

DATENSCHUTZ UND DATENSICHERHEIT

Schriftliche Ausarbeitung im Rahmen des Seminars

Computer- und Informationsethik

Rolf Haynberg

Matrikelnummer: 1298877

Dozentin: Dr. Jessica Heesen

Wintersemester 09/10

Inhaltsverzeichnis

I	Datenschutz	2
1	Datenschutz in Deutschland	2
2	Datenschutzmaßnahmen	2
3	Einflussfaktoren auf den Datenschutz	3
4	Prinzipien des Datenschutzes	6
II	Datensicherheit	8
5	Sicherheitsbegriffe in der Datensicherheit	9

Teil I

Datenschutz

1 Datenschutz in Deutschland

1970 verabschiedete Hessen als erstes Bundesland der Bundesrepublik ein Datenschutzgesetz [1]. Der Geltungsbereich des Gesetzes umfasste in seiner ursprünglichen Form den Schutz gespeicherter Daten und ihre Verarbeitung vor unerwünschtem Zugriff und Verlust. Seither hat sich die Bedeutung des Begriffs in Deutschland gewandelt und bezeichnet heute vielmehr den *Schutz persönlicher Daten vor Missbrauch*. Das Bundesdatenschutzgesetz (BDSG) definiert in §1 Abs. 1 den Datenschutz als „Schutz des Einzelnen vor Beeinträchtigung seines Persönlichkeitsrechts beim Umgang mit seinen personenbezogenen Daten“ [2].

Grundrechtliche Bedeutung erlangte der Datenschutz durch das Volkszählungsurteil Ende des Jahres 1983. Auf höchstrichterlicher Ebene wurde das Recht auf informationelle Selbstbestimmung als allgemeines Persönlichkeitsrecht festgeschrieben. Geschützt werden muss dabei die Privatsphäre, d. h. die Persönlichkeitsdaten. Der Schutz personenbezogener Daten stützt sich also auf das Prinzip der informationellen Selbstbestimmung [3].

2 Datenschutzmaßnahmen

Die Umsetzung des Datenschutzes erfolgt mit Hilfe der Datenschutzmaßnahmen. Es ist wichtig, diese Maßnahmen als dynamischen Prozess zu verstehen, deren Durchgängigkeit von großer Bedeutung ist. Das heißt, dass die Datenschutzmaßnahmen aufeinander abgestimmt und jeweils an die konkrete Situation angepasst werden müssen. Formulierungen von Maßnahmen sind daher bedeutungslos, wenn das Umfeld und die Zusammenhänge außer Acht gelassen werden. Deswegen können in dieser Arbeit Maßnahmen nur sehr allgemein beschrieben werden. Im Folgenden werden vier der wichtigsten Maßnahmentypen erläutert.

Gesetzliche Datenschutzmaßnahmen Zu nennen sind hier vor Allem das Bundesdatenschutzgesetz sowie die Betroffenenrechte, die sich aus dem Volkszählungsurteil ergeben. Letztere umfassen unter Anderem das Auskunfts-, Benachrichtigungs- und Löschungsrecht (siehe ferner BDSG §6).

Datenschutzkontrollen Datenschutzkontrollen helfen dem Betroffenen, seine Rechte durchzusetzen (siehe oben). Sie lassen sich in Selbst-, Eigen- und Fremdkontrollen aufteilen. Bei der Selbstkontrolle wird der Betroffene selbst aktiv und macht von seinen Rechten Gebrauch. Die Eigenkontrolle geht von der verarbeitenden Stelle aus. Dies kann entweder intern (z. B. durch Auditing) oder von Fremdinstanzen (wie z. B. Datenschutzbeauftragten) durchgeführt werden. Eine Fremdkontrolle wird hingegen stets von Fremdinstanzen (wie z. B. der zuständigen Aufsichtsbehörde) initiiert¹.

Technische und organisatorische Maßnahmen Diese Maßnahmen tragen zur Datensicherheit bei (siehe Teil II). Sie greifen also vor Allem dann, wenn Daten bereits angefallen sind. Einige diese Maßnahmen sind z. B. in der Anlage des BDSG §9 und anderen Gesetzestexten beschrieben.

