschlossen. Der

Therapeut ist in diesem Vertrag auf Auftraggeber und bleibt damit Herr der Daten, der Dienstleister ist der Auftragnehmer. In dem Vertrag wird der Umgang mit den besonderen Personendaten geregelt. Bei einer solchen ADV liegt keine Übermittlung von Daten an Dritte vor, einer Einwilligung des Patienten bedarf es folglich nicht. Eine ADV regelt, aus und zu welchem Zweck die personenbezogenen Daten durch den Dienstleister verarbeitet werden sollen und beinhaltet als Anlage eine Auflistung der oben genannten technischen und organisatorischen Maßnahmen des Dienstleiters. Auf diese Weise kann der Therapeut überprüfen (lassen), ob der Dienstleister selbst einen angemessenen Datenschutz gewährleistet oder nicht.

Auch die Nutzung einer „Online-Software“ wird durch eine ADV rechtsicher geregelt, hierbei handelt es sich um die Datenverarbeitung im SaaS-Modell (Software as a Service), auch als Cloud-Dienste, Cloud-Computing oder einfach nur „Cloud“ bekannt. In diesem Modell werden die Aufgaben Umsetzung, Infrastruktur, Anwendungsbetrieb, Wartung und Datensicherung an einen Dienstleister „outsourced“.

Begriffsdefinition „Cloud“

Aus Desktop-Computern wurden Smartphone, Tablet und Notebook. Anwendungen bzw. Programme nennt man schlichtweg „Apps“. Und für alles andere – also analog zu „Ding“, hat man heute den Begriff „Cloud“.

Aber was ist die Cloud? Eigentlich ist die Cloud eines der ältesten Sinnbilder der Informationstechnik und steht als solches für Rechnernetze. Immer dann, wenn man in einer Zeichnung das Netzwerk zwischen Computern angeben wollte, hat man eine kleine Wolke gezeichnet.

Spricht man heute von der Cloud, kann man ohne Kontext nicht verstehen, was genau gemeint ist. Von Microsoft kam vor einigen Jahren ein Werbefilm, in dem eine Mutter erfolglos versucht, ein nettes Bild der Familie auf dem Sofa zu machen. Mal dreht einer den Kopf, mal hat ein anderes Familienmitglied die Augen zu. Verzweifelt gibt die Mutter das Fotoshooting auf und will das Problem mit einer Bildbearbeitung lösen. An dieser Stelle kommt die Werbebotschaft „Ab in die Cloud“. Die Cloud kann demnach, wenn man Microsoft und den Medien Glauben schenkt, sogar eine Fotobearbeitung sein.

Auch Apple wirbt mit einem Produkt namens iCloud. In diesem Kontext handelt es sich einerseits um die Synchronisierung zwischen den Apple-Geräten, andererseits auch um Web-Anwendungen wie Kalender, Kontakte u.v.m.

Cloud ist somit in erster Linie alles, was man über das Internet bekommen kann. Natürlich sind alle Web-Anwendungen somit per Definition „in der Cloud“. Betreibt man den Web-Server im eigenen Keller, dann spricht man von der „private Cloud“, wird der Web-Server in einem Rechenzentrum außer Haus betrieben, so handelt es sich in diesem Fall um eine „public Cloud“.

Etwas differenzierter wird der Begriff „Cloud“ in der IT-Branche verwendet. Hier wird von „Cloud-Computing“ gesprochen. Nutzt man eine Anwendung über die Cloud, so spricht man an dieser Stelle von „Software as a Service“, oder „SaaS“. Die Google Suche, der Google Kalender, Facebook und viele andere Webseiten sind per Definition SaaS-Angebote. Über das Internet kann aber auch auf angemietete Infrastruktur zugegriffen werden – hier spricht man von „Infrastructure as a Service“, oder „IaaS“. Beispiele für IaaS sind angemietete Rechner, Netzwerke, usw. Wenn man als Dienstleistung eine Datenbank anmietet, dann spricht man hier von „Platform as a Service“, oder „PaaS“

