AOK VERLAG

Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

www.aok-verlag.info/ds-im-blick

Ausgabe Juli/August 2022 | **Seite 1**

Inhalt

Neues aus den Tätigkeitsberichten

Die Tätigkeitsberichte der Datenschutzaufsichtsbehörden sind eine sehr gute Informationsquelle, um die Meinungen der Aufsichtsbehörden und die aktuellen Themen im Blick zu behalten. Jede Aufsichtsbehörde veröffentlicht ihren Tätigkeitsbericht in der Regel jährlich. Neben allgemeinen Darstellungen enthalten die Tätigkeitsberichte eine Vielzahl an Fällen mit enormer Praxisrelevanz. Dieser Beitrag stellt kurz einige Fälle der aktuellsten Tätigkeitsberichte vor. Darüber hinaus werten wir die Tätigkeitsberichte mit Blick auf den Gesundheitsbereich auch regelmäßig und systematisch aus und stellen die Ergebnisse im Loseblattwerk „Datenschutz im Gesundheitswesen“ dar.

Sven Venzke-Caprarese

Ein Tipp für die Praxis

Bevor es mit ausgesuchten Fällen aus den Tätigkeitsbereichen weitergeht, möchten wir am Anfang noch einen Tipp für die Praxis geben. Die Tätigkeitsberichte werden von den Aufsichtsbehörden auf ihren jeweiligen Internetpräsenzen veröffentlicht. Darüber hinaus existiert seit Jahren ein Projekt, welches alle Tätigkeitsberichte aller deutschen Datenschutzaufsichtsbehörden an zentraler Stelle

zusammengetragen hat – und zwar seit dem ersten Tätigkeitsbericht. Die Webseite des Projekts ist unter https://www.zaftda.de/ erreichbar und wird mittlerweile von der Stiftung Datenschutz betrieben.

Rechnungs-E-Mail der Apotheke

Der aktuelle Tätigkeitsbericht des LfD Hessen beschäftigt sich über mehrere Seiten mit einem Fall, in dem eine Apotheke Rechnungen per E-Mail an Kunden versendete. Der LfD stellt dabei fest, dass aufgrund der Sensibilität der Rechnungsdaten eine Inhaltsverschlüsselung erforderlich sei – also eine Verschlüsselung mittels S/MIME, PGP oder per Verschlüsselung der Rechnung an sich (z.B. mittels eines geschützten ZIP-Containers).

Dabei weist der LfD ausdrücklich darauf hin, dass eine reine Transportverschlüsselung nicht ausreichend sei.

Alternativ komme auch eine Portallösung in Betracht, bei der Nutzer über einen personalisierten Bereich bereitgestellte Daten mittels Links und Passwort abrufen können. Allerdings müssen die Daten nach Ansicht des LfD auch in diesem Fall so auf dem Server des Portalanbieters abgelegt werden, dass dieser keinen Zugriff erhalte.

Ein unverschlüsselter Versand der Rechnung per E-Mail sei, so der LfD, selbst bei dem Vorliegen einer Einwilligung des Nutzers unzulässig.

Insgesamt erscheinen die Anforderungen des LfD an dieser Stelle sehr hoch, decken sich aber mit den Anforderungen anderer Aufsichtsbehörden. Allerdings akzeptieren etwa der LfD Hamburg

und auch andere Aufsichtsbehörden in bestimmten Fällen eine Abdingbarkeit der Inhaltsverschlüsselung durch eine freiwillige Einwilligung der betroffenen Person. Hierzu muss eine Inhaltsverschlüsselung aber grundsätzlich angeboten werden, es reicht nicht aus, dem Nutzer einfach keine Wahl zu lassen.

Auch die Forderung, dass Daten bei dem Betreiber einer Datenaustauschplattform so abgelegt werden müssen, dass dieser keinen Zugriff auf die Klardaten erhält, könnte hinterfragt werden. So erlaubt § 203 Abs. 3 StGB über den Begriff der „mitwirkenden Person“ in bestimmten Fällen ein Outsourcing von Daten, die dem Berufsgeheimnis unterliegen.

Insgesamt lässt sich jedoch feststellen, dass es sowohl im Sinne von Apotheken als auch von betroffenen Personen ist, sensible Daten möglichst sicher zu übermitteln.

