EINLEITUNG **1**

GANG DER UNTERSUCHUNG **3**

ERSTER TEIL

DATENSCHUTZ IM MULTINATIONALEN KONZERN **5**

A. BESTIMMUNG DER WESENTLICHEN BEGRIFFE **5**

1. Datenschutz 5
2. Personenbezogene Daten 5
3. Unternehmen / Konzern / Unternehmensgruppe 6

3.1 Unternehmen 6

3.1.1. Überblick 6

3.1.2 Herrschendes Unternehmen 7

3.1.3 Abhängiges Unternehmen 7

3.2 Konzern 8

3.3 Konzernbegriff im Datenschutz 9

4. Verantwortliche Stelle 9
5. Datenübermittlung 9
6. Empfänger / Dritter 10
7. Auftragsdatenverarbeitung 10
8. Drittstaaten 11
9. Informationssicherheit 11

B. DER KONZERN ALS DATENSAMMELSTELLE **12**

I. Allgemeines **12**

II. Ausgangssituation im Konzern **13**

III. Zwischenergebnis **15**

IV. Referenzbereiche **16**

1. Personalwesen 16

1.1 Überblick 16

1.2 Entgeltabrechnung 17

1.3 Skill-Datenbank 17

2. Informationstechnik / Informationssysteme 18
2.1 Überblick 18
2.2 Konzernweites Adressbuch 19
2.3 Bereitstellen von Email- und Internetdiensten 19
3. Entwicklungsabteilung 20

C. ZULÄSSIGKEIT DES GRENZÜBERSCHREITENDEN DATENVERKEHRS 22

I. Rechtsgrundlagen 22

1. Entwicklung des Datenschutzrechts 22
1.1 Überblick 22
1.2 OECD 22
1.3 Vereinte Nationen 23
1.4 Europarat 23
1.5 Europäische Union / Europäische Gemeinschaft 25
2. Nationales Recht 27
2.1 Überblick 27
2.2 Hessisches Landesdatenschutzgesetz / Bundesdatenschutzgesetz von 1977 29
2.3 Recht auf informationelle Selbstbestimmung / Volkszählungsentscheidung 29
2.4 Auswirkungen der EG-Datenschutzrichtlinie auf das Bundesdatenschutzgesetz 2001 32
2.5 Bundesdatenschutzgesetz 2009 33
2.6 Referentenentwurf zur Neuregelung des Beschäftigtendatenschutzes 33

II. Grundsätze der Konzerndatenverarbeitung 34
1. Grundsätzliches 34
2. Interessen der Beteiligten 35
2.1. Überblick 35
2.2 Interesse der Konzerne 36
2.3 Interesse der Betroffenen 38
3. Zweckbindung der Daten 39
4. Verfahrensmäßige Konsequenzen 42
4.1 Überblick 42
4.2 Datentransparenz 42
4.3. Betrieblicher Datenschutzbeauftragter 43
4.3.1. Überblick 43
4.3.2 Wahlfreiheit 45
4.3.3 Qualifikation 45
4.3.4 Aufgaben des Datenschutzbeauftragten 46

4.4 Vorabkontrolle ... 48
4.5 Datenschutzleitlinien ... 49
4.6 Technisch-organisatorischer Datenschutz ... 51
4.6.1. Allgemeines ... 51
4.6.2. Technische und organisatorische Maßnahmen ... 52
4.6.2.1 Zutrittskontrolle ... 52
4.6.2.2 Zugangskontrolle ... 52
4.6.2.3 Zugriffskontrolle ... 53
4.6.2.4 Weitergabekontrolle ... 53
4.6.2.5 Eingabekontrolle ... 54
4.6.2.6 Auftragskontrolle ... 54
4.6.2.7 Verfügbarkeitskontrolle ... 54
4.6.2.8 Trennungsgebot (Verwendungszweckkontrolle) ... 55
4.7 Verpflichtung gemäß § 5 BDSG ... 55

III. Voraussetzungen des Datenverkehrs innerhalb Deutschlands ... 56
1. Grundsätzliches ... 56
2. Zulässigkeit der Datenübermittlung ... 57
2.1 Überblick ... 57
2.2 Einwilligung ... 57
2.3 Gesetzliche Erlaubnistatbestände ... 58
2.4 Betriebsvereinbarungen als Rechtsvorschrift ... 58
2.5 Automatisiertes Abrufverfahren ... 60
3. Auftragsdatenverarbeitung ... 61
3.1 Überblick ... 61
3.2. Formalrechtliche Voraussetzungen ... 63
3.4. Pflichten des Auftraggebers ... 65
3.5 Pflichten des Auftragnehmers ... 66
3.6 Zusammenfassung ... 66
4. Abgrenzung Auftragsdatenverarbeitung / Funktionsübertragung ... 66
4.1 Überblick ... 66
4.2 Abgrenzungskriterien ... 67
4.2.1 Auftragsdatenverarbeitung ... 67
4.2.2 Funktionsübertragung ... 68

