

INHALTSÜBERSICHT

INHALT	VII
TEIL A DIE DATENERFASSUNG DURCH WEB 2.0-FUNKTIONEN IN DER INNERBETRIEBLICHEN TELEKOMMUNIKATION	1
A Das Web 2.0 und der Datenschutz.....	3
B Das Buzzword „Web 2.0“.....	9
C Die betriebsinterne Kommunikation	28
D Die Verwendung von Web 2.0-Funktionen im Intranet - Eine Herausforderung für den Datenschutz	42
TEIL B DIE LEGITIMATION DER DATENERFASSUNG AUFGRUND GESETZLICHER ERLAUBNISTATBESTÄNDE	55
A Zur Anwendung des BDSG	55
B Die gesetzlichen Erlaubnistatbestände für Datenumgänge durch nicht-öffentliche Stellen	70
C Die Eingabe von Daten in das Intranet.....	90
D Die Legitimation der Dateneingabe	104
E Der betriebsinterne Datenfluss	145
F Die Datenübermittlung an Dritte.....	166
G Die Überwachung der Intranetnutzung	202
H Die weiteren Verwendungsmöglichkeiten der Intranetdaten.....	243
TEIL C DIE LEGITIMATION AUFGRUND VON EINWILLIGUNG UND BETRIEBSVEREINBARUNG.....	259
A Die Einwilligung des Beschäftigten	259
B Die Einwilligung in die Zurschaustellung von Bildnissen im Intranet...	306
C Die Mitbestimmung des Betriebsrats	326
TEIL D DIE RISIKOBEHAFTETE SITUATION DES ARBEITGEBERS	347
A Die Haftungsrisiken des Arbeitgebers.....	347
B Die Schwierigkeit der Schaffung eines rechtssicheren Datenschutzkonzepts.....	362
TEIL E DIE ERLAUBTE PRIVATNUTZUNG DES INTRANETS.....	371
A Der Anwendungsvorrang von TKG und TMG	371

B Die Anwendung von TKG und TMG	409
C Die Verschärfung der schwierigen Lage des Arbeitgebers	466
TEIL F EINE BETRACHTUNG DER RECHTSLAGE - DE LEGE LATA ET DE LEGE FERENDA	485
A Die Situation des Arbeitgebers nach der aktuellen Rechtslage	485
B Die Reformvorschläge der letzten Jahre.....	491
C Gedanken zur Modernisierung des Beschäftigtendatenschutzes.....	549
D Die Reformbedürftigkeit des Beschäftigtendatenschutzes.....	576
LITERATUR	581
RECHTSPRECHUNG.....	609

INHALT

INHALTSÜBERSICHT	IV
TEIL A DIE DATENERFASSUNG DURCH WEB 2.0-FUNKTIONEN IN DER INNERBETRIEBLICHEN TELEKOMMUNIKATION	1
A Das Web 2.0 und der Datenschutz	3
I. Die Speicherung von Beschäftigtendaten im Zugriffsbereich des Arbeitgebers	4
II. Der grundrechtliche Schutz durch das Recht auf informationelle Selbstbestimmung	4
B Das Buzzword „Web 2.0“	9
I. Zum Fehlen einer Definition	9
II. Die Schlüsselprinzipien des Web 2.0	10
1. Das Web als Plattform	10
2. Die Nutzung der kollektiven Intelligenz.....	11
3. Die Daten als zentrale Komponente des Geschäftserfolgs	13
4. Eine Software ohne Lebenszyklus	14
5. Die Vielfalt durch leichtgewichtige Programmkomponenten	14
6. Die leistungsstarken Benutzeroberflächen im Webbrowser dank „Ajax“	15
7. Die fehlende Bindung an ein konkretes Gerät	18
III. Die einzelnen Web 2.0-Funktionen.....	19
1. Der Blog als „klassische“ Web 2.0-Funktion	19
2. Das Mikroblogging.....	20
3. Das Wiki	22
4. Die sozialen Netzwerke	22
5. Feeds - Die Nachrichtenkanäle des Web 2.0	24
6. Das Mashup als Mittel der individuellen Anpassung	25
7. Die Suchfunktionen des Web 2.0	26
C Die betriebsinterne Kommunikation	28
I. Zur unterschiedlichen Nutzung von Web 2.0 im betrieblichen Umfeld	28
II. Das betriebsinterne Unternehmensnetzwerk.....	29
III. Zur Datensicherheit und den weiteren Vorteilen der Nutzung eines betriebsinternen Netzwerks.....	30
IV. Die Verwendung von Web 2.0-Funktionen im Intranet.....	34
1. Die Strategie der Unternehmen	35
2. Der Datenschutz als Teil der Unternehmensstrategie	40

