

# INHALTSÜBERSICHT

<b>ABKÜRZUNGEN .....</b>	<b>XV</b>
<b>A KONFLIKTE AM ARBEITSPLATZ BEI DEM UMGANG MIT PRIVATEN ENDGERÄTEN UND BETRIEBLICHEN KOMMUNIKATIONSMITTELN .....</b>	<b>1</b>
<b>B RECHTSFRAGEN DER NUTZUNG PRIVATER ELEKTRONISCHER GERÄTE FÜR BETRIEBLICHE ZWECKE .....</b>	<b>7</b>
<b>C PRIVATER GEBRAUCH BETRIEBLICHER KOMMUNIKATIONSMITTEL UNTER BESONDERER BERÜCKSICHTIGUNG DER ANFORDERUNGEN AN EINE RECHTSKONFORME NUTZUNG VON TWITTER IM UNTERNEHMEN ..</b>	<b>121</b>
<b>D PROFESSIONELLER UMGANG DER UNTERNEHMEN MIT KALKULIER- BAREN RISIKEN .....</b>	<b>187</b>
<b>LITERATUR.....</b>	<b>191</b>

# INHALT

ABKÜRZUNGEN .....	XV
<b>A KONFLIKTE AM ARBEITSPLATZ BEI DEM UMGANG MIT PRIVATEN ENDGERÄTEN UND BETRIEBLICHEN KOMMUNIKATIONSMITTELN .....</b>	<b>1</b>
<b>B RECHTSFRAGEN DER NUTZUNG PRIVATER ELEKTRONISCHER GERÄTE FÜR BETRIEBLICHE ZWECKE .....</b>	<b>7</b>
<b>I. Der Trend zur Verwendung eines einzigen Endgerätes für alle privaten und dienstlichen Anforderungen .....</b>	<b>7</b>
<b>II. Bring your own device als Chance für Unternehmen .....</b>	<b>9</b>
1. Einsparung von Investitionen.....	9
2. Steigerung der Produktivität .....	10
3. Modernisierung der Unternehmens-IT .....	11
<b>III. Rechtskonformität bei der Implementierung eines Bring your own device-Programms zur Vermeidung von Bedrohungslagen .....</b>	<b>11</b>
1. Strafrecht und Strafbarkeitsrisiken für Arbeitgeber und Arbeitnehmer .....	15
a) Strafbarkeit nach §§ 17, 18 UWG .....	15
b) Strafbarkeit nach § 206 StGB .....	19
c) Strafbarkeit nach § 202a StGB .....	21
d) Strafbarkeit nach § 202b StGB .....	22
e) Strafbarkeit nach § 202c StGB .....	23
f) Strafbarkeit nach § 203 StGB .....	23
g) Strafbarkeit nach § 303a StGB .....	24
2. Urheberrechtsverletzungen von Arbeitnehmern und Haftungsfolgen für das Unternehmen .....	24
a) Gefahren für Unternehmen durch die Verwendung nicht ausreichend lizenzierter Software durch Arbeitnehmer .....	25
b) Haftung des Unternehmens für Urheberrechtsverletzungen .....	26
aa) Ansprüche des Verletzten unter anderem auf Schadensersatz, Unterlassung, Vernichtung, Rückruf und Überlassung .....	26
bb) Weitere Rechtsfolgen von Urheberrechtsverletzungen .....	30
c) Haftungsrisiken der Unternehmensleiter (IT-Compliance) .....	30
d) Wege aus der Haftungsfalle .....	34
3. Datenschutzrechtliche Aspekte .....	35
a) Arbeitnehmer als Auftragsdatenverarbeiter .....	36
b) Kontrollrechte und -pflichten des Arbeitgebers aus § 9 BDSG .....	39
c) Schutz von Daten der Arbeitnehmer .....	42