Aus Anwendersicht spielt diese Differenzierung kaum eine Rolle. Als Endanwender wird man kaum eine Datenbank oder einen Rechner in einem Rechenzentrum anmieten wollen. Kommt ein Endanwender bewusst oder unbewusst mit Cloud-Diensten in Berührung, dann handelt es sich fast ausschließlich um SaaS-Angebote. Das SaaS-Modell basiert auf dem Grundsatz, dass die genutzte Software und die notwendige Infrastruktur bei einem externen IT-Dienstleister betrieben und vom Kunden als Service genutzt werden. Für die Nutzung werden ein internetfähiger Computer sowie eine Internetanbindung benötigt. Der Zugriff auf die Software wird meist über einen Webbrowser oder einer App auf einem mobilen Gerät realisiert.

Sensibilisierung im Hinblick auf den Umgang mit Cloud-Diensten

SaaS beschreibt ein sehr interessantes Modell des Softwarevertriebs. Der Endan-

Exkurs: Die Analogie zum Aktenschrank

Betrachten Sie als Therapeut auch die elektronisch erfassten Daten wie die Daten in einem Aktenschrank. Der Aktenschrank sollte abschließbar sein, um seine Aufgabe ordnungsgemäß zu erfüllen. Wenn eine dritte Person Zugriff zu den Akten in diesem Aktenschrank bekommen soll, müssen die Patienten zugestimmt haben.

Wo der Aktenschrank letztendlich steht, spielt keine Rolle. Sie können sich in einem Lager einen Aktenschrank anmieten oder Ihren eigenen Schrank in angemietete Räumlichkeiten hinstellen – solange nur Sie Zugriff auf den Schrank haben, ist alles ok.

Sobald eine Firma allerdings Reparatur- und Wartungsarbeiten an dem Schrank durchführt, müssen Sie mit dieser Firma einen speziellen Vertrag abschließen. In diesem Vertrag wird unter anderem festgehalten, dass diese Firma in Ihrem Auftrag arbeiten darf und dass die Akten nicht gelesen werden dürfen. Es wird festgehalten, welche technischen und organisatorischen Maßnahmen ergriffen werden, die dafür sorgen, dass die Daten in den Akten geschützt sind. Es wird desweiteren festgehalten, dass die Firma nicht unbefugt Kenntnis von den personenbezogenen Daten und damit faktisch auch Verfügungsmacht darüber erhalten darf.

Sie können natürlich auch für die Dauer der Reparatur- und Wartungsarbeiten den Vorgang überwachen und somit sicherstellen, dass der Inhalt der Akten nicht angeschaut wurde. Oder sie leeren einfach Ihren Schrank – wo keine Daten drin sind, sind auch keine Datenschutzregelungen zu beachten.

wender bekommt ein Produkt, das praktisch wartungsfrei genutzt werden kann. Der Anbieter ist für Updates, Backups, die Weiterentwicklung und die Verfügbarkeit im Allgemeinen zuständig. Alles Aufgaben, die nicht im Mittelpunkt der üblichen Tätigkeit eines Therapeuten liegen.

Ein Therapeut darf streng genommen einen Cloud-Dienst nur dann verwenden, wenn eine entsprechende ADV mit dem Anbieter abgeschlossen wurde. Und der Therapeut muss auch sicherstellen, dass die Daten nicht außerhalb der Europäischen Union abgelegt werden – das ist im Kontext besonderer Personendaten in § 4 b Abs. 2 S. 2 BDSG geregelt. Im außereuropäischen Ausland ist ein angemessener Schutz dieser personenbezogenen Daten nach Auffassung des Gesetzgebers nicht gegeben.