D Die Verwendung von Web 2.0-Funktionen im Intranet - Eine Herausforderung für den Datenschutz	42
I. Die Personenbezogenheit von Daten im Web 2.0.....	42
II. Zur Möglichkeit der Anonymisierung und Pseudonymisierung	47
III. Zum Datenschutz durch Technik	52
TEIL B DIE LEGITIMATION DER DATENERFASSUNG AUFGRUND GESETZLICHER ERLAUBNISTATBESTÄNDE	55
A Zur Anwendung des BDSG	55
I. Die Anwendung des BDSG bei verbotener Privatnutzung des Intranets.....	55
II. Zur räumlichen Anwendung des deutschen Datenschutzrechts	57
III. Das Verbot mit Erlaubnisvorbehalt.....	68
B Die gesetzlichen Erlaubnistatbestände für Datenumgänge durch nicht-öffentliche Stellen	70
I. Die Anwendbarkeit der §§ 27 bis 32 BDSG	70
II. § 32 BDSG als spezielle Regelung zum Beschäftigtendatenschutz	73
1. Die Legaldefinition des „Beschäftigten“	74
2. Der Zweck der Datenerhebung und -verwendung als maßgebliches Kriterium	75
a) Die Datenumgangszwecke des § 32 Abs. 1 S. 1 BDSG	76
b) Die konkrete Zweckfestlegung	79
c) Die nachträgliche Zweckänderung.....	81
3. Die Erforderlichkeit zur Zweckerreichung.....	82
III. Der Rückgriff auf § 28 BDSG.....	85
1. Die Erhebung und Verwendung von Arbeitnehmerdaten zu beschäftigungsfremden Zwecken.....	85
2. Der Datenumgang zu Zwecken des Beschäftigungsverhältnisses.....	87
C Die Eingabe von Daten in das Intranet	90
I. Die Dateneingabe als Erhebung i.S.v. § 3 Abs. 3 BDSG	91
1. Die Dateneingabe durch den Betroffenen	91
2. Die Dateneingabe durch den Arbeitgeber	94
3. Die Dateneingabe durch die Kollegen	95
4. Die automatische Datenerfassung	98
5. Die Informationspflichten bei der Erhebung	98
II. Die Dateneingabe als Speicherung und Nutzung	100
D Die Legitimation der Dateneingabe	104
I. Die Zulässigkeit der Dateneingabe zum Zweck der Erbringung der Arbeitsleistung	105