Risikomanagement Jede Art von Schutz stellt ein Kompromiss dar. Die Abwägung sollte dabei möglichst nachvollziehbar sein. Dies ist das Ziel des Risikomanagements. Wichtige Einflussgrößen sind dabei der potentielle Schaden und seine Eintrittswahrscheinlichkeit, die gewünschten Schutzziele und die verfügbaren Mittel. Eine gute Evaluation der Maßnahmen ist ein unverzichtbarer Teilprozess zur Umsetzung des Datenschutzes (und ist damit selbst eine Datenschutzmaßnahme). Es handelt sich dabei um einen iterativen Prozess.

3 Einflussfaktoren auf den Datenschutz

Der Datenschutz ist ein veränderlicher Begriff: Er unterliegt dem Einfluss vieler Entwicklungen. Die Ausgestaltung der rechtlichen Bestimmungen des Datenschutzes muss früher oder später an diese Entwicklungen angepasst werden. Deshalb ist

¹Weitere Informationen sind unter [4] zu finden.

es wichtig, die Einflussfaktoren rechtzeitig zu erkennen und ihre Bedeutung für den Datenschutz zu verstehen. Während in früheren Jahren ethische Vorstellungen vorrangig waren, sind heute insbesondere informations- und kommunikationstechnische Entwicklungen von Bedeutung. In diesem Abschnitt werden vier wichtige Einflussfaktoren auf die rechtlichen Grundlagen des Datenschutzes genauer betrachtet.

Technikentwicklung Die Entwicklung der Informations- und Kommunikationstechnik zeigte in den vergangenen Jahren einen rasanten Fortschritt. An dieser Stelle soll auf Kennzahlen verzichtet werden². Im Folgenden werden drei Indikatoren der Technikentwicklung, die für den Datenschutz eine wichtige Rolle spielen, genauer betrachtet:

- Immer höhere Kommunikations- und Rechenkapazitäten führen zu einer **Ver-
ringerung von zeitlichen und räumlichen Restriktionen** (vgl. [6]). Die nahezu vollständige Aufhebung räumlicher Distanzen durch das Internet führt dazu, dass Daten leichter erhoben werden können und bereits vorhandene Daten für viele weitere verantwortliche Stellen nutzbar werden. Hohe Rechenkapazitäten erlauben es, immer mehr Daten zu verarbeiten und diese immer aufwendigeren Auswertungen zu unterziehen.
- Der stetig steigende **Grad der Automatisierung** führt zu der Erschließung neuer Bereiche für die Erhebung personenbezogener Daten. Dies sind insbesondere die Bereiche, in denen eine manuelle Erhebung zu aufwendig, zu teuer oder unmöglich ist. Erst automatisierte Lösungen und die damit einhergehenden kostengünstigen Möglichkeiten zur Vervielfältigung der verarbeiteten Daten, ermöglichen Erhebungen mit vertretbaren Kosten.
- Die Fortsetzung dieses Gedankens führt schließlich zum Konzept der **allgegenwärtigen Datenverarbeitung** (*engl. Ubiquitous Computing*): Allgegenwärtige und durchdringende Informationssysteme begleiten den Einzelnen in seiner Umwelt und können so personenbezogene Daten mit hoher Aussagekraft generieren. Mit der Dichte der Informationssysteme nimmt offenbar auch der Um-

²Zahlen hierzu lassen sich z. B. in [5] finden.

fang der erhobenen Daten zu. Gleichzeitig könnte die fortschreitende Miniaturisierung nahezu unbemerkte Erhebungen ermöglichen. Denkbar sind in diesem Zusammenhang beispielsweise kommunikationsfähige Sensoren in Haus, Verkehr und Kleidung. Bereits heute können Entwicklungen in diese Richtung beobachtet werden [7, 8].

Die so erhobenen Daten könnten neue, vielversprechende Anwendungen ermöglichen. Roßnagel ([5]) spricht in diesem Zusammenhang von der Erweiterung der Sinne, der Unterstützung des Gedächtnisses, der Entlastung von Arbeit und der Erhöhung der eigenen Sicherheit.

