

Inhaltsverzeichnis

Literaturverzeichnis.....	XV
Einleitung	1
Terminologischer Epilog.....	3
I. Abgrenzung von Daten und Informationen.....	3
1. Daten.....	3
2. Informationen	4
II. Relevante Datenarten	6
1. Inhaltsdaten.....	6
2. Bestandsdaten	6
3. Nutzungsdaten	7
4. Verkehrs- und Abrechnungsdaten	7
III. Netzwerkarchitektur.....	8
1. Client-Server.....	8
2. Peer-to-Peer	8
IV. Softwarearchitektur	9
Teil 1: B2B im Internet	11
I. B2B als integraler Bestandteil des Electronic Business.....	11
II. Entwicklungsstufen des B2B	12
1. Datenaustausch via EDI	12
2. Plattformbezogenes E-Business	13
3. E-Business-Integration	14
4. Dynamisches E-Business	15
4. Ausblick.....	18
III. Datenverarbeitungsprozesse des B2B.....	18
1. Enterprise Resource Planning	19
2. Customer Relationship Management	19
3. Identitätsmanagement.....	21

4. Data Warehousing	21
5. Data Mining.....	23
IV. Zusammenfassung	24
Teil 2: Verfassungsrechtlicher Schutz von Daten im B2B	25
I. Grundrechtsberechtigung der Unternehmen im B2B.....	25
II. Staatliche Schutzpflichten aus Grundrechtsschutz	27
III. Wirkung des Grundrechtsschutzes zwischen Unternehmen.....	28
III. Persönlichkeitsrechtsschutz für Daten.....	30
1. Informationelle Selbstbestimmung	31
2. Vertraulichkeit und Integrität informationstechnischer Systeme.....	32
3. Persönlicher Schutzbereich	33
4. Konsequenzen für den B2B.....	35
IV. Telekommunikationsgeheimnis für Daten im B2B.....	36
1. Sachliche Anwendbarkeit.....	36
2. Persönliche Gewährleistung	38
3. Konsequenzen für den B2B.....	39
V. Eigentumsgarantie für Daten im B2B.....	39
1. Gewerbliche Schutzrechte	39
2. Betriebs- und Geschäftsgeheimnisse.....	40
3. „Geronnene Vermögenswerte“	41
4. Mittelbarer Schutz als Bestandteil des Gewerbebetriebs.....	43
5. Konsequenzen für den B2B.....	44
VI. Unternehmerische Betätigungsfreiheit und Daten im B2B.....	45
VII. Wirtschaftliche Handlungsfreiheit und Daten im B2B.....	47
VIII. Zusammenfassung.....	47
Teil 3: „Datenschutz“ für Unternehmensdaten	49
I. Schutz vorgehaltener personenbezogener Daten.....	49
1. Anwendbares Datenschutzrecht	49

2. Personenbezug der Daten	52
3. Datenverarbeitungsvorgänge im B2B	54
a. Datenerhebung	54
b. Datennutzung	55
c. Datenverarbeitung im engeren Sinne	55
aa. Speicherung	55
bb. Veränderung	56
cc. Übermittlung	56
dd. Sperrung	57
ee. Löschung	58
d. Datenverarbeitung im Auftrag	58
4. Verwendung von Daten für eigene Geschäftszwecke	60
a. Eigene Geschäftszwecke	61
b. Vertragliche oder vertragsähnliche Zweckbestimmung	61
c. Wahrung berechtigter Interessen	62
d. Allgemein zugängliche Daten	63
e. Zweckkonkretisierung	64
f. Konzerninterner Datenaustausch	65
5. Verwendung von Daten als Handelsgegenstand	67
6. Einwilligung der Betroffenen in die Datenverwendung	68
a. Entscheidungsautonomie	69
b. Aufklärung der Betroffenen	69
c. Befugnis zur Einwilligung	71
d. Form der Einwilligung	71
7. Determinanten der Datenverarbeitung im B2B	74
a. Direkte und informierte Erhebung	74
b. Zweckbindung	75
c. Datenvermeidung und Datensparsamkeit	76