1. Der Verzicht auf Web 2.0-Funktionen als milderes Mittel	105
2. Die Vergleichbarkeit mit der Internetveröffentlichung.....	108
3. Die Dateneingabe und die Legitimation der damit verbundenen Datenumgänge.....	110
a) Die Angabe von beruflichen Kontaktdaten	110
a) Die Expertenfindung - Zur Angabe beruflicher Qualifikationen.....	111
b) Zur Erfassung von Informationen aus der Privatsphäre des Beschäftigten	113
c) Zur Offenbarung personenbezogener Daten durch Bildnisse	116
d) Die Kontaktliste	117
e) Die Erfassung des Aufenthaltsortes	118
f) Die Angabe von Arbeitszeiten	122
g) Zu Personalakteninhalten, Prüfungsergebnissen, Rennlisten und Newsblogs - Die Verbreitung ausgewählter Inhalte im Intranet.....	124
h) Feeds, Mashups, Suchfunktionen und die Erforderlichkeit eines Datenumgangs	128
4. Der Datenumgang mit besonderen Arten von personenbezogenen Daten i.S.v. § 3 Abs. 9 BDSG	132
II. Die Verbindungsdaten und die Zugangskontrolle	136
1. Die Personenbezogenheit der Netzwerkadresse und die Legitimation des Umgangs mit Verbindungsdaten	136
2. Zur Erfassung biometrischer Daten	141
3. Der Einsatz von Social Plug-ins	143
E Der betriebsinterne Datenfluss	145
I. Die Kenntnisnahme als Datennutzung	145
II. Die Einsichtnahme des Arbeitgebers in Web 2.0-Inhalte	146
1. Die Einsichtnahme in dienstliche Mitarbeiter-E-Mails durch den Arbeitgeber	147
2. Die Vergleichbarkeit der Rechtslage im Hinblick auf Web 2.0-Beiträge.....	151
3. Die Grenzen der Kenntnisnahme durch den Arbeitgeber.....	153
III. Die Kenntnisnahme der Betriebsratsmitglieder	157
IV. Die Auftragsdatenverarbeitung durch einen externen Dienstleister...	159
F Die Datenübermittlung an Dritte.....	166
I. Die Weitergabe der erfassten Daten an Dritte	166
II. Die Teilnahme Dritter am betriebsinternen Netzwerk.....	170
1. Der Einbezug einzelner Dritter in die betriebsinterne Telekommunikation	171
2. Der Zugriff durch ein anderes Konzernunternehmen	172
3. Die Auslandsübermittlung	181

a)	Die Datenübermittlung innerhalb der EU bzw. des EWR	182
b)	Die Datenübermittlung in ein Drittland	183
aa)	Die Zulässigkeit bei einem angemessenen Datenschutzniveau.....	185
bb)	Die Zulässigkeit beim Fehlen eines angemessenen Datenschutzniveaus.....	190
cc)	Die behördliche Genehmigung von Drittlandsübermittlungen	194
III.	Die Übermittlung an einen in einem Drittland ansässigen externen Dienstleister	199
IV.	Die Einrichtung eines automatisierten Abrufverfahrens.....	200
G	Die Überwachung der Intranetnutzung.....	202
I.	Compliance - Zu den Überwachungspflichten des Arbeitgebers	204
II.	Die Zulässigkeit von Überwachungsmaßnahmen	211
1.	Die Überwachung zur Aufdeckung von Straftaten.....	212
2.	Die präventive Überwachung und die Kontrolle nichtstrafbarer Regelverstöße.....	216
3.	Die Voraussetzungen von Überwachungsmaßnahmen nach § 32 Abs. 1 S. 1 BDSG.....	221
4.	Die Verwendung von Intranetdaten zu ausgewählten Überwachungszwecken	224
a)	Die Kontrolle des Verbots der Privatnutzung	225
b)	Die Leistungskontrolle	229
c)	Die Kontrolle durch Bewegungsprofile	230
5.	Die Verwendung der Intranetdaten zu Datenabgleichen.....	232
III.	Zur Gegenläufigkeit von Datenschutz und Überwachungsverpflichtungen	241
H	Die weiteren Verwendungsmöglichkeiten der Intranetdaten	243
I.	Der Einbezug der Intranetdaten in die Personalplanung	243
II.	Die Datensicherung	248
III.	Die Löschung von Daten	248
1.	Die Datenlöschung auf Wunsch des Arbeitgebers	250
2.	Die Löschpflichten des Arbeitgebers	254
TEIL C	DIE LEGITIMATION AUFGRUND VON EINWILLIGUNG UND BETRIEBSVEREINBARUNG.....	259
A	Die Einwilligung des Beschäftigten	259
I.	Die Freiwilligkeit der Einwilligung als Ausdruck einer selbstbestimmten Entscheidung.....	260
1.	Die strukturelle Überlegenheit des Arbeitgebers.....	262
2.	Zur fehlenden Freiwilligkeit im Übrigen	266
3.	Die Grenzen der Einwilligung	269