<b>4. Eigentumsrechtliche Lage und Umfang der Nutzungsrechte an den Kommunikationsmitteln .....</b>	<b>46</b>
a) Eigentumsrechtliche Lage .....	47
b) Vertragsrechtliche Einordnung der Nutzungsverhältnisse .....	47
c) Entstehung einer für Arbeitgeber verpflichtenden betrieblichen Übung .....	49
d) Entstehung einer für Arbeitnehmer verpflichtenden betrieblichen Übung .....	51
<b>5. Anforderungen aus dem Arbeitszeitgesetz .....</b>	<b>52</b>
<b>6. Einhaltung von gesetzlichen Aufbewahrungsfristen .....</b>	<b>57</b>
<b>7. Private Mobilfunkverträge und Bring your own device .....</b>	<b>58</b>
<b>8. Schutzmaßnahmen für den Einsatz mobiler Endgeräte im Unternehmen .....</b>	<b>59</b>
a) Mobile Device Management (MDM) .....	59
b) Sandboxing .....	59
c) Informationsschutz .....	61
aa) Data Loss oder Leakage Prevention (DLP) .....	62
(1) Technische Möglichkeiten von DLP-Systemen .....	62
(2) Rechtliche Bedenken gegen DLP-Systeme .....	63
bb) Web- und Netzsicherheit via Monitoring .....	64
cc) Datenverschlüsselung .....	64
d) Weitere Möglichkeiten zum Schutz vor Angriffen .....	64
<b>9. Pflichten des Arbeitnehmers zur Herausgabe seines im Rahmen eines Bring your own device-Programms verwendeten Endgeräts .....</b>	<b>65</b>
<b>10. Verpflichtung zu Instandhaltung und Updating von zu dienstlichen Zwecken eingesetzten privaten Endgeräten .....</b>	<b>67</b>
<b>11. Ersatzpflichten und Handlungsmöglichkeiten von Arbeitgeber und Arbeitnehmer bei Verlust beziehungsweise Beschädigung privater mobiler Endgeräte oder betrieblicher Daten .....</b>	<b>68</b>
a) Verlust bzw. Beschädigung der Endgeräte .....	68
aa) Ersatzpflicht des Arbeitgebers .....	68
bb) Verpflichtung des Arbeitnehmers zur Ersatzbeschaffung .....	73
b) Löschung betrieblicher Daten durch Arbeitnehmer .....	75
<b>12. Kostenerstattung für die betriebliche Nutzung privater Endgeräte und steuerrechtliche Auswirkungen .....</b>	<b>76</b>
a) Vereinbarung über die Kostenerstattung und Nutzungsentgelt zwischen Arbeitgeber und Arbeitnehmer .....	76
b) Aufwendungsersatzanspruch des Arbeitnehmers .....	79
<b>13. Vertrauliche Behandlung von Unternehmensinterna und -geheimnissen .....</b>	<b>80</b>
a) Definition von Betriebs- und Geschäftsgeheimnissen .....	80