d. Vertraulichkeit und Sicherheit der Daten	77
e. Bestandsschutz	77
8. Zwischenergebnis	78
II. Schutz übertragener Daten	78
1. Abgrenzung von Datenschutz- und Telekommunikationsrecht.....	79
2. Wirkung des Fernmeldegeheimnisses im B2B	80
3. „Datenschutz“ für unternehmensbezogene Daten.....	81
4. Telekommunikation bei B2B	82
5. Telekommunikationsrechtliche Verantwortlichkeit.....	83
a. Konzernverbund	83
b. Geschlossene Netzwerke	83
c. Virtuelle Netzwerke	85
6. Möglichkeiten der Einflussnahme von B2B-Handelspartnern	85
7. Zwischenergebnis	86
III. Ergebnis	86
Teil 4: Gewerblicher Rechtsschutz für Unternehmensdaten.....	88
I. Erfindungsschutz für Daten im B2B	88
1. Erfindungsbegriff	88
2. Erfindungscharakter geschäftlicher Methoden	89
3. Computerimplementierte Geschäftsmethoden	92
4. Zwischenergebnis	95
II. Schutz von Daten als Datenbankwerke.....	95
1. Sammlung unabhängiger Einzelelemente	95
2. Systematisch-methodische Anordnung der Daten	96
3. Schöpfungscharakter	96
a. Auswahl der Daten	97
b. Anordnung der Daten.....	99
4. Zwischenergebnis	100

III. Schutz von Daten in einfachen Datenbanken	100
1. Wesentliche Investition in eine Datenbank im B2B	100
2. Reichweite des Datenbankschutzes	103
a. Wesentliche Teile	103
b. Unwesentliche Teile	104
c. Einzelne Datensätze	105
3. Zwischenergebnis	105
IV. Ergebnis	106
Teil 5: Wettbewerbsrechtlicher Schutz für Unternehmensdaten	107
I. Schutz der Daten aus dem Verbot unlauteren Wettbewerbs	107
1. Geschäftliche Handlungen im B2B	108
a. Unternehmensbezogenheit der Handlung	108
b. Marktbezogenheit der Handlung	109
c. Ausrichtung auf Absatz und Bezug von Waren und Dienstleistungen	109
d. Förderung des Wettbewerbs	110
e. Beeinflussung von Marktverhältnissen	111
2. Wettbewerbsbeeinträchtigung	111
a. Objektive Eignung	112
b. Nachteiligkeit	112
3. Spürbarkeit	113
4. Rechtsbruch	114
5. Nachahmung	114
a. Angebot von Waren und Dienstleistungen	115
b. Wettbewerbliche Eigenart	116
c. Nachahmungscharakter	118
d. Unredliche Erlangung von Kenntnissen und Daten	120
aa. Erschleichen von Kenntnissen	120

bb. Nutzen von Daten unter Vertrauensbruch	121
6. Allgemeine Unlauterkeit	122
a. Missbilligenswerte Wettbewerbshandlung	123
b. Verletzung anständiger Gepflogenheiten in Wettbewerb und Handel	124
7. Verhältnis zum leistungsrechtlichen Datenbankschutz.....	125
8. Zwischenergebnis.....	125
II. Schutz der Daten als Unternehmensgeheimnisse	126
1. Unternehmensbezug.....	128
a. Wirtschaftliche Aspekte	128
b. Technische Aspekte	129
c. Zuordnung	130
2. Vermögenswert.....	131
3. Geheimnischarakter.....	132
a. Fehlende Offenkundigkeit.....	132
b. Geheimhaltungsinteresse	134
c. Geheimhaltungsabsicht	134
d. Grenzen des Geheimnisschutzes.....	135
4. Ausspähen geheimer Daten	136
5. Zwischenergebnis	136
III. Ergebnis	137
Teil 6: Schutz durch regulierte IT-Sicherheit.....	138
I. Technisch-organisatorischer Datenschutz.....	139
1. Authentifizierung der Teilnehmer des B2B-Handels.....	140
2. Autorisierung der Handlungsbefugnisse im B2B	141
3. Absicherung der Transaktion von Daten.....	142
4. Dokumentation der Handelsvorgänge.....	144
5. Gewährleistung der Verfügbarkeit der Daten	145

6. Zwischenergebnis	146
II. Organisatorische Richtlinien und Standards	146
1. Zertifizierung	147
2. IT-Sicherheitsleitlinien	149
3. Verhaltenskodizes	151
4. Zwischenergebnis	152
III. Technische Sicherheitsmaßnahmen	152
1. Schutzfähigkeit der Daten	153
2. Zustand der Daten	154
3. Zugänglichkeit der Daten	155
5. Zwischenergebnis	157
IV. Ergebnis	157
Zusammenfassende Bewertung in Thesen	159
Anhang 1: Sicherheitsarchitektur im B2B	162
I. SSL	162
II. XML	162
III. ebXML	164
Anhang 2: B2B-Handelsszenario mit ebXML	167
I. Vorbereitung der Unternehmen	167
II. Begründung der Geschäftsbeziehung	167
III. Ablauf des Geschäftsvorgangs	168