II.	Die Einwilligungserklärung.....	271
1.	Der Zeitpunkt der Erklärungsabgabe	271
2.	Zum Schriftformerfordernis und der Möglichkeit davon abzuweichen.....	274
3.	Zur konkludenten Einwilligung durch die Eingabe von personenbezogenen Daten in Web 2.0-Funktionen	280
4.	Die informierte Einwilligung	284
5.	Zur Formulierung der Einwilligungserklärung	288
a)	Der Bestimmtheitsgrundsatz	288
b)	Die Verknüpfung der Einwilligung mit weiteren Erklärungen	290
c)	Die Einwilligung mittels Allgemeiner Geschäftsbedingungen	291
III.	Die Einholung einer Einwilligung trotz Vorliegen eines gesetzlichen Erlaubnistatbestandes	295
IV.	Die Einwilligungserklärung durch einen Vertreter	297
V.	Die datenschutzrechtliche Einwilligung durch minderjährige Beschäftigte und Erwachsene mit fehlender Einsichtsfähigkeit	299
VI.	Der Widerruf der Einwilligung.....	301
B	Die Einwilligung in die Zurschaustellung von Bildnissen im Intranet...	306
I.	Die Bildnisse von Mitarbeitern im Intranet	307
II.	Die öffentliche Zurschaustellung im Intranet	310
III.	Die Ausnahmen des § 23 KUG	313
IV.	Die Einwilligung in die Zurschaustellung des Mitarbeiterfotos	315
1.	Die einheitlichen Voraussetzungen einer Einwilligung nach dem KUG und dem BDSG	315
2.	Zu den abweichenden Voraussetzungen einer Einwilligung nach dem KUG und dem BDSG	317
3.	Zum Anwendungsvorrang des KUG	321
V.	Die Konsequenzen eines Verstoßes gegen das KUG.....	325
C	Die Mitbestimmung des Betriebsrats	326
I.	Die Mitbestimmungsrechte des Betriebsrats.....	327
1.	Das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG	327
2.	Zu den Mitbestimmungsrechten des Betriebsrats im Übrigen	335
3.	Die Ausübung des Mitbestimmungsrechts	337
II.	Die Legitimation von Datenumgängen mittels Betriebsvereinbarung .	339
III.	Zur Legitimation durch Tarifverträge und Regelungsabreden	344
TEIL D	DIE RISIKOBEHAFTETE SITUATION DES ARBEITGEBERS	347
A	Die Haftungsrisiken des Arbeitgebers.....	347
I.	Zu den Folgen eines Datenschutzverstoßes.....	347

II. Das Durchsetzungsdefizit und die Rechte der Betroffenen	355
B Die Schwierigkeit der Schaffung eines rechtssicheren Datenschutzkonzepts	362
I. Zur Unzulänglichkeit der gesetzlichen Legitimationstatbestände	363
II. Die Einwilligung als Alternative	364
III. Zur Sinnhaftigkeit einer Betriebsvereinbarung	367
TEIL E DIE ERLAUBTE PRIVATNUTZUNG DES INTRANETS	371
A Der Anwendungsvorrang von TKG und TMG	371
I. Der Arbeitgeber im Anwendungsbereich des TKG	371
II. Die Anwendbarkeit des TMG	380
III. Die Erlaubnis der Privatnutzung	381
1. Die alleinige Entscheidungsbefugnis des Arbeitgebers	382
2. Die Erlaubniserteilung	384
3. Zur Entstehung einer betrieblichen Übung	389
4. Die Einbindung des Betriebsrats	394
IV. Die dienstliche und private Nutzung der betrieblichen Telekommunikationsmittel	396
V. Der Umfang und die Grenzen der erlaubten Privatnutzung	399
VI. Die Rücknahme der Erlaubnis	405
B Die Anwendung von TKG und TMG	409
I. Zum Anwendungsbereich des TMG	409
1. Die Web 2.0-Funktionen als Telemedienangebot	410
2. Die gleichzeitige Zugangsvermittlung zum Intranet	413
3. Zur Anwendung von §§ 15 Abs. 8, 16 Abs. 2 Nr. 4 TMG	416
II. Die Anwendung der Vorschriften des TKG	419
1. Der räumliche Anwendungsbereich des TKG	420
2. Der Schutzbereich des Fernmeldegeheimnisses	420
a) Dem Arbeitgeber frei zugängliche Telekommunikationsinhalte	422
b) Die Zugriffbeschränkung gegenüber dem Arbeitgeber	424
aa) Die Reichweite des Schutzes durch das Fernmeldegeheimnis	424
bb) Zu den Ausnahmen vom Schutzbereich des Fernmeldegeheimnisses	431
3. Die Einhaltung der telekommunikationsrechtlichen Datenschutzbestimmungen	436
4. Die Einwilligung der Beschäftigten in die Kenntnisnahme	439
a) Zum Erfordernis der Einwilligung aller Beschäftigter	440
b) Die Voraussetzungen der Einwilligung in die Kenntnisnahme	444