Gleichzeitig birgt diese technische Entwicklung aber auch Gefahren. Insbesondere das Recht auf informationelle Selbstbestimmung wäre gefährdet, weshalb diese Entwicklung einen großen Einfluss auf Datenschutzregelungen hätte. Roßnagel stellt in seinem Gutachten die These auf, dass das Datenschutzrecht sich nicht nur an die Bedingungen der allgegenwärtigen Datenverarbeitung anpassen, sondern auch seinerseits Einfluss auf deren Entwicklung und Gestaltung gewinnen muss, um informationelle Selbstbestimmung zu ermöglichen. Er fordert daher „eine Modernisierung des Datenschutzrechts, die Datenschutz in die Technik integriert“ [5].

Ethische Anforderungen Werte und Normen einer Gesellschaft sind ebenfalls entscheidende Einflussfaktoren auf den Datenschutz und weisen ebenfalls veränderliche Entwicklungslinien auf. Umgekehrt hängen Entwicklung und Entfaltung einer Gesellschaft grundlegend von datenschutzrechtlichen Bestimmungen ab. Dies macht das Bundesverfassungsgericht (BVerfG) in seinem Urteil zum Volkszählungsurteil deutlich:

„Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.“
(BVerfG, 15.12.1983)

Effizienz, Effektivität und Kosten Jede Art von Schutz stellt ein Kompromiss zwischen Schutzvorkehrungen und aufgewendeten Mitteln (also den Kosten) dar. Weil die verfügbaren Mittel stets begrenzt sind, handelt es sich dabei um einen wichtigen Einflussfaktor. Dies gilt auch für den Datenschutz. Die Kosten können sowohl materieller Art sein, wie etwa finanzielle oder technische Aufwände, oder nichtmateriell, wie zum Beispiel Zeitaufwand, Personal oder Bequemlichkeit. Die Risikoanalyse hilft dabei, die Maßnahmen angemessen zu wählen (siehe Risikomanagement, Seite 3).

Rechtliche Anforderungen Einfluss auf die Ausgestaltung rechtlicher Bestimmungen des Datenschutzes haben ebenfalls die bestehenden, rechtlichen Anforderungen. Diese gesetzlichen Grundlagen betrachten den Datenschutz gewöhnlich aus zwei Perspektiven (vgl. [9]): Zum einen kann Privatheit als Besitz aufgefasst werden. In diesem Fall wird eine Verletzung des Datenschutzes als *Datendiebstahl* verstanden. Andererseits kann Privatheit auch als eine gewisse Art von Schutz aufgefasst werden. Die Verletzung des Datenschutzes wird dann als Angriff auf beispielsweise das Recht auf Persönlichkeitsentfaltung verstanden.

4 Prinzipien des Datenschutzes

In den letzten Abschnitten wurde deutlich, dass die Ziele, die Maßnahmen und auch die Einflussfaktoren des Datenschutzes situationsabhängig sind. Umso wichtiger ist es, situationsunabhängige Gemeinsamkeiten zu finden. Diese allgemein gültigen Prinzipien bieten unter Anderem Anhaltspunkte um Datenschutzregelungen zu gestalten. Wie diese Prinzipien später umgesetzt werden, ist wiederum bereichsabhängig. Darüber hinaus können die Prinzipien in einigen Fällen helfen, die Datenschutzfreundlichkeit von Prozessen zu beurteilen. Dies ist hilfreich, da es Maßnahmen gibt, bei denen nicht direkt ersichtlich ist, ob sie den Datenschutz gefährden oder fördern. Einige der wichtigsten Prinzipien werden im Folgenden erläutert³.

³Weiterführende Informationen zu den hier beschriebenen Prinzipien finden sich beispielsweise in [6].

Verbot mit Erlaubnisvorbehalt Regelungen, die festlegen, wann eine Datenverarbeitung von persönlichen Daten zulässig ist, können nach zwei dualen Methoden konstruiert werden: Entweder die Datenverarbeitung ist grundsätzlich erlaubt und Ausnahmen werden explizit geregelt (Erlaubnis mit Verbotsvorbehalt) oder aber, das Erheben, Verarbeiten oder Nutzen personenbezogener Daten ist zunächst verboten. Das Verbot kann in diesem Fall nur dann außer Kraft gesetzt werden, wenn eine ausdrückliche Gestattungserlaubnis vorliegt (Verbot mit Erlaubnisvorbehalt). Letztere beschreibt ein Prinzip des Datenschutzes.