Das Finden einer praxisgerechten Lösung wird sich jedoch nicht immer ganz einfach gestalten. Vor diesem Hintergrund weist der LfD Rheinland-Pfalz in seinem Tätigkeitsbericht auf den Entwurf des Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetzes hin, wonach zentrale und sichere Kommunikationsdienste geschaffen werden sollen, die auch

einen Sofortnachrichtendienst umfassen. Möglicherweise wird sich hierdurch in Zukunft einiges einfacher gestalten.

Anlasslose Überprüfung von Krankenhäusern in Niedersachsen

Die LfD Niedersachsen berichtet in ihrem aktuellen Tätigkeitsbericht von der anlassunabhängigen Überprüfung von 30 Krankenhäusern. Tatsächlich handelt es sich hierbei um die Fortsetzung einer Aktion, mit der die LfD bereits in den Vorjahren begonnen hat.

Im Ergebnis weist die LfD darauf hin, dass die Datenschutzbeauftragten der Krankenhäuser mit den nötigen (zeitlichen) Ressourcen ausgestattet sein müssen. Die LfD führt in diesem Rahmen aus, *„dass bereits in einem Krankenhaus mittlerer Größe mit mehreren Dutzend Beschäftigten und mehreren Tausend Patienten pro Jahr mindestens eine Vollzeitstelle pro Niederlassung für den Datenschutz eingeplant werden sollte“.*

Spannende Zahlen legt die LfD auch vor, wenn es um die Verzeichnisse der Verarbeitungstätigkeiten der überprüften Krankenhäuser geht. So bewegte sich die Bandbreite der dokumentierten Verarbeitungstätigkeiten der vorgelegten Verzeichnisse zwischen 17 und 800.

Die LfD fasst den reinen Stand der Zahlen wie folgt zusammen: „In kleineren Häusern mit weniger als 20.000 Patienten im Jahr lag der Durchschnitt bei 90 Verarbeitungstätigkeiten, in Häusern mit mehr als 20.000 Patienten im Jahr bei 207.“

Neben den genannten Themen wurde auch der Umgang mit Betroffenenrechten geprüft und es wurden Verbesserungsbedarfe hinsichtlich der Nutzung von Krankenhausinformationssystemen festgestellt.

Auslagerung der Terminvergabe

Die LfD Berlin nimmt in ihrem aktuellen Tätigkeitsbericht die Auslagerung der Terminvergabe an Terminverwaltungsunternehmen näher in den Blick.

Ein solcher Einsatz externer Unternehmen sei auch ohne Einwilligung möglich, wenn dieser als Auftragsverarbeitung ausgestaltet wird und die betroffenen Personen über den Einsatz des Dienstleisters informiert werden. Diese Ansicht ist praxisnah und überzeugt.

Die Nutzung einer Terminerinnerungsfunktion per E-Mail oder SMS sei jedoch nur dann zulässig, wenn die betroffenen Personen vorher freiwillig in diese eingewilligt haben.

Masernschutz im Krankenhaus

Der LfD Bayern beantwortet in seinem aktuellen Tätigkeitsbericht Fragen zur Umsetzung des Masernschutzgesetzes in Krankenhäusern. In diesem Rahmen stellt er kurz die Verpflichtung aus § 20 Abs. 8 und 9 Infektionsschutzgesetz dar, wonach Personen die nach dem 31. Dezember 1970 geboren wurden und in Krankenhäusern betreut werden oder tätig sind, grundsätzlich entweder einen ausreichenden Masernimpfschutz oder eine Immunität gegen Masern aufweisen müssen.

Entsprechende Nachweise können z.B. über die Einsicht in den Impfpass oder durch Vorlage einer ärztlichen Bescheinigung erbracht werden. Die Einsicht muss allerdings datensparsam erfolgen und sollte sich, soweit möglich, auf den relevanten Eintrag beschränken. Darüber hinaus ist die Anfertigung von Kopien des Impfpasses oder des ärztlichen Nachweises unzulässig.