IV. Voraussetzungen des grenzüberschreitenden Datenverkehrs ... 68
1. Grundsätzliches ... 68
1.1 Überblick / Anwendbarkeit des Bundesdatenschutzgesetzes ... 68
1.2 Innerhalb der EU / des EWR ... 70

1.3 Außerhalb der EU / des EWR ... 70
1.3.1 In Drittstaaten ... 70
1.3.2 Staaten mit angemessenen Datenschutzniveau ... 73
1.3.3 Staaten ohne angemessenes Datenschutzniveau ... 73
2. Datentransfer in die Referenzländer ... 73
2.1 Überblick ... 73
2.2 Österreich ... 74
2.3 Schweiz ... 74

D. ZULÄSSIGKEIT DES DATENVERKEHRS IN DEN REFERENZBEREICHEN ... 75

I. PERSONALWESEN ... 75

1. Entgeltabrechnung ... 75
1.1 Überblick ... 75
1.2 Abgrenzung Auftragsdatenverarbeitung / Funktionsübertragung ... 76
1.3 Datenschutzrechtliche Voraussetzungen innerhalb Deutschlands ... 78
1.3.1 Auftragsdatenverarbeitung ... 78
1.3.2 Funktionsübertragung ... 78
1.3.2.1 Allgemeines ... 78
1.3.2.2 Einwilligung ... 79
1.3.2.3 Durchführung des Arbeitsverhältnisses ... 79
1.3.2.4 Für eigene Geschäftszwecke ... 80
1.4 Datenschutzrechtliche Voraussetzungen für den Datentransfer nach Österreich ... 84
1.5 Datenschutzrechtliche Voraussetzungen für den Datentransfer in die Schweiz ... 85
1.6 Ergebnis ... 85
2. Skill-Datenbank ... 88
2.1 Überblick ... 88
2.2 Datenschutzrechtliche Voraussetzungen innerhalb Deutschlands ... 89
2.2.1 Übermittlung an eine zentrale Stelle ... 89
2.2.1.1 Allgemeines ... 89
2.2.1.2 Einwilligung ... 89
2.2.1.3 Durchführung des Arbeitsverhältnisses ... 90
2.2.1.4 Für eigene Geschäftszwecke ... 91
2.2.1.5 Zusammenfassung ... 93
2.2.2 Einrichtung eines automatisierten Abrufverfahrens ... 93
2.2.2.1 Allgemeines ... 93
2.2.2.2 Zulässigkeit der Einrichtung eines automatisierten Abrufverfahrens ... 94
2.2.2.3 Zulässigkeit der einzelnen Abrufe ... 96

2.2.2.4 Zusammenfassung 97
2.3 Datenschutzrechtliche Voraussetzungen für den Datentransfer nach Österreich 98
2.4 Datenschutzrechtliche Voraussetzungen für den Datentransfer in die Schweiz 98
2.4.1 Allgemeines 98
2.4.2 Übermittlung an eine zentrale Stelle 98
2.4.3 Einrichtung eines automatisierten Abrufverfahrens 99
2.5 Ergebnis 100

II. Informationstechnik / Informationssysteme 103
1. Konzernweites Adressbuch 103
1.1 Überblick 103
1.2 Datenschutzrechtliche Voraussetzungen innerhalb Deutschlands 104
1.2.1 Übermittlung an eine zentrale Stelle 104
1.2.1.1 Allgemeines 104
1.2.1.2 Einwilligung 104
1.2.1.3 Zur Durchführung des Arbeitsverhältnisses 105
1.2.1.4 Für eigene Geschäftszwecke 105
1.2.2 Einrichtung eines automatisierten Abrufverfahrens 107
1.2.2.1 Allgemeines 107
1.2.2.2 Zulässigkeit der Einrichtung 107
1.2.2.3 Zulässigkeit einzelner Abrufe 109
1.2.2.4 Zusammenfassung 109
1.3 Datenschutzrechtliche Voraussetzungen für den Datentransfer nach Österreich 110
1.4 Datenschutzrechtliche Voraussetzungen für den Datentransfer in die Schweiz 110
1.4.1 Allgemeines 110
1.4.2 Übermittlung an eine zentrale Stelle 111
1.4.3 Einrichtung eines automatischen Abrufverfahrens 111
1.5 Ergebnis 112
2. Bereitstellen von Email- / Internetdiensten 113
2.1 Überblick 113
2.2 Datenschutzrechtliche Voraussetzungen innerhalb Deutschlands 114
2.2.1 Überblick 114
2.2.2 Durchführung des Beschäftigungsverhältnisses 114
2.2.3 Für eigene Zwecke 115
2.3 Datenschutzrechtliche Voraussetzungen für den Datentransfer nach Österreich 116
2.4 Datenschutzrechtliche Voraussetzungen für den Datentransfer in die Schweiz 116
2.5 Ergebnis 116

