Vassilios Karanikas

Ein Leitfaden für die Berücksichtigung datenschutzrechtlicher Fragen bei der Entwicklung von betrieblichen Anwendungssystemen

Diplomarbeit

Diplom.de

Bibliografische Information der Deutschen Nationalbibliothek:

Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de/ abrufbar.

Dieses Werk sowie alle darin enthaltenen einzelnen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsschutz zugelassen ist, bedarf der vorherigen Zustimmung des Verlages. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen, Auswertungen durch Datenbanken und für die Einspeicherung und Verarbeitung in elektronische Systeme. Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Copyright © 2004 Diplom.de
ISBN: 9783832486518

https://www.diplom.de/document/223845

Vassilios Karanikas

Ein Leitfaden für die Berücksichtigung datenschutzrechtlicher Fragen bei der Entwicklung von betrieblichen Anwendungssystemen

Diplom.de

Karanikas Vassilios

Ein Leitfaden für die Berücksichtigung datenschutzrechtlicher Fragen bei der Entwicklung von betrieblichen Anwendungssystemen

Diplomarbeit
Universität - Gesamthochschule Essen
Fachbereich Wirtschaftswissenschaften
Abgabe Januar 2004

Diplomica GmbH
Hermannstal 119k
22119 Hamburg

Fon: 040 / 655 99 20
Fax: 040 / 655 99 222

agentur@diplom.de
www.diplom.de

ID 8651
Vassilios, Karanikas: Ein Leitfaden für die Berücksichtigung datenschutzrechtlicher Fragen bei der Entwicklung von betrieblichen Anwendungssystemen
Hamburg: Diplomica GmbH, 2005
Zugl.: Universität - Gesamthochschule Essen, Diplomarbeit, 2004

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtes.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Die Informationen in diesem Werk wurden mit Sorgfalt erarbeitet. Dennoch können Fehler nicht vollständig ausgeschlossen werden, und die Diplomarbeiten Agentur, die Autoren oder Übersetzer übernehmen keine juristische Verantwortung oder irgendeine Haftung für evtl. verbliebene fehlerhafte Angaben und deren Folgen.

Diplomica GmbH
http://www.diplom.de, Hamburg 2005
Printed in Germany

I. Inhaltsverzeichnis

II. Abbildungsverzeichnis ... 3

III. Tabellenverzeichnis ... 4

IV. Abkürzungsverzeichnis ... 5

1 Einleitung und Aufgabenstellung ... 7

2 Grundlagen betriebswirtschaftlicher Anwendungen ... 9

2.1 Information und Daten ... 9
2.2 Systembetrachtung ... 10
2.3 Betriebliche Anwendungssysteme ... 11

3 Grundlagen des Datenschutzes ... 15

3.1 Terminologie des Datenschutzes und der Datensicherheit ... 15
3.2 Gesetzliche Rahmenbedingungen ... 17
3.2.1 EG-Datenschutzrichtlinie ... 17
3.2.2 EU-Datenschutzrichtlinie für elektronische Kommunikation ... 19
3.2.3 Bundesdatenschutzgesetz ... 20
3.2.4 Multimediagesetze ... 27

4 Systementwicklung ... 34

4.1 Beschreibung von Vorgehensmodellen ... 35
4.2 Phasenkonzept ... 39

5 Vorphase der Projektbegründung ... 42

5.1 Projekt und Projektmanagement ... 43
5.2 Möglichkeiten datenschutzrechtlicher Maßnahmen ... 45
5.3 Mitwirkung des Datenschutzbeauftragten im Entwicklungsprozess ... 46
5.3.1 Bestellung eines Datenschutzbeauftragten ... 47
5.3.2 Aufgaben des Datenschutzbeauftragten ... 49
5.4 Technische und organisatorische Vorüberlegungen ... 52
5.4.1 Risikomanagement ... 53
5.4.2 Wirtschaftlichkeit ... 55

6 Analyse ... 57

6.1 Analyse des Ist-Zustandes ... 57

6.1.1 Methoden zur Erfassung des Ist-Zustandes ... 58
6.1.2 Internwirksame Schicht ... 59
6.1.2.1 Personalinformationssystem ... 59
6.1.2.2 Datenschutzrechtliche Fragen ... 60
6.1.3 Externwirksame Schicht ... 65
6.1.3.1 E-Commerce-Anwendungen ... 65
6.1.3.2 Datenschutzrechtliche Fragen ... 66
6.1.4 Datenauswertung und Datenverwendung ... 69
6.1.5 Informationspflichten und Kennzeichnungspflichten ... 73
6.1.6 Rechte der Betroffenen ... 75
6.1.7 Technisch-organisatorische Ist-Zustandserfassung ... 77
6.2 Soll-Konzept ... 81
6.2.1 Grundsatz der Transparenz ... 82
6.2.2 Datensparsamkeit und Datenvermeidung ... 85
6.2.3 Anforderungen an die Datenverarbeitung ... 87
6.2.4 Technisch-organisatorische Anforderungen ... 89