Auch im Hinblick auf den von der Nachweispflicht betroffenen Personenkreis gibt der LfD Bayern eine praxisnahe Einordnung anhand mehrerer Beispiele. Insbesondere im Hinblick auf externe Dienstleister (z.B. Handwerker) müsse die Nachweispflicht im Einzelfall beurteilt werden. Dabei komme es darauf an, dass die Personen regelmäßig und zeitlich nicht nur vorübergehend in der Einrichtung tätig sind. Nicht nachweispflichtig seien demnach:

- „Einzelaufträge bis zu 14 Tagen (absolute Grenze);“
- „wiederkehrende Tätigkeiten bis zu 1 Tag pro Monat (also pro Jahr maximal 12 × 1 Tag);“
- „Tätigkeiten, die ausschließlich auf den außerhalb der Räumlichkeiten bestehenden Baustellen stattfinden.“

Ebenfalls für die Praxis besonders relevant ist die Aussage des LfD Bayern, dass es im Falle von nachweispflichtigen Tätigkeiten externer Dienstleister ausreiche, wenn die Einrichtung belegen kann, dass sie die eingesetzten Dienstleister privatrechtlich verpflichtet hat, nur Personen in der Einrichtung einzusetzen, die die Anforderungen erfüllen.

Eine eigene Kontrolle der Einrichtung ist demnach nicht zwingend erforderlich.

Bußgeld wegen der Nutzung von WhatsApp

Die LfD Brandenburg berichtet im aktuellen Tätigkeitsbericht über den Fall einer Ärztin, die ihre neue Praxisanschrift über eine WhatsApp-Gruppe an 230 Personen mitgeteilt hat.

Die jeweiligen Telefonnummern bzw. Kontakte waren dabei innerhalb der Gruppe für alle Mitglieder einsehbar. Die LfD Brandenburg begründet, warum dies eine datenschutzrechtlich unzulässige Datenverarbeitung darstellte und führt aus, dass in diesem Fall ein vierstelliges Bußgeld verhängt wurde.

Krankenhaus und Medizinische Versorgungszentren

Häufig werden Medizinische Versorgungszentren von Krankenhäusern gegründet und betrieben. Nicht selten befinden sich die MVZ in unmittelbarer Nähe zum Krankenhaus oder sogar in eigens dafür bereitgestellten Räumlichkeiten innerhalb des Krankenhauses. Kernaufgabe ist die ambulante medizinische Versorgung von Patienten, während der Schwerpunkt des Krankenhauses in der stationären Versorgung liegt. Auf Grund der Nähe zum Krankenhaus wird im MVZ regelmäßig auf die IT-Infrastruktur des Krankenhauses zurückgegriffen. Da das in den Krankenhäusern beschäftigte medizinische Personal auch an der vertragsärztlichen Versorgung teilnehmen kann (§ 116 SGB V), können auch dessen berufsmäßig tätigen Gehilfen sowohl im Krankenhaus als auch im Medizinischen Versorgungszentrum beschäftigt sein.

Dr. Sebastian Ertel

Datenschutzrechtliche Verantwortlichkeit

Nach der Definition des Art. 4 Nr. 7 DSGVO ist datenschutzrechtlich Verantwortlicher die natürliche oder juristische Person, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Da § 95 Abs. 1a SGB V regelt, dass auch Krankenhäuser MVZ gründen können, könnte angenommen werden, dass den Krankenhäusern daher auch die datenschutzrechtliche Verantwortlichkeit für die Datenverarbeitung im Medizinischen Versorgungszentrum obliegt. Allein das genügt jedoch nicht. Die MVZ sind in der Regel als eigene juristische Person gegründet. Sie sind in medizinischen Fragen weisungsfrei (§ 95 Abs. 1 S. 3 SGB V) und können daher auch die Prozesse zur Durchführung der Diagnostik und Heilbehandlung festlegen. Darüber hinaus erfolgt die medizinische Versorgung zu eigenen Zwecken – der Erfüllung der Verpflichtungen aus dem Behandlungsvertrag.

Auftragsverarbeitung

Aus der datenschutzrechtlichen Verantwortlichkeit des MVZ folgt zunächst, dass mit dem Krankenhaus ein Vertrag zur Auftragsverarbeitung abgeschlossen werden muss, wenn auf die dortigen Ressourcen, insbesondere die IT-Infrastruktur, zurückgegriffen wird. Gleiches gilt andersherum, wenn das Krankenhaus auf Ressourcen des MVZ zurückgreift. Besonderheiten können sich hierbei bei konfessionellen Krankenhäusern ergeben.