III. Entwicklungsabteilung 117

1. Grundsätzliches ... 117
2. Datenschutzrechtliche Voraussetzungen in Deutschland ... 118
2.1 Überblick ... 118
2.2 Übermittlung an eine zentrale Stelle ... 118
2.3 Auftragsdatenverarbeitung ... 119
2.4 Einrichtung eines automatisierten Abrufverfahrens ... 119
2.4.1 Allgemeines ... 119
2.4.2 Zulässigkeit der Einrichtung eines automatisierten Abrufverfahrens ... 120
2.4.3 Zulässigkeit der einzelnen Abrufe ... 121
2.5 Zusammenfassung ... 121
3. Datenschutzrechtliche Voraussetzungen für den Datentransfer nach Österreich ... 122
4. Datenschutzrechtliche Voraussetzung für den Datentransfer in die Schweiz ... 122
4.1 Allgemeines ... 122
4.2 Übermittlung an eine zentrale Stelle ... 123
4.3 Einrichtung eines automatischen Abrufverfahrens ... 123
5. Ergebnis ... 124

ZWEITER TEIL

INFORMATIONSSICHERHEIT IM KONZERN ... 127

A. ANFORDERUNGEN AN DIE INFORMATIONSSICHERHEIT ... 127

I. Situation im Konzern ... 127

II. Grundwerte der Informationssicherheit ... 128
1. Überblick ... 128
2. Vertraulichkeit ... 128
3. Verfügbarkeit ... 129
4. Integrität ... 129

III. Gesetzliche Regelungen zur Informationssicherheit ... 129
1. Allgemeine gesetzliche Regelungen ... 129
2. IT-Sicherheitsgesetz ... 131

IV. Unternehmerische Anforderungen ... 133

B. MAßNAHMEN ZUR INFORMATIONSSICHERHEIT ... 135

I. Grundsätzliches ... 135

II. Informationssicherheitsmanagement ... 135

1. Allgemeines ... 135
2. Informationssicherheitsmanagement ... 136
   - 2.1 Überblick ... 136
   - 2.2 Informationssicherheitsbeauftragter ... 137
   - 2.3 Leitlinie / -richtlinie ... 138
   - 2.4 Risikomanagement / Klassifizierung ... 139
   - 2.5 Sensibilisierung / Schulungen ... 139
3. Lebenszyklus einer Information ... 140
4. Klassifizierung und Kennzeichnung ... 142
   - 4.1 Überblick ... 142
   - 4.2 Vertraulichkeit ... 142
     - 4.2.1 Streng geheim / Geheim ... 142
     - 4.2.2 Vertraulich ... 143
     - 4.2.3 Intern ... 143
     - 4.2.4 Öffentlich ... 143
   - 4.3 Verfügbarkeit ... 144
   - 4.4 Integrität ... 145
5. Risikomanagement ... 146
   - 5.1 Überblick ... 146
   - 5.2 Risikomanagementprozess ... 149
   - 5.3 Risikoidentifizierung und -analyse ... 149
     - 5.3.1 Analyse der Geschäftsauswirkungen ... 149
     - 5.3.2 Bedrohungsanalyse ... 149
     - 5.3.3 Schwachstellenanalyse ... 151
     - 5.3.4 Risikobewertung ... 151
   - 5.4 Risikobehandlung ... 153
   - 5.5 Dokumentation, Berichterstattung und Informationssicherheitskonzept ... 154
6. Maßnahmen der Informationssicherheit ... 154

III. Standards / Zertifizierung ... 155

1. Überblick ... 155
2. ISO 27001 ... 156
3. BSI-Grundschutz ... 157
4. Durchführung der Zertifizierung ... 158
   - 4.1 ISO 27001 ... 158
   - 4.2. BSI-Grundschutz ... 158