Der Datenschutz in Deutschland orientiert sich an diesem Prinzip. Bei der Zulässigkeitsprüfung wird verlangt, dass mindestens einer der folgenden Fälle zutrifft:

1. Es existiert eine Einwilligung des Betroffenen: Eine solche Einwilligung muss auf einer freiwilligen Entscheidung des Betroffenen basieren. Darüber hinaus muss der Betroffene u. A. über den geplanten Zweck umfassend informiert worden sein.
2. Die Daten sind öffentlich: Daten können als öffentlich angesehen werden, wenn der Betroffene sie offenkundig selbst veröffentlicht hat oder eine entsprechende Einwilligungserklärung für die Veröffentlichung vorliegt.
3. Es liegt eine gesetzliche Ermächtigung vor: Gesetze, Verordnungen oder Satzungen können als gesetzliche Erlaubnis angesehen werden, wenn diese ausdrücklich das Erheben, Verarbeiten oder Nutzen gestatten.

Zweckentsprechung Jedes Verfahren zur Datenverarbeitung folgt einem Zweck. Dieser Zweck sollte bereits vor der Erhebung festgelegt und dem Betroffenen mitgeteilt werden. Das Prinzip der Zweckentsprechung fordert nun, dass dieser Zweck der Datenverarbeitung abhängig von der geplanten Verwendung der Daten ist.

Transparenz Um den Datenschutz zu wahren, ist es wichtig, dass der Betroffene die Verfahren kennt und nachvollziehen kann. Das Prinzip der Transparenz fordert genau dies. Es zeigt sich beispielsweise in der Wahrung des Auskunftsrechts und in der Benachrichtigungspflicht.

Direkterhebung Das Prinzip der Direkterhebung besagt, dass erforderliche Daten direkt vom Betroffenen erhoben werden. Dies führt gleichzeitig auch zu mehr Transparenz des Verfahrens.

Datensparsamkeit und Verhältnismäßigkeitsprinzip Ziel ist es, die Datenerhebung und –speicherung, wenn möglich, zu vermeiden. Dazu dürfen insbesondere nur so viele Daten erhoben werden, wie notwendig oder erforderlich sind, um unverhältnismäßigen Aufwand oder unverhältnismäßige Kosten zu vermeiden. Dem förderlich sind die so genannten *datenschutzfreundlichen Techniken*.

Teil II

Datensicherheit

Die Datensicherheit⁴ umfasst „alle relevanten Informationen einer Organisation oder eines Unternehmens, einschließlich personenbezogener Daten“[3]. Dabei spielt die Form, in der die Informationen vorliegen, keine Rolle. Sie befasst sich also neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch mit der Sicherheit von nicht-elektronisch verarbeiteten Informationen. Die Sicherheit von Informationen rund um IT-Systeme wird als *IT-Sicherheit* bezeichnet.

Obwohl Datensicherheit eine größere Klasse von Daten umfasst, ist Datenschutz kein Teilaspekt der Datensicherheit. Denn Datenschutz umfasst z. B. eine deutlich umfangreichere Menge von Maßnahmen. Datensicherheit ist notwendig für effektiven Datenschutz aber nicht hinreichend. Dieser Zusammenhang ist in Abbildung 1 dargestellt.

In Bezug auf Datenschutz beschreibt Datensicherheit in der Regel die technischen und organisatorische Maßnahmen (vgl. [10]). Diese sind in der Anlage zum §9 BDSG und in den Landesdatenschutzgesetzen beschrieben.

⁴In der Literatur wird häufig auch der Begriff *Informationssicherheit* verwendet.