Während bei MVZ immer der Anwendungsbereich der DSGVO eröffnet ist, gilt bei katholischen und evangelischen Krankenhäusern das jeweilige kirchliche Datenschutzrecht (KDG bei katholischen bzw. DSG-EKD bei evangelischen Einrichtungen).

Dies hat zur Folge, dass – je nachdem, wer Auftraggeber und wer Auftragnehmer ist – der Auftragsverarbeitungsvertrag nach kirchlichem Recht oder nach der DSGVO geschlossen werden muss.

Datenweitergabe

Aufgrund der separaten datenschutzrechtlichen Verantwortlichkeiten bedarf es (außerhalb einer Auftragsverarbeitung) einer Rechtsgrundlage, wenn personenbezogene Daten zwischen den Einrichtungen ausgetauscht werden sollen. Da Krankenhäuser lediglich im Rahmen ambulanter Notfallbehandlung in Ausnahmefällen Überweisungen für Labor-, Pathologie- und Radiologieleistungen ausstellen können, wird der Schwerpunkt in der Datenweitergabe vom MVZ an das Krankenhaus liegen.

Für die Durchführung des Behandlungsvertrags wird in den meisten Fällen aus datenschutzrechtlicher Sicht keine Datenweitergabe an das Krankenhaus erforderlich sein, sodass hier in der Regel eine Einwilligung erforderlich ist.

Gemeinsames Personal

Häufig sind einzelne Mitarbeitende sowohl im MVZ als auch im Krankenhaus angestellt, sodass diese, je nach der aktuell ausgeübten Tätigkeit, auf die Daten der Behandelten des Krankenhauses bzw. des MVZ zugreifen können. Die Informationen, die die Mitarbeitenden in einer Einrichtung über die Behandelten in Erfahrung bringen, dürfen nicht ohne Rücksprache mit der betroffenen Person in der anderen Einrichtung verwendet werden. Aufgrund der jeweils eigenen Verantwortlichkeit der Einrichtungen besteht auch hier wieder die Erforderlichkeit einer Rechtsgrundlage für diese Datenweitergabe.

Eine Ausnahme besteht in Notfallsituationen, in denen keine Rücksprache mit der betroffenen Person gehalten werden kann, die Information für die Notfallbehandlung elementar ist und davon ausgegangen werden kann, dass die betroffene Person in die Weitergabe der Information eingewilligt hätte, wenn sie dazu in der Lage gewesen wäre.

Gemeinsamer OP-Plan

Da das medizinische Personal des Medizinischen Versorgungszentrums neben der IT-Infrastruktur auch die medizinischen Ressourcen des Krankenhauses nutzt, beispielsweise die Operationsräume, bedarf es einer abgestimmten Planung, um Doppelbelegungen zu vermeiden. Hierzu wird regelmäßig ein Zugriff auf das Krankenhaus-Informations-System des Krankenhauses eingerichtet, über den die Belegung der OP-Räume aufgerufen und die Planung von Operationen erfolgen kann.

Dass ein Zugriff auf die Daten der Behandelten des Krankenhauses durch die MVZ-Mitarbeitenden nicht erfolgen darf, ist selbstverständlich und wird meist durch das Berechtigungskonzept grundsätzlich auch abgebildet. An den OP-Plan wird hierbei jedoch häufig nicht gedacht. So können die Mitarbeitenden des MVZ häufig nicht nur sehen, wann ein OP-Raum bereits für eine andere Operation gebucht ist. In vielen Fällen sind auch Angaben zur konkreten Operation, zur operierenden Person und zum Behandelten (Name, Geburtsdatum, Versicherungsdaten und Gesundheitsdaten) hinterlegt.

Die gleiche Problematik besteht in diesen Fällen auch in umgekehrter Richtung, sodass die Mitarbeitenden des Krankenhauses die Daten der MVZ-Operationen sehen können.

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) berichtet in seinem aktuellen Tätigkeitsbericht über einen Sachverhalt, in dem ein MVZ gemeinsam mit diversen Kliniken für die Verarbeitung der Patientendaten ein gemeinsames Krankenhausinformationssystem nutzt. Über den übergreifenden Terminkalender konnten alle beteiligten Einrichtungen sehen, welche Behandelten Termine in der psychiatrischen Klinik des MVZ hatten (40. Tätigkeitsbericht, Punkt 4.5.7).