7 Entwurf ... 98

7.1 Einsatzbedingungen ... 98
7.2 System- und Programmentwurf ... 99

8 Realisierung und Test ... 104

8.1 Prinzipien der Programmierung ... 104
8.2 Programm- und Systemtest ... 107

9 Einführungsphase ... 110

10 Wartung ... 112

10.1 Anforderungen an die Wartung ... 112
10.2 Datenschutz in der Wartungsphase ... 114

11 Konzept der Zertifizierung ... 118

11.1 Zertifizierungsprozess ... 118
11.2 Datenschutzaudit ... 120

12 Zusammenfassung und Schlussfolgerung ... 126

Literatur- und Quellenverzeichnis ... 128

Eidesstattliche Versicherung ... 142

II. Abbildungsverzeichnis

Abbildung 1: Entwicklungsphasen der Information 10
Abbildung 2: Strömungsgrössen zwischen den Elementen 11
Abbildung 3: Klassifizierung der Operationen 23
Abbildung 4: Das Wasserfall-Modell 35
Abbildung 5: Das V-Modell 37
Abbildung 6: Das Spiralmodell 38
Abbildung 7: Datenschutzbeauftragte in Unternehmen 47
Abbildung 8: PIS als integrativer Bestandteil eines Gesamtsystems 60
Abbildung 9: Modell eines PIS 61
Abbildung 10: Knowledge Discovery in Databases-Prozess 71
Abbildung 11: Asymmetrische Verschlüsselung 80
Abbildung 12: Modell der Zugriffskontrolle 92
Abbildung 13: Die Verteilung der Wartungstätigkeiten 114
Abbildung 14: Der Zertifizierungsprozess 119

III. Tabellenverzeichnis

Tabelle 1: Standardsoftware versus Individualsoftware 13
Tabelle 2: Aufbau des BDSG 26
Tabelle 3: Ebenen des Kommunikationsprozesses 28
Tabelle 4: Kontrollfunktionen des Betriebsrats 64
Tabelle 5: Rechte des Betroffenen 77
Tabelle 6: Pflichten von Auftragnehmer und Auftraggeber bei der Auftragskontrolle 96
Tabelle 7: Datenschutzrechtliche Regelungen der Wartung in der privaten Wirtschaft 117
Tabelle 8: Vor- und Nachteile des Datenschutzaudits 122

IV. Abkürzungsverzeichnis

Abs. .....Absatz
ACM .....Association for Computing Machinery
Art. .....Artikel
Az. .....Aktenzeichen
BAG .....Bundesarbeitsgericht
B.A.T .....British American Tobacco
Bd. .....Band
BDA .....Bundesvereinigung der Deutschen Arbeitgeberverbände
BDI .....Bundesverband der Deutschen Industrie
BDSG .....Bundesdatenschutzgesetz
BetrVG .....Betriebsverfassungsgesetz
BfD .....Bundesbeauftragter für den Datenschutz
BGB .....Bürgerliches Gesetzbuch
BGBl .....Bundesgesetzblatt
BSI .....Bundesamt für Sicherheit in der Informationstechnik
BVerfGE .....Bundesverfassungsgericht
bzgl. .....bezüglich
bzw. .....beziehungsweise
CLF .....Common Logfile Format
d. h. .....das heißt
DIN .....Deutsches Institut für Normung
DKE .....Deutsche Kommission Elektrotechnik Elektronik Informationstechnik
DNS .....Desoxyribonukleinsäure
DSAVO .....Datenschutzauditverordnung
DSL .....Digital Subscriber Line
DuD .....Datenschutz und Datensicherheit (Zeitschrift)
DV .....Datenverarbeitung
EDI .....Electronic Data Interchange
e. g. .....example given
EG .....Europäische Gemeinschaft
EU .....Europäische Union
e. V. .....eingetragener Verein
EVA .....Eingabe, Verarbeitung, Ausgabe
f. .....folgende
ff. .....fortfolgende
GmbH .....Gesellschaft mit beschränkter Haftung
GS .....Gesetz
GVOBL .....Gesetz- und Verordnungsblatt
Hrsg. .....Herausgeber
ICANN .....Internet Corporation for Assigned Names and Numbers
i. d. R. .....in der Regel
IDS .....Intrusion Detection Systems
i.e. .....in example
IEC .....International Electrotechnical Commission
IEEE .....Institute of Electrical and Electronics Engineers
i. e. S. .....im engeren Sinn
incl. . .....inclusive
IP .....Internet Protokoll
IPv4 .....Internet Protokoll Version 4
i. S. d. .....im Sinne des
ISDN .....Integrated Service Digital Network
ISO .....International Organization for Standardization
IT .....Informationstechnologie