5. Zur Unzulänglichkeit der Betriebsvereinbarung als Legitimationsgrundlage.....	448
6. Die Sanktionierung von Verstößen gegen die Vorschriften des TKG	449
a) Zur Strafbarkeit nach § 206 StGB	450
b) Zur Strafbarkeit nach § 303a StGB	456
c) Zur Erfüllung weiterer Straftatbestände	459
III. Zum Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	463
C Die Verschärfung der schwierigen Lage des Arbeitgebers.....	466
I. Die Abwägung der Erlaubniserteilung.....	466
II. Die Umsetzung der Entscheidung.....	472
III. Zum Inhalt der Nutzungsregelung	477
TEIL F EINE BETRACHTUNG DER RECHTSLAGE - DE LEGE LATA ET DE LEGE FERENDA	485
A Die Situation des Arbeitgebers nach der aktuellen Rechtslage.....	485
B Die Reformvorschläge der letzten Jahre	491
I. Der Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes.....	491
1. Die gesetzlichen Erlaubnistatbestände nach dem BDSG-E	493
a) Zu den gesetzlichen Erlaubnistatbeständen im Allgemeinen	493
b) Die Legitimation von Datenumgängen im andauernden Kommunikationsvorgang	495
c) Die Legitimation von Datenumgängen nach Abschluss des Kommunikationsvorgangs	499
d) Zur Unzulänglichkeit der gesetzlichen Erlaubnistatbestände des BDSG-E	506
2. Die Einwilligung nach § 32l BDSG-E	508
3. Die Rolle der Betriebsvereinbarung nach dem BDSG-E	514
4. Der Erkenntnisgewinn durch den BDSG-E	516
II. Die Datenschutzgrundverordnung	519
1. Die unmittelbare Geltung der Verordnung	520
2. Die Öffnungsklausel des Art. 88 DS-GVO	524
3. Zu den inhaltliche Änderungen der DS-GVO	527
a) Der Anwendungsbereich der DS-GVO	527
b) Die gesetzlichen Erlaubnistatbestände nach der DS-GVO	530
c) Die Einwilligung nach der DS-GVO	531
d) Die Rechte des Betroffenen nach der DS-GVO	535
e) Zur Durchsetzung des Datenschutzrechts nach der DS-GVO.....	541

f) Die Verschärfung der Sanktionen	547
4. Ein Schritt in die richtige Richtung	548
C Gedanken zur Modernisierung des Beschäftigtendatenschutzes.....	549
I. Die Klarstellung datenschutzrechtlicher Streitpunkte	550
1. Die Unsicherheiten der Interessensabwägung	550
2. Der Arbeitgeber im Anwendungsbereich von TKG und TMG	554
3. Zur Schaffung eines Konzernprivilegs	557
4. Zum Spannungsverhältnis zwischen Compliance und Datenschutz ..	561
II. Zur Behebung des Durchsetzungsdefizits	562
III. Die Stärkung der Selbstbestimmung als Ziel.....	566
D Die Reformbedürftigkeit des Beschäftigtendatenschutzes.....	576
 LITERATUR	 581
 RECHTSPRECHUNG.....	 609