Diese Sichtbarkeit stellt eine Datenweitergabe dar, für die es einer rechtlichen Grundlage bedarf (siehe oben). Da eine solche nicht besteht, war diese Datenweitergabe unzulässig. Um eine datenschutzkonforme Verarbeitung zu gewährleisten, wäre eine informierte Einwilligung der Behandelten erforderlich, die jedoch eine Folge an Nachfolgeproblemen nach sich ziehen würde (insbesondere Verweigerung oder Widerruf der Einwilligung).

Erschwerend kommt hinzu, dass hierin auch ein Bruch der ärztlichen Schweigepflicht liegt. Auch für diesen gab es keine Grundlage, sodass hierbei sogar eine strafrechtliche Relevanz nach § 203 StGB gegeben ist.

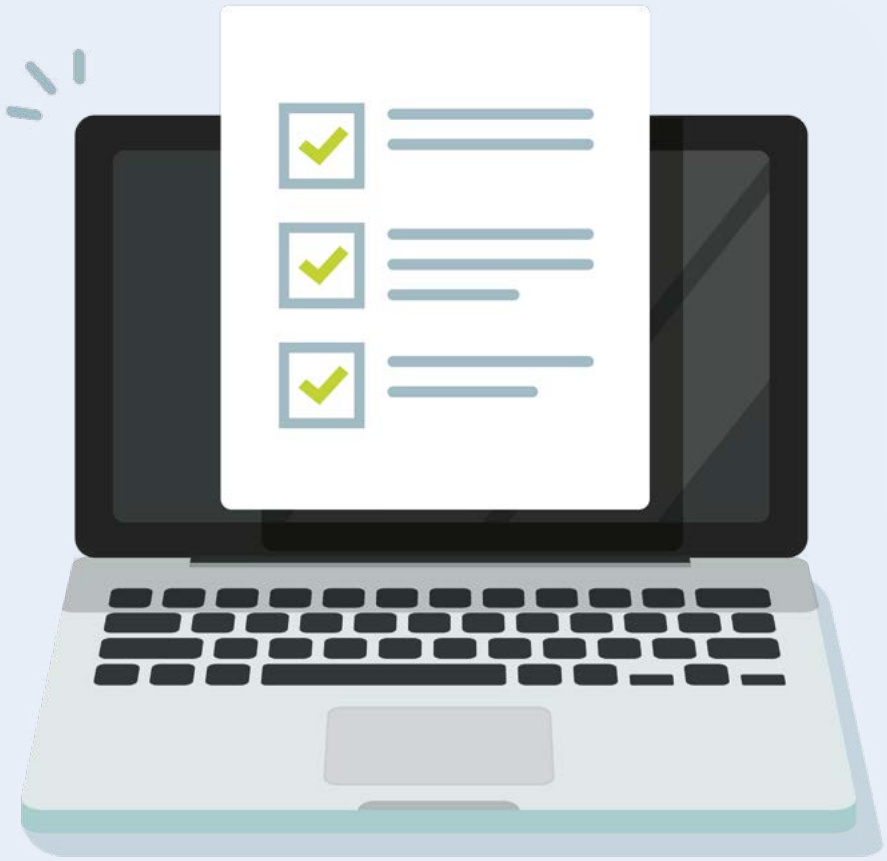
Für die Terminplanung sind derartig weitreichende Informationen, insbesondere zu den Behandelten, nicht erforderlich. Es genügt grundsätzlich, wenn aus der Terminplanung erkennbar ist, dass ein bestimmter OP-Raum zu einem bestimmten Zeitpunkt belegt ist und damit nicht zur Verfügung steht. Welche Operation konkret und an wem durchgeführt wird, spielt keine Rolle. Allenfalls die Information zur operierenden Person kann angezeigt werden, wenn dies für bestimmte Koordinierungen (z. B. Tauschen von Terminbelegungen) erforderlich sein kann.

Datenschutzkonform, so auch das ULD, ist es, wenn die geteilten OP-Kalender so konfiguriert sind, dass die MVZ- bzw. Krankenhaus-Mitarbeitenden ausschließlich ihre Behandelten sehen können. Bereits gebuchte Termine werden dann lediglich farblich als „belegt“ angezeigt.