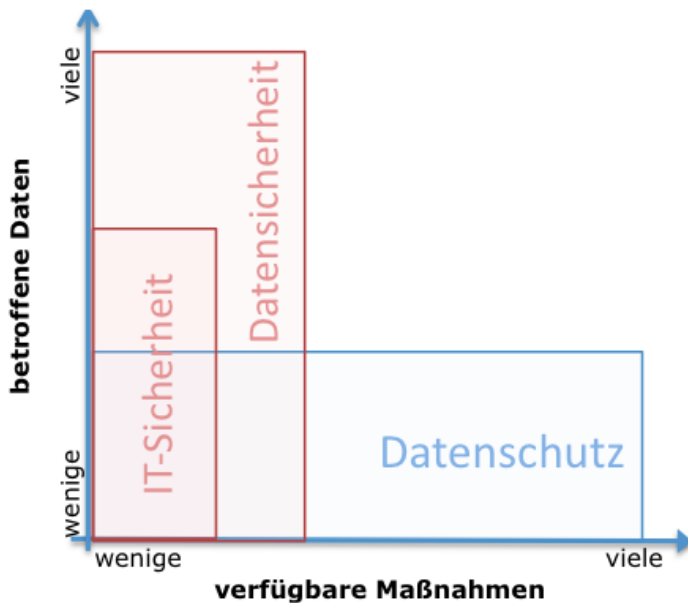


Abbildung 1: Datenschutz und Datensicherheit überschneiden sich in Daten und Maßnahmen. Jedoch umfasst der Datenschutz noch weitere Maßnahmen, während Datensicherheit eine größere Menge von Daten betrifft. IT-Sicherheit ist ein Teil der Datensicherheit.

5 Sicherheitsbegriffe in der Datensicherheit

In der klassischen und allgemein anerkannten Definition ([10, S. 63]) von Datensicherheit ist mit dem Begriff der Sicherheit eigentlich *Verlässlichkeit* gemeint. Darunter fallen drei Sicherheitskriterien:

Verfügbarkeit (*engl. availability*) Die Verfügbarkeit gewährleistet, dass Daten für befugte Nutzer zugänglich sind. Bei technischen Systemen wird sie meist durch die Ausfallzeit des betrachteten Systems quantisiert.

Vertraulichkeit (*engl. privacy*) Gewährleistung, dass Daten nur durch befugte Nutzer interpretiert werden können. Diese allgemeine Definition schließt implizit auch Zugriffskontrollen mit ein. Denn Daten, auf die unbefugte Nutzer keinen Zugriff haben, können in diesem Sinne auch nicht interpretiert werden. Besonders wichtig ist dabei auch, dass die Authentizität der Nutzer entsprechend gewährleistet wird.

Integrität (*engl. integrity*) Gewährleistung, dass Daten nur durch befugte Nutzer verändert werden können. Darunter fällt auch, dass Daten nicht von Unbefugten vernichtet oder unbrauchbar gemacht werden können. Da nach Definition

für die Integrität eine Unterscheidung zwischen befugten und unbefugten Nutzern notwendig ist, muss in der Praxis auch die Authentizität gewährleistet sein.

Datensicherheit hat laut dieser Definition also das Ziel, Daten jeglicher Art in ausreichendem Maße vor Verlust, Manipulationen, unberechtigter Kenntnisnahme durch Dritte und anderen Bedrohungen zu schützen.

Es gibt noch zwei weitere Sicherheitskriterien, die insbesondere für die IT-Sicherheit von Bedeutung sind und zusammenfassend mit dem Begriff der *Beherrschbarkeit* beschrieben werden. Werden die Kriterien der Verlässlichkeit hinzugenommen, ist von *mehrseiter IT-Sicherheit*⁵ die Rede.

Zurechenbarkeit (*engl. accountability*) Die Zurechenbarkeit fordert, dass jederzeit bezüglich eines Prozesses festgestellt werden kann, welche Person oder welcher Prozess diesen ausgelöst hat. Diese Definition umfasst zum Einen die Forderung nach einem Prozess, der eine solche Protokollierung erlaubt und zum Anderen wird (implizit) auch ein Mechanismus gefordert, der es erlaubt, die Personen oder die Prozesse eindeutig zu identifizieren. Zurechenbarkeit gewährleistet also implizit auch Authentizität. Die Eigenschaft also, die auch für Vertraulichkeit und Integrität eine wichtige Voraussetzung ist (siehe oben).