b) Trennung zwischen privaten und dienstlichen Daten auf den mobilen Geräten der Arbeitnehmer .....	81
c) Risiken bei der Nutzung von Cloud Services .....	82
d) Empfehlungen zum Schutz von Betriebs- und Geschäftsgeheimnissen.....	84
14. Betriebliche Mitbestimmung bei der Installation eines Bring your own device-Programms .....	85
a) Informationsrechte des Betriebsrats bei Bring your own device .....	86
b) Mitbestimmungsrechte des Betriebsrats bei Bring your own device .....	86
aa) Einführung und Anwendung von technischen Einrichtungen (§ 87 Abs. 1 Nr. 6 BetrVG) .....	86
bb) Ordnung und Verhalten im Betrieb (§ 87 Abs. 1 Nr. 1 BetrVG) .....	88
cc) Beginn und Ende der Arbeitszeit (§ 87 Abs. 1 Nr. 2 BetrVG) und Vorübergehende Änderung der betriebsüblichen Arbeitszeit (§ 87 Abs. 1 Nr. 3 BetrVG) .....	90
dd) Arbeits- und Gesundheitsschutz (§ 87 Abs. 1 Nr. 7 BetrVG).....	90
ee) Mitbestimmung bei Maßnahmen der Berufsbildung (§ 97 Abs. 2 BetrVG) .....	92
ff) Durchführung betrieblicher Bildungsmaßnahmen (§ 98 BetrVG) .....	93
c) Kontrollrechte des Betriebsrats bei Bring your own device .....	93
d) Folgen der Nichtbeteiligung des Betriebsrats .....	94
15. Risikobeherrschung .....	96
a) Mitarbeiter-PC-Programm .....	96
aa) Steuerliche Vorteile .....	97
bb) Einrichtung eines MPP .....	98
cc) Individuelle Vereinbarung zwischen Arbeitgeber und Arbeitnehmer .....	98
b) Choose your own device .....	98
c) Vereinbarung zu Bring your own device .....	99
aa) Ausgestaltung als Unternehmensrichtlinie .....	99
bb) Abschluss einer Betriebsvereinbarung .....	100
(1) Unmittelbare und zwingende Wirkung .....	101
(2) Keine Anwendbarkeit des AGB-Rechts.....	102
(3) Datenschutzrechtliche Vorteile.....	102
(4) Zuständige Arbeitnehmervertretung .....	103
cc) Individualvertragliche Umsetzung .....	104
16. Nutzungsvereinbarung zu Bring your own device .....	104
a) Mögliche Inhalte einer Nutzungsvereinbarung .....	104
aa) Freiwillige Leistung .....	105
bb) Umfang und Dauer der Nutzung privater Endgeräte zu dienstlichen Zwecken .....	105

cc) Ausgewählte Regelungen zu sicherheitsrelevanten Themen .....	106
(1) Einsatz von Sicherheits-Software .....	106
(2) Zentrale Geräte-Konfiguration .....	106
dd) Informationspflicht .....	108
ee) Umgang mit Daten und Software .....	109
(1) Trennung zwischen privaten und geschäftlichen Daten .....	109
(2) Datenspeicherung.....	109
(3) Datenlöschung vom privaten Endgerät des Arbeitnehmers .....	109
(4) Ändern von Daten des Arbeitnehmers.....	110
(5) Nutzung von Cloud-Diensten .....	111
(6) Installation von Apps .....	111
ff) Kostentragung.....	111
gg) Haftung.....	112
b) Muster einer Nutzungsvereinbarung .....	112
17. Bewertung von Bring your own device .....	120
 <b>C PRIVATER GEBRAUCH BETRIEBLICHER KOMMUNIKATIONSMITTEL UNTER BESONDERER BERÜCKSICHTIGUNG DER ANFORDERUNGEN AN EINE RECHTSKONFORME NUTZUNG VON TWITTER IM UNTERNEHMEN..</b>	<b>121</b>
 <b>I. Nutzung und Kontrolle der betrieblichen E-Mail- und Internet- systeme: Compliance zur Vermeidung von Betrug und Korruption ....</b>	<b>121</b>
1. Der Interessenkonflikt zwischen Arbeitgeber und Arbeitnehmer hinsichtlich der Nutzung und Kontrolle der betrieblichen E-Mail- und Internetsysteme .....	121
a) Interessenlage des Arbeitgebers.....	121
b) Interessenlage der Arbeitnehmer .....	122
2. Kontrollpflichten für Unternehmen aufgrund von Compliance- anforderungen.....	122
a) Entwicklung und Bedeutung des Begriffs Compliance .....	122
b) Compliance als Verpflichtung des Managements .....	124
3. Kontrolle der betrieblichen E-Mail- und Internetsysteme durch Arbeitgeber bei gestatteter Privatnutzung .....	126
a) Telekommunikationsrecht als Grenze von Kontrollmaßnahmen ...	126
b) Kontrollmöglichkeiten der Arbeitgeber .....	130
aa) Fernmeldegeheimnis nach § 88 TKG .....	130
bb) Kontrolle von Verkehrsdaten .....	131
(1) Voraussetzungen von § 96 TKG .....	132
(2) Voraussetzungen von § 100 TKG .....	132
(3) Voraussetzungen von §§ 109 ff. TKG.....	132
cc) Kontrolle von Inhaltsdaten.....	132
dd) Spamfilter und Virenbekämpfung .....	133