Kurznotiz

Checkliste zur Cybersicherheit

Bereits seit einiger Zeit stellen der Bayerische Landesbeauftragte für den Datenschutz und das Bayerische Landesamt für Datenschutzaufsicht eine Best-Practice-Checkliste zur Cybersicherheit für medizinische Einrichtungen zur Verfügung. Das entsprechende Dokument kann unter https://www.datenschutz-bayern.de/technik/best_practices/medizin.pdf abgerufen werden und ermöglicht einen ersten „Selbst-Check" der Einrichtung. Dabei werden unter anderem Themen wie Patch-Management, Schutz gegen Malware und Ransomware, Authentisierung, E-Mail-Sicherheit sowie Backups und Notfallkonzepte behandelt. Auch Punkte wie Homeoffice und die Funktion des Datenschutzbeauftragten kommen zur Sprache.



Die Checkliste bietet Datenschutzbeauftragten medizinischer Einrichtungen eine gute Möglichkeit für eine erste Selbstbewertung der Einrichtung.

© AOK-Verlag GmbH | Lilienthalstraße 1-3 | 53424 Remagen | Tel 02642 931-333 | Fax 02642 931-215
Mail: fachinfo@aok-verlag.de | Web: http://www.aok-verlag.info | Herausgeber: AOK-Verlag GmbH, Remagen
Geschäftsführung: Frank Schmidt | Redaktion: Prof. Dr. Benedikt Buchner, Dr. Sebastian Ertel, Sven Venzke-Caprarese
Der Inhalt des vorliegenden Newsletters ist mit größter Sorgfalt zusammengestellt worden.
Eine Haftung für die Angaben übernimmt der Verlag jedoch nicht. | Bildnachweise: GettyImages, AOK-Verlag

Praxishandbuch für Datenschutzbeauftragte im Gesundheitswesen

Welche Patientendaten dürfen an wen und in welcher Form übermittelt werden? Wie ist ein Empfangsbereich im Krankenhaus zu strukturieren, damit die Privatsphäre jedes Einzelnen gewährleistet wird? Wie muss ein Datenschutzkonzept aussehen, damit es als Grundlage für einen Audit dienen kann? Und wer hat eigentlich auf welche Patientendaten Zugriff?

Die Herausforderung ist, dass die innerbetrieblichen Abläufe durch die Umsetzung datenschutzrechtlicher Vorgaben nicht beeinträchtigt werden sollen - ein Spagat, der gemeistert werden muss. Hinzu kommt, dass viele Datenschutzbeauftragte diese Tätigkeit neben ihrem Hauptaufgabengebiet ausüben und sich ein fundiertes Wissen im IT-Bereich erst aneignen müssen, um mit Kollegen oder Externen auf Augenhöhe zu kommunizieren.

Das Handbuch „Datenschutz im Gesundheitswesen“ greift die typischen Arbeits- und Problemfelder auf und liefert Lösungen, die Rechtssicherheit, Nachhaltigkeit und Akzeptanz bei Aufsichtsbehörden bieten. Der Schwerpunkt des Handbuches liegt in der praktischen Umsetzung der datenschutzrechtlichen Vorgaben im betrieblichen Alltag, bspw. bei den spezifischen Anforderungen in den verschiedenen Bereichen des Gesundheitswesens, wie Krankenhaus oder Arztpraxis.

Im exklusiven Online-Kundenbereich finden Sie das Werk als E-Book. Mittels pdf-Download laden Sie kapitelweise Ihr Handbuch herunter und können es direkt an Ihrem Rechner einsetzen. So sind Sie unabhängig von Ihrem Arbeitsort und haben jederzeit Zugriff auf die Datenschutzbestimmungen.

- 2 Ordner mit Register im Format DIN A5,
- ca. 1.500 Seiten Inhalt
- ISBN: 978-3-553-43000-5
- Preis **177,20 €** inkl. MwSt.
- Uneingeschränkter Online-Zugriff
  inkl. 3-4 kostenpflichtige Nachtragslieferungen
  pro Jahr zum Preis von jeweils **89,90 €** inkl. MwSt.
  und versandkostenfreier Zusendung im Inland.