Spätestens an dieser Stelle dürfte klar geworden sein, dass weder der Google noch der iCloud Kalender für die Terminplanung von Behandlungen verwendet werden kann, sobald auch nur indirekt auf besondere Personendaten (z.B. Gesundheitsdaten) geschlossen werden kann.

Auch Dropbox – die elegante Synchronisierung von Dateien zwischen mehreren Computern – darf in diesem Kontext nicht verwendet werden, sobald besondere Daten

im Spiel sind. Sehr gerne werden Dropbox oder Google Docs verwendet, um Tabellenkalkulationen mit Abrechnungsinformationen abzulegen. Abrechnungsinformationen enthalten üblicherweise Anschrift, Geburtsdatum, Diagnose und eine Auflistung der erbrachten Leistungen. In diesem Fall dürften so ziemlich alle Vorschriften missachtet worden sein.

Google, iCloud und Dropbox haben ihre Server im außereuropäischen Ausland.

Wann wurde die Cloud zum Problem?

Eigentlich ist die Idee hinter dem Cloud-Computing genial. Das erste Problem besteht jedoch darin, dass Cloud-Dienste zweckentfremdet verwendet werden. Nur weil es Dropbox gibt, heißt es nicht, dass es für alles verwendet werden darf. Das zweite Problem ist, dass viele SaaS-Anbieter ihr Angebot über die Schaltung von Werbung oder über das Sammeln von werbetechnisch relevanten Informationen finanzieren. Die aussagekräftigste Botschaft im Zusammenhang mit Cloud-Diensten ist wohl die folgende: **Zahlt man nicht für einen Dienst, dann ist man nicht der Kunde, sondern das Produkt.**

Natürlich haben die jüngsten Skandale rund um Spionage ausländischer (und in-

ländischer) Geheimdienste auch dazu beigetragen, dass Cloud-Angebote mit Skepsis beäugt werden. Inwiefern Dienstleister in Deutschland oder im Ausland sich gegen Geheimdienste wehren können, und inwiefern der Computer in den eigenen vier Wänden sicherer ist, steht auf einem anderen Blatt.

Richtiger Umgang mit Cloud-Diensten

Dank der aktuellen Rechtslage in Bezug auf die besonderen Personendaten kommen viele Anbieter von cloudbasierten Lösungen für den Einsatz in Praxen nicht in Frage. Die Gesetzgebung wurde für den Schutz unser aller persönlichsten Daten 2009 überarbeitet (Novellierung) und hat somit überhaupt die Möglichkeit erschaffen, rechtssicher Patientendaten in der Cloud zu speichern. Nicht jede Cloud, denn gewisse Voraussetzungen müssen erfüllt werden:

- Die gespeicherten Daten dürfen nicht den Europäischen Raum verlassen.
- Es muss eine Vertrag über eine Auftragsdatenverarbeitung zwischen den Therapeuten und dem Anbieter (Schriftform ist Pflicht) abgeschlossen werden.
- Bei dem Dienstleister ist auf eine ausreichende Verschlüsselung zu achten, ansonsten kann es zu datenschutzrechtlichen oder sogar strafrechtlichen Konsequenzen kommen.

Wichtig in diesem Zusammenhang ist, dass der Therapeut in keinem Moment die Herrschaft und die Verantwortung über die Daten aufgibt.

Literatur

1) BDSG Absatz 9: Beispiele für besondere Daten. Online verfügbar unter http://www.bfdi.bund.de/bgdi_wiki/index.php/3_BDSG_Kommentar_Absatz_9_Beispieler

2) Helmholtz-Zentrum Dresden-Rossendorf (HZDR): Grundregeln zum Datenschutz (Anlage zu §9 Satz 1 des BDSG). Online verfügbar unter <https://www.hzdr.de/db/Cms?pNid=420>

Dipl. Wi-Ing. Papick G. Taboada
Bachstr. 11
76185 Karlsruhe
E-Mail: info@pgt.de
Internet: <http://lemniscus.de>