ee) Dauer des Schutzes des Fernmeldegeheimnisses .....	134
ff) Umfang der Kontrollrechte des Arbeitgebers bei gestatteter Privatnutzung betrieblicher E-Mail- und Internetsysteme/ Beweisverwertung .....	136
4. Kontrolle der betrieblichen E-Mail- und Internetsysteme durch Arbeitgeber bei untersagter Privatnutzung .....	138
a) Datenschutzrecht als Grenze von Kontrollmaßnahmen .....	138
b) Kontrollmöglichkeiten der Arbeitgeber .....	140
aa) Keine Totalüberwachung .....	140
bb) Kontrolle von Verkehrsdaten .....	143
cc) Kontrolle von Inhaltsdaten .....	145
dd) Spamfilter und Virenbekämpfung .....	146
ee) Umfang der Kontrollrechte des Arbeitgebers bei untersagter Privatnutzung betrieblicher E-Mail- und Internetsysteme/ Beweisverwertung .....	147
5. Zwischenfazit .....	147
<b>II. Verwendung von Twitter im unternehmerischen Kontext .....</b>	<b>147</b>
1. Chancen und Risiken für Unternehmen .....	147
a) Einsatzmöglichkeiten von Twitter .....	148
b) Funktionsweise von Twitter .....	149
2. Anforderungen an die Rechtskonformität bei der Einrichtung des Twitter-Accounts .....	150
a) Nutzernamen .....	150
aa) Vorgaben bei der Anmeldung .....	150
bb) Rechtliche Maßnahmen gegen Identitätsbetrug .....	151
b) Profil- und Kopfzeilenfoto .....	152
c) Impressumspflicht .....	152
aa) Darstellung der Rechtslage .....	152
bb) Rechtliche Würdigung .....	153
3. Haftung für den Inhalt von Tweets .....	156
a) (Re-) Tweets und Urheberrecht .....	156
b) Hyperlinks und Haftung für fremde Inhalte .....	158
c) Meinungsäußerung und Schmähkritik .....	158
d) Werbebotschaften und Wettbewerbsrecht .....	159
4. Arbeitsrechtliche Implikationen bei der Nutzung von Twitter am Arbeitsplatz .....	160
a) Problemaufriss .....	160
b) Pflichtverstöße bei der Nutzung von Twitter .....	160
aa) Exzessive Nutzung von Twitter während der Arbeitszeit .....	160
(1) Dienstliche Nutzung .....	160
(2) Private Nutzung .....	161

(3) Arbeitsrechtliche Konsequenzen der exzessiven Nutzung von Twitter während der Arbeitszeit .....	163
(4) Mitbestimmungsrechte des Betriebsrats .....	167
bb) Nutzung von Twitter außerhalb der Arbeitszeit .....	168
cc) Unternehmensschädigende Äußerungen und unternehmensschädigendes Verhalten .....	168
dd) Verletzung der Pflicht zur Verschwiegenheit .....	173
ee) Anzeige von Gesetzesverstößen .....	174
(1) Compliance-Programme und Verpflichtung zu Whistleblowing .....	174
(2) Arbeitsrechtliche Konsequenzen von Whistleblowing .....	176
ff) Identifizierung des Arbeitnehmers als „Täter“ .....	178
c) Recruiting via Twitter .....	178
d) Erwartung weiterer (arbeitsrechtlicher) Rechtsstreitigkeiten .....	180
5. Social Media Policy .....	180
a) Bedeutung des Erlasses einer Social Media Policy .....	180
b) Mögliche Inhalte einer Social Media Policy .....	181
c) Beteiligung des Betriebsrats .....	181
d) Muster einer Social Media Policy - ausgelegt für eine Nutzung von Twitter .....	182
6. Zwischenfazit .....	184
 D PROFESSIONELLER UMGANG DER UNTERNEHMEN MIT KALKULIERBAREN RISIKEN .....	 187
 LITERATUR .....	 191