ITSEC .....Information Technology Security Evaluation Criteria
ITSEM .....Information Technology Security Evaluation Manual
IuKDG .....Informations- und Kommunikationsdienste-Gesetz
IV .....Informationsverarbeitung
i. w. S. .....im weiteren Sinn
KDD .....Knowledge Discovery in Databases
LDSG-SH .....Landesdatenschutzgesetz Schleswig Holstein
MDStV .....Mediendienste-Staatsvertrag
MIT .....Massachusetts Institute of Technology
MMR .....Multimedia und Recht (Zeitschrift)
NJW .....Neue Juristische Wochenschrift (Zeitschrift)
Nr. .....Nummer
NWGVBl .....Nordrhein-Westfalen Gesetz- und Verordnungsblatt
OSI .....Open Systems Interconnection
o.V. .....ohne Verfasser
PAISY .....Personalabrechnungs- und Informationssystem
PET .....Privacy enhancing technologies
PGP .....Pretty Good Privacy
PIN .....Personal Identification Number
PIS .....Personalinformationssystem
RDV .....Recht der Datenverarbeitung (Zeitschrift)
RegTP .....Regulierungsbehörde für Telekommunikation und Post
S. .....Seite
SAP .....Systeme, Anwendungen, Produkte in der Datenverarbeitung
Sch.-H. .....Schleswig-Holstein
SGB .....Strafgesetzbuch
SigG .....Signaturgesetz
SprAuG .....Sprecherausschußgesetz
TDDSG .....Teledienstedatenschutzgesetz
TDG .....Teledienstegesetz
TDSV .....Telekommunikations-Datenschutzverordnung
TKG .....Telekommunikationsgesetz
u. a. .....und andere
ULD .....Unabhängiges Landeszentrum für Datenschutz
usw. .....und so weiter
v. .....vom
vgl. .....vergleiche
z. B. .....zum Beispiel

1 Einleitung und Aufgabenstellung

Die globale Vernetzung und die rasante Entwicklung in der Informations- und Kommunikationstechnik weist immer größere Mittel und Chancen der Datenverarbeitung, des Datentransfers und der Datenauswertung auf. Der zunehmende Handel mit Daten und Informationen und die Beurteilung der Werthaltigkeit von Unternehmen, gemessen an dem Bestand von Kundendaten, impliziert bei Unternehmen eine größere Bedeutung des Aspektes Einhaltung von datenschutzrechtlichen Vorgaben [SPI02, S. 177]. Möglichst viele Informationen insbesondere personenbezogene Daten zu sammeln und auszuwerten mit dem Ziel, neue Geschäftsfelder aufzudecken, wird als primärer Antrieb von Unternehmen betrachtet [TIN98, S. 5]. Die Ware „*Information*“ wird folglich von Unternehmen verstärkt als strategischer Wettbewerbsfaktor bezeichnet [BÜL00, S. 1]. Die negative Folge der Ausweitung an Informationen sind immer größere Datenschutzprobleme und Gefahren auf die sich Unternehmen, Behörden und einzelne Personen nur bedingt einstellen können. Daher bedarf es klarer Regelungen, wie die informationelle Selbstbestimmung des Individuums vor allgemeiner Verfügbarkeit seiner Daten zu schützen ist. Zum Schutze der informationellen Selbstbestimmung hat die Europäische Union Datenschutzrichtlinien eingeführt mit der Zielausrichtung, im Bereich der Technologieentwicklung einen gemeinsamen Standard zu erreichen. Die Datenschutzrichtlinien sind in den europäischen Ländern in nationales Gesetz umzusetzen bzw. umgesetzt worden. In Deutschland wird der Datenschutz durch das Bundesdatenschutzgesetz (BDSG) und zahlreiche bereichsspezifische Rechtsvorschriften geregelt.