C. INFORMATIONSSICHERHEITSMANAGEMENT IN DEN REFERENZBEREICHEN. 159

I. Grundsätzliches 159

II. Personalwesen 159

1. Entgeltabrechnung 159

1.1. Überblick 159

1.2 Klassifizierung 160

1.2.1 Vertraulichkeit 160

1.2.2 Verfügbarkeit 161

1.2.3 Integrität 161

1.3. Risikomanagement 161

1.4 Mögliche Maßnahmen 164

2. Skill-Datenbank 164

2.1. Überblick 164

2.2 Klassifizierung 165

2.2.1 Vertraulichkeit 165

2.2.2 Verfügbarkeit 166

2.2.3 Integrität 166

2.3. Risikomanagement 166

2.4 Mögliche Maßnahmen 168

III. Informationstechnik / Informationssysteme 169

1. Konzernweites Adressbuch 169

1.1. Überblick 169

1.2 Klassifizierung 169

1.2.1 Vertraulichkeit 169

1.2.2 Verfügbarkeit 170

1.2.3 Integrität 170

1.3. Risikomanagement 170

1.4 Mögliche Maßnahmen 172

2. Bereitstellen von Email- / Internetdiensten 172

2.1. Überblick 172

2.2 Klassifizierung 173

2.2.1 Vertraulichkeit 173

2.2.2 Verfügbarkeit 173

2.2.3 Integrität 173

2.3. Risikomanagement 174

2.4 Mögliche Maßnahmen 175

IV. Entwicklungsabteilung ... 175
1. Überblick ... 175
2. Klassifizierung ... 176
2.1 Vertraulichkeit ... 176
2.2 Verfügbarkeit ... 177
2.3 Integrität ... 177
3. Risikomanagement ... 177
4. Mögliche Maßnahmen ... 179

DRITTER TEIL

SYNERGIEN VON DATENSCHUTZ UND INFORMATIONSSICHERHEIT ... 181

A. SYNERGIEN IM ALLGEMEINEN ... 181

I. Grundsätzliches ... 181

II. Gegenüberstellung der Maßnahmen ... 182
1. Technische und organisatorische Maßnahmen ... 182
1.1 Überblick ... 182
1.2 Zutrittskontrolle ... 186
1.3 Zugangskontrolle ... 189
1.4 Zugriffskontrolle ... 193
1.5 Weitergabekontrolle ... 196
1.6 Eingabekontrolle ... 199
1.7 Auftragskontrolle ... 200
1.8 Verfügbarkeitskontrolle ... 202
1.9 Trennungsgebot (Verwendungszweckkontrolle) ... 206
1.10 Synergien bei den technischen und organisatorischen Maßnahmen ... 207
2. Datenschutz- und Informationssicherheitsmanagement ... 207
2.1 Überblick ... 207
2.2 Beauftragte für Informationssicherheit / Betriebliche Datenschutzbeauftragte ... 208
2.3 Erstellen, Umsetzen und Überprüfen der Leit-/ Richtlinien ... 210
2.4 Risikomanagement ... 210
2.5 Sensibilisierung / Schulungen ... 212
2.6 Mitarbeiterverpflichtung ... 212
2.7 Bestehende Synergien ... 212

B. SYNERGIEN ANHAND DER REFERENZBEREICHE 214

I. Allgemeines 214

II. Synergien im Bereich Personalwesen 215

1. Entgeltabrechnung 215

1.1 Überblick 215

1.2 Informationssicherheitsmanagement 215

1.3 Datenschutzmanagement 217

1.4 Synergien 219

2. Skill-Datenbank 223

2.1 Überblick 223

2.2 Informationssicherheitsmanagement 223

2.3 Datenschutzmanagement 224

2.4 Synergien 226

III. Synergien im Bereich Informationstechnik / Informationssysteme 228

1. Konzernweites Adressbuch 228

1.1 Überblick 228

1.2 Informationssicherheitsmanagement 228

1.3 Datenschutzmanagement 229

1.4 Synergien 230

2. Email- / Internetprotokolldaten 233

2.1 Überblick 233

2.2 Informationssicherheitsmanagement 233

2.3 Datenschutzmanagement 234

2.4 Synergien 234

IV. Synergien im Bereich Entwicklung 237

1. Überblick 237

2. Informationssicherheitsmanagement 237

3. Datenschutzmanagement 238

4. Synergien 239

VIERTER TEIL

ERGEBNIS UND SCHLUSSFOLGERUNGEN 243

A. ERGEBNISSE DER UNTERSUCHUNG 243

B. HANDLUNGSEMPFEHLUNG FÜR KONZERNE 246

I. Integriertes Datenschutz- und Informationssicherheitsmanagement 246

II. Umsetzung 246

C. SCHLUSSFOLGERUNGEN 249

ABBILDUNGSVERZEICHNIS 253

LITERATURVERZEICHNIS 255