Rechtsverbindlichkeit (*engl. legal-liablility*) Diese Eigenschaft gewährleistet, dass Vorgänge gegenüber Dritten jederzeit rechtskräftig nachgewiesen werden können. Die Forderung nach Rechtsverbindlichkeit ist somit eine Forderung nach Korrektheit der Prozesse, die verwendet werden, um Sicherheit zu gewährleisten. Ohne einen solchen Kontrollmechanismus ist es möglich, dass Prozesse so inhärent fehlerbehaftet sind, dass sie nach außen kein Fehlverhalten erkennen lassen. Dies würde die Sicherheitsbegriffe bedeutungslos machen.

Literatur

[1] *RFID Journal - FAQ*. <http://www.rfidjournal.com/faq>, Abruf: 13.04.2010

⁵Ausführliche Informationen zu diesem Thema lassen sich in [10] finden.

- [2] ANDY FELONG: *Andy's Wearable Computing Notebook*. <http://redwoodhouse.com/wearable>, Abruf: 13.04.2010
- [3] DER BUNDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSSICHERHEIT: *Datenschutzkontrolle*. http://www.bfdi.bund.de/cln_029/nn_531474/DE/Themen/GrundsatzlichesZumDatenschutz/Einzelfragen/Artikel/Datenschutzkontrolle.html__nnn=true, Abruf: 12.04.2010
- [4] HESSISCHES MINISTERIUM FÜR DES INNEREN UND FÜR SPORT: *Informationen zum Datenschutz*. http://www.hessen.de/irj/HMdI_Internet?cid=6f321fe2e5aca033c1f7bfe5890df8f0, Abruf: 12.04.2010
- [5] JURIS GMBH (Hrsg.): *Bundesdatenschutzgesetz (BDSG)*. Bundesministerium der Justiz in Zusammenarbeit mit der juris GmbH, 1990 http://www.gesetze-im-internet.de/bundesrecht/bdsg_1990/gesamt.pdf. – Zuletzt geändert durch Art. 1 G v. 14.8.2009 I 2814, Letzter Abruf: 12.04.2010
- [6] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD): *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html, Abruf: 13.04.2010
- [7] POMMERENING, Prof. Dr. K.: *Datenschutz und Datensicherheit*. Mainz : Johannes-Gutenberg-Universität, 1991 <http://www.staff.uni-mainz.de/pommeren/Artikel/ds.pdf>. – Letzer Abruf: 13.04.2010
- [8] ROSSNAGEL, Prof. Dr. A.: *Datenschutz im 21. Jahrhundert*. Bd. APuZ 5-6/2006. Nora-Platiel-Str. 5, 34109 Kassel : Bundeszentrale für Politische Bildung, 2006 <http://www.bpb.de/publikationen/9GGQGR.html>. – Letzter Abruf: 12.04.2010
- [9] ROSSNAGEL, Prof. Dr. A. ; BEATE MARTIN, Thomas D. (Hrsg.): *Gutachten: Datenschutz in einem informatisierten Alltag*. Hiroshimastraße 17, D-10785 Berlin : Stabsabteilung der Friedrich-Ebert-Stiftung, 2007 <http://www.fes.de/stabsabteilung>. – ISBN 978-3-89892-681-2

- [10] *Kapitel 6: Informational Privacy: Concepts, Theories and Controversies.*
In: TAVANI, Herman T.: *The Handbook of Information and Computer Ethics.*
John Wiley & Sons, Inc., 2008
- [11] WIKIPEDIA-COMMUNITY: *Informationssicherheit.* de.wikipedia.org/wiki/Informationssicherheit, Abruf: 1.12.2009
- [12] WITT, Bernhard C.: *IT-Sicherheit kompakt und verständlich : Eine praxisorientierte Einführung.* Wiesbaden : Friedr.Vieweg & Sohn Verlag / GWV Fachverlage GmbH, 2006 <http://dx.doi.org/10.1007/978-3-8348-9077-1>.
– ISBN 978-3-8348-9077-1. – In: Springer-Online
- [13] WITT, Bernhard C.: *Datenschutz kompakt und verständlich : Eine praxisorientierte Einführung.* Wiesbaden : Friedr.Vieweg Sohn Verlag — GWV Fachverlage GmbH, 2008 <http://dx.doi.org/10.1007/978-3-8348-9442-7>. – ISBN 978-3-8348-9442-7. – In: Springer-Online