Basierend auf der Zielsetzung einen Leitfaden für Unternehmen zu entwickeln, werden zunächst die grundlegenden Begrifflichkeiten erläutert, die im Kontext mit betrieblichen Anwendungssystemen stehen. Dazu gehört die Erläuterung der Begriffe Information, System und die Abgrenzung des Begriffes Anwendungssystem. Diese Diplomarbeit, die als Empfehlung für Unternehmen und nicht als verbindliche Richtlinie anzusehen ist, orientiert sich am Lebenszyklus von Produkten, speziell denen der betrieblichen Anwendungssysteme, die anhand des Phasenkonzeptes auf datenschutzrechtliche Fragen untersucht werden. Die Aufteilung anhand des Phasenmodells im Rahmen eines IT-Projektes soll aufzeigen, dass der Datenschutz nicht erst auf der Anwendungsebene zu unterstützen ist, sondern bereits zum Zeitpunkt der Vorüberlegung und Gestaltung von Anwendungssystemen datenschutzrechtliche Aspekte zu beachten sind.

Die grundlegendsten und wichtigsten Datenschutzgesetze, das BDSG und bereichsspezifische Vorschriften im Zusammenhang mit Anwendungssystemen sind inhaltliche Schwerpunkte des zweiten Kapitels. Anschließend erfolgt ein Überblick über die unterschiedlichen Arten von Vorgehensmodellen zur Systementwicklung und das für diese Arbeit ausgewählte Phasenkonzept. Das klassische Phasenkonzept mit dem Aufbau Vorphase, Ist-Analyse, Soll-Konzeption, Entwurf, Realisierung, Test, Einführung und Wartung dient als Basis für die Verknüpfung datenschutzrechtlicher Fragen bei der Entwicklung von betrieblichen Anwendungssystemen. Die Zertifizierung und Datenschutzauditierung als neue Instrumente des Datenschutzes werden im Hinblick auf Anwendungen der Informationstechnologie explizit im Kapitel 11 betrachtet. Abschließend erfolgt die Beurteilung von datenschutzrechtlichen Regelungen im Hinblick auf die Entwicklung von betrieblichen Anwendungssystemen.

2 Grundlagen betriebswirtschaftlicher Anwendungen

Ziel dieses Kapitels ist die Einführung in die allgemeinen Grundlagen der betriebswirtschaftlichen Anwendungen. Die Begrifflichkeiten Information, System und betriebliche Anwendungssysteme werden zunächst definiert und erläutert, bevor wesentliche Aspekte für die software-technische Entwicklung von betrieblichen Anwendungssystemen diskutiert werden.

2.1 Information und Daten

Die Disziplin Wirtschaftsinformatik setzt sich mit Systemen zur Beschaffung, Verarbeitung, Übertragung, Speicherung und Bereitstellung von Informationen auseinander. Dieser Komplex konkretisiert sich im Begriff der Informationsverarbeitungssysteme. Die Begriffe Information und Daten, die in inhaltlichem Zusammenhang stehen, weisen eine grundlegende Bedeutung auf. Der Terminus Information leitet sich aus der lateinischen Vokabel „*informatio*“ ab und bedeutet „*Erläuterung oder Deutu*ng“. In der Literatur herrscht keine einheitliche Verwendung des Begriffes Information vor. In der Theorie der Nachrichtenübertragung bedeutet Information Kenntnis über Abläufe, Tatsachen oder Ereignisse [SCW00, S. 39]. Umgangssprachlich wird unter Information das Wissen über Sachverhalte und Vorgänge verstanden. Der in der Betriebswirtschaftslehre verbreitete Informationsbegriff sieht in der Information das zweckgebundene bzw. zielgerichtete Wissen mit dem Zweck, wirtschaftliches Handeln vorzubereiten und durchzuführen, mit dem ein Teil der Realität durch Daten abgebildet wird. Eine Konkretisierung der Bezeichnung Information im Informatikbereich ist noch nicht erfolgt [GRA97, S. 22]. Die folgende Verwendung der Bezeichnung Information ist an die Definition der Betriebswirtschaftslehre angelehnt.

Die kleinste Informationseinheit stellen Zeichen dar. Unter Zeichen versteht man „ ... *Elemente zur Darstellung von Daten bzw. Informationen.*“ [SCW00, S. 41]. Zeichen können in der Form der Musik, der Sprache oder bei Zahlen zum Ausdruck kommen. Die Semiotik, die Lehre von Zeichen, kann in die folgend genannten Ebenen unterteilt werden [SCW00, S. 41 f.]: