Inhalt

Abkürzungsverzeichnis.....XXV
Abbildungsverzeichnis.....XXXIV

1 Einleitung.....1
1.1 Cloud Computing als Dienstleistung.....6
1.2 Konsequenzen des Cloud Computing für sonstige Dienstleistungen im Internet..7
1.3 Bedeutung der Sicherheit.....8
1.3.1 IT-Sicherheit.....8
1.3.2 Rechtssicherheit.....9
1.4 Vorlaufende Technikgestaltung anhand der KORA-Methode.....10
1.5 Rolle des Rechts im Verhältnis zur Technik.....10
1.5.1 Einordnung der KORA-Methode in den Gesamtzusammenhang.....10
1.5.2 Technikrecht als historisch gewachsenes Beispiel für das Verhältnis zwischen Recht und Technik.....12
1.6 Forschungsbedingungen und Notwendigkeit einer interdisziplinären Herangehensweise.....14
1.7 Gang der Untersuchung.....14

2 Untersuchungsgegenstand.....16
2.1 Begriff des Cloud Computing.....16
2.1.1 Cloud Computing als Hype?.....17
2.1.2 Definitionsversuche.....22
2.1.3 Vorzugswürdige Definition.....24
2.1.4 Informationstechnische Systeme, Cloudsysteme und Cloudumgebungen.....24
2.2 Begriffliche Einordnung.....25
2.2.1 Technologie und Technik.....26
2.2.2 Konzept.....26
2.2.3 Paradigma und Inhalt des Paradigmenwechsels.....27

Bibliografische Informationen
http://d-nb.info/1031105948

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

2.2.4 Geschäftsmodell 28
2.2.5 Konsequenzen der begrifflichen Einordnung 28
2.3 Detailstruktur des Cloud Computing 28
2.3.1 Architektur und Erscheinungsformen (Schichtenmodell) 29
2.3.1.1 Infrastructure as a Service (IaaS) 29
2.3.1.2 Platform as a Service (PaaS) 30
2.3.1.3 Software as a Service (SaaS) 30
2.3.1.4 Weitere Services (XaaS) 31
2.3.2 Nutzungsmodelle 32
2.3.2.1 Public und External Cloud 32
2.3.2.2 Private Cloud 33
2.3.2.3 Internal Cloud 33
2.3.2.4 Hybrid Cloud 34
2.3.2.5 Virtual Private Cloud 35
2.3.2.6 Community Cloud 36
2.3.3 Beteiligte 37
2.3.3.1 Cloudnutzer und Cloudanbieter 37
2.3.3.2 Ressourcenanbieter (Subunternehmen) 38
2.3.3.3 Telekommunikationsanbieter 38
2.3.4 Technische und infrastrukturelle Voraussetzungen 38
2.3.4.1 Virtualisierung 39
2.3.4.1.1 Vorteile der Virtualisierung 39
2.3.4.1.2 Virtualisierung und Cloud Computing 40
2.3.4.2 Virtualisierungsformen 41
2.3.4.2.1 Hypervisorbasierte Virtualisierung 42
2.3.4.2.2 Netzwerkvirtualisierung mittels VLAN und VPN 42
2.3.4.2.3 Speichervirtualisierung 43
2.3.4.3 Verteilte Systeme, Parallelisierung und Computercluster 43
2.3.4.4 Flächendeckende Durchsetzung von Breitbandinternetzugängen 45
2.3.5 Merkmale und Eigenschaften des Cloud Computing 47
2.3.5.1 Mehrmandantenfähigkeit 47

2.3.5.2 Schnelle Bereitstellung und Self-Service-Modell 47
2.3.5.3 Einfachere Wartung und Aufrüstung 48
2.3.5.4 On-Demand-Nutzung 49
2.3.5.5 Geographische Verteilung der Server 49
2.3.5.6 Zuverlässigkeit, Verfügbarkeit und Robustheit 50
2.3.5.7 Skalierbarkeit 51
2.3.5.8 Homogenität 51
2.3.5.9 Messbarkeit und Überprüfbarkeit 52
2.3.5.10 Lizenzfreiheit und -klarheit 52
2.3.6 Entwicklung des Cloud Computing und Abgrenzung zu seinen Vorläufermodellen 52
2.3.6.1 Internet und verteilte Systeme 54
2.3.6.2 Cluster Computing 55
2.3.6.3 Grid Computing 56
2.3.6.4 Utility Computing 58
2.3.6.5 Klassisches IT-Outsourcing 58
2.3.6.6 Application Service Providing (ASP) 61
2.3.6.7 Verhältnis von Cloud Computing zu serviceorientierten Architekturen (SoA) 63
2.3.7 Anwendungsbereiche, Anwendungsbeispiele und Einsatzszenarien 64
2.3.7.1 Privatbereich 64
2.3.7.1.1 Mailservices 64
2.3.7.1.2 Fotodienste und Webalben 65
2.3.7.1.3 Filehosting und Storage 65
2.3.7.1.4 Spiele (Cloud Gaming) 66
2.3.7.1.5 Weitere Dienste 68
2.3.7.2 Unternehmensbereich 69
2.3.7.2.1 Startupunternehmen 69
2.3.7.2.2 Unternehmen mit bestehender Infrastruktur 69
2.3.7.2.3 Konkrete Anwendungsbereiche in Unternehmen 70
2.3.7.3 Behörden und öffentliche Verwaltung 71

2.3.8 Ausgewählte Cloudprovider 72
2.3.8.1 Amazon 73
2.3.8.2 Salesforce 76
2.3.8.3 Google 78
2.3.8.4 Microsoft 80
2.3.9 Weitere Cloudprovider 82
2.3.10 Provider im öffentlichen Bereich 83
2.4 Soziale Folgen des Cloud Computing 84
2.4.1 Chancen und Risiken des Cloud Computing 85
2.4.1.1 Vorteile und Chancen 85
2.4.1.1.1 Kostenersparnis 85
2.4.1.1.2 Förderung des Wirtschaftswachstums 87
2.4.1.1.3 Hohe Skalierbarkeit 88
2.4.1.1.4 Verfügbarkeit 89
2.4.1.1.5 Elastizität und Flexibilität 90
2.4.1.1.6 Energieeffizienz und Umweltschutz 90
2.4.1.1.7 Ortsunabhängigkeit 93
2.4.1.1.8 Einfachheit 94
2.4.1.1.9 Unabhängigkeit von proprietären Betriebssystemen 94
2.4.1.1.10 Sicherheit 95
2.4.1.1.11 Verringerung von Datensätzen und Verarbeitungsvorgängen durch Zentralisierung 97
2.4.1.1.12 Demokratisierung und Innovationsförderung 98
2.4.1.1.13 Zukunftssicherheit 99
2.4.1.2 Nachteile und Risiken 101
2.4.1.2.1 Unvorhersehbare Fehler 101
2.4.1.2.2 Lock-In-Effekte und fehlende Standards 102
2.4.1.2.3 Oligopolbildung und marktbeherrschende Stellung 103
2.4.1.2.4 Gefahr der Profilbildung und Weitergabe von Daten 103
2.4.1.2.5 Bedrohungen 104

3 Rechtsrahmen und rechtliche Aspekte des Cloud Computing 105
3.1 Datenschutzrecht 105
3.1.1 Entwicklung des Datenschutzrechts 105
3.1.2 Zwischenstaatliche Regelungen zum Datenschutz 107
3.1.2.1 Internationale Abkommen 107
3.1.2.2 Europarecht und Europäische Abkommen 108
3.1.2.2.1 EU-Ebene 108
3.1.2.2.2 Europaratsebene 109
3.1.3 Nationales Verfassungsrecht 110
3.1.3.1 Recht auf informationelle Selbstbestimmung 110
3.1.3.2 Vertraulichkeit und Integrität informationstechnischer Systeme 112
3.1.3.3 Telekommunikationsgeheimnis 113
3.1.3.4 Wirtschaftsgrundrechte 113
3.1.4 Cloud Computing als Telekommunikation oder Telemedium? 115
3.1.4.1 Cloud Computing als Telekommunikationsdienstleistung? 115
3.1.4.2 Cloud Computing als Telemediendienst? 116
3.1.4.3 Konsequenzen für den Datenschutz und Abgrenzung 116
3.1.5 Anwendungs- und Geltungsbereich des Bundesdatenschutzgesetzes 118
3.1.5.1 Normadressaten 118
3.1.5.2 Sachlicher Anwendungsbereich 118
3.1.5.3 Personenbezogene Daten 119
3.1.5.3.1 Definition gemäß § 3 BDSG und Relativität des Personenbezugs 119
3.1.5.3.2 Einordnung verschlüsselter personenbezogener Daten 120
3.1.5.4 Räumlicher Geltungsbereich 121
3.1.6 Datenschutzprinzipien 123
3.1.6.1 Notwendigkeit eines Erlaubnistatbestands und Gedanke der Selbstbestimmung 123
3.1.6.2 Transparenz 123
3.1.6.3 Grundsatz der Direkterhebung 124
3.1.6.4 Erforderlichkeit 124

3.1.6.5 Datenvermeidung und Datensparsamkeit 125
3.1.6.6 Zweckfestlegung, Zweckbindung, informationelle Gewaltenteilung 127
3.1.7 Cloud Computing und Behörden 128
3.1.7.1 Datenschutzrecht 128
3.1.7.2 Verbot der Mischverwaltung gemäß Art. 83 GG 129
3.1.7.3 IT-Zusammenarbeit gemäß Art. 91c GG 130
3.1.8 Auftragsdatenverarbeitung 130
3.1.8.1 Auftrag 131
3.1.8.2 Beteiligte, Privilegierungsfunktion und Rechtsstellung 132
3.1.8.3 Theorie der Funktionsübertragung 133
3.1.8.4 Cloud Computing als Auftragsdatenverarbeitung? 136
3.1.8.4.1 Infrastructure as a Service 137
3.1.8.4.2 Restliche Services (PaaS, SaaS) 138
3.1.8.5 Detailstruktur der Auftragsdatenverarbeitung 139
3.1.8.5.1 Pflichten des Auftraggebers und wesentliche Merkmale einer Auftragsdatenverarbeitung den Auftraggeber betreffend 139
3.1.8.5.2 Kontrollrechte des Auftraggebers 148
3.1.8.5.3 Pflichten des Auftragnehmers 149
3.1.8.5.4 Wartungs- und Servicearbeiten 151
3.1.8.5.5 Bußgeldtatbestände 151
3.1.8.6 Mögliches Transparenzproblem und Problem der Unterbeauftragung (Auslagerungsketten) 152
3.1.8.7 Spezialregelungen 154
3.1.8.8 Datenschutzrechtlicher Reformbedarf 156
3.1.9 Technisch-organisatorische Maßnahmen zur IT- und Datensicherheit 157
3.1.9.1 IT-Sicherheit und Datensicherheit 157
3.1.9.2 Bedeutung der Sicherheit allgemein und für den weiteren Gang der Untersuchung 158
3.1.9.3 Geltende Rechtslage 160
3.1.9.3.1 Regelungsinhalt des § 9 BDSG und der Anlage zu Satz 1 161
3.1.9.3.2 Maßnahmen gemäß der Anlage 162

3.1.9.3.2.1 Zutrittskontrolle (Nr. 1) 163
3.1.9.3.2.2 Zugangskontrolle (Nr. 2) 164
3.1.9.3.2.3 Zugriffs- und Speicherkontrolle (Nr. 3) 166
3.1.9.3.2.4 Weitergabekontrolle (Nr. 4) 167
3.1.9.3.2.5 Eingabekontrolle (Nr. 5) 169
3.1.9.3.2.6 Auftragskontrolle (Nr. 6) 170
3.1.9.3.2.7 Verfügbarkeitskontrolle (Nr. 7) 171
3.1.9.3.2.8 Trennungsgebot (Nr. 8) 172
3.1.9.3.3 Spezialvorschrift des § 109 TKG 172
3.1.9.3.4 Wertungen des Bundesverfassungsgerichts zur Vorratsdatenspeicherung 174
3.1.9.4 Datenschutzrechtlicher Reformbedarf 175
3.1.9.5 Schutzziele der IT-Sicherheit 176
3.1.9.5.1 Vertraulichkeit 176
3.1.9.5.2 Unverkettbarkeit 177
3.1.9.5.3 Nicht-Verfolgbarkeit 178
3.1.9.5.4 Unbeobachtbarkeit 179
3.1.9.5.5 Verdecktheit 179
3.1.9.5.6 Anonymität und Pseudonymität 180
3.1.9.5.7 Transparenz 181
3.1.9.5.8 Zurechenbarkeit 182
3.1.9.5.9 Authentizität 183
3.1.9.5.10 Revisionsfähigkeit 183
3.1.9.5.11 Verfügbarkeit 184
3.1.9.5.12 Integrität 185
3.1.9.5.13 Verlässlichkeit 185
3.1.9.5.14 Beherrschbarkeit 186
3.1.9.5.15 Nicht-Vermehrbarkeit 186
3.1.9.5.16 Kontingenz und glaubhafte Abstreitbarkeit 187
3.1.9.6 Konzept der mehrseitigen Sicherheit 188
3.1.9.7 Zentrale Probleme des Cloud Computing 190

3.1.9.7.1 Vertraulichkeit 190
3.1.9.7.2 Integrität 191
3.1.9.7.3 Transparenz 192
3.1.9.7.3.1 Technikbedingte Intransparenz 193
3.1.9.7.3.2 Anbieterbedingte Intransparenz 193
3.1.9.7.4 Bedeutung sonstiger Schutzziele 194
3.1.9.8 Bedrohungsanalyse 194
3.1.9.8.1 Begriffsdefinitionen und gegenseitige Abgrenzung 196
3.1.9.8.1.1 Bedrohung, Gefährdung und verwandte Begriffe 196
3.1.9.8.1.2 Bedeutungen des Gefahrbegriffs und Abgrenzung zur Gefährdung 197
3.1.9.8.1.3 Schadensbegriff 199
3.1.9.8.1.4 Risiko und Risikovorsorge 201
3.1.9.8.2 Bedrohungsklassifizierungen 204
3.1.9.8.2.1 Unbeabsichtigte Eingriffe 204
3.1.9.8.2.2 Beabsichtigte Eingriffe 205
3.1.9.8.3 Komplexität und IT-Sicherheit 206
3.1.9.8.4 Angreifertypen 209
3.1.9.8.5 Angriffsarten 210
3.1.9.8.5.1 Passive Angriffe 210
3.1.9.8.5.2 Aktive Angriffe 212
3.1.9.9 Allgemeine Sicherheitsmaßnahmen 213
3.1.9.9.1 Verschlüsselung 214
3.1.9.9.2 Systemtrennung, Abschottung und Kanalisierung von Datenströmen 215
3.1.9.9.3 Datentrennung 216
3.1.9.9.4 Rollentrennung 217
3.1.9.9.5 Protokollierung 217
3.1.9.9.6 Redundanz 218
3.1.9.9.7 Nutzungskompetenz und IT-Sicherheitsbewusstsein 218
3.1.9.9.8 Audits und Zertifizierungen 219

3.1.9.10 Neuartige cloudspezifische Bedrohungen und notwendige Sicherheitsmaßnahmen 221
3.1.9.10.1 Bedrohungen durch unzureichende Trennung und Segmentierung 221
3.1.9.10.1.1 Hypervisorsicherheit 222
3.1.9.10.1.2 Absicherung des Management Interfaces und des Datenverkehrs durch Trennung 224
3.1.9.10.2 Kontrollverlust durch Verteilung 225
3.1.9.10.3 Kontrollverlust durch die Weiterübermittlung von Daten 226
3.1.9.10.4 Abhängigkeit der Nutzer vom Provider in Sicherheitsfragen 226
3.1.9.10.5 SoA-bedingte Bedrohungen 227
3.1.9.10.6 Bedrohungen für Rechtsgüter Dritter durch Clouddienste 227
3.1.9.11 Sicherheitskonzept 228
3.1.10 Datenschutzaudit 229
3.1.11 Verpflichtung der Mitarbeiter auf das Datengeheimnis 231
3.1.12 Datenübermittlung ins außereuropäische Ausland 233
3.1.12.1 Erlaubnisnormen und Zusammenwirken mit §§ 4b und 4c BDSG 234
3.1.12.1.1 Öffentliche und nichtöffentliche Stellen als Übermittler 234
3.1.12.1.2 Erforderlichkeit 235
3.1.12.1.3 Weitere Voraussetzungen 235
3.1.12.1.4 Interesse des Betroffenen an einem Ausschluss der Übermittlung 236
3.1.12.1.5 Einwilligung 237
3.1.12.1.6 Zwischenergebnis 237
3.1.12.2 Besondere Arten personenbezogener Daten 237
3.1.12.3 Bereichsspezifische Vorschriften außerhalb des BDSG 238
3.1.12.4 Angemessenheit des Datenschutzniveaus als Interessensaspekt 239
3.1.12.5 Ausnahmen gemäß § 4c BDSG 239
3.1.12.5.1 EU-Standardvertragsklauseln 241
3.1.12.5.1.1 Inhalt und Bedeutung 241
3.1.12.5.1.2 Möglichkeit der Unterauftragsverarbeitung 242

3.1.12.5.1.3 Anwendbarkeit bei innereuropäischer Unterauftragsdatenverarbeitung? ... 243
3.1.12.5.2 Binding Corporate Rules und Codes of Conduct ... 247
3.1.12.5.3 Safe-Harbor-Übereinkommen ... 248
3.1.12.6 Verhältnis zur Auftragsdatenverarbeitung ... 253
3.2 Infrastrukturrecht ... 256
3.2.1 Cloud Computing als kritische Infrastruktur? ... 257
3.2.2 Staatliche Schutz- und Gewährleistungspflicht für Cloudinfrastruktur? ... 259
3.3 Deutsches und europäisches Kartellrecht ... 260
3.4 Internationales Privatrecht ... 263
3.5 Vertragsrecht ... 265
3.5.1 Vertragstypologische Einordnung ... 265
3.5.1.1 Bereitstellung von Speicherplatz ... 266
3.5.1.2 Bereitstellung von Software und Verarbeitung von Daten ... 267
3.5.1.3 Bereitstellung von Rechenleistung ... 268
3.5.2 Back-to-Back-Verträge zwischen Cloudprovidern und Subunternehmen ... 269
3.5.3 Service Level Agreements (SLAs) ... 269
3.5.3.1 Funktion und Formen ... 269
3.5.3.2 Vertragsgestaltung und konkrete Regelungsinhalte ... 271
3.5.3.2.1 Leistungspflichten und Leistungsbeschreibung ... 271
3.5.3.2.2 Reaktions- und Mängelbeseitigungsfristen ... 272
3.5.3.2.3 Verfügbarkeit und Latenzzeiten ... 272
3.5.3.2.4 Service Level Management ... 273
3.5.3.2.5 Sanktionen ... 274
3.5.3.2.6 Vertragsbeendigung und weiterer Umgang mit Daten (Exit Management) ... 275
3.5.3.2.7 Urheber- und Nutzungsrechte ... 276
3.5.3.2.8 Datenschutz, Rechtswahl und Gerichtsstand ... 276
3.5.3.3 Einschränkungen durch AGB-Recht ... 276
3.5.4 Bedeutung von DIN SPEC 1041 ... 278
3.6 Compliance und Aufbewahrungspflichten ... 280

3.6.1 Allgemeine Compliancevorschriften, Haftung und Risikomanagement 280
3.6.2 Bereichsspezifische Regelungen (Risikomanagement, territoriale Beschränkungen und nationale Aufbewahrungspflichten) 282
3.7 Urheberrecht 283
3.7.1 Lizenzierung der Software und Wegfall des Lizenzmanagements für die Nutzer 283
3.7.2 Geltende Rechtslage nach dem UrhG 285
3.7.3 Internationales Urheberrecht 287
3.7.3.1 Räumlicher Anwendungsbereich 287
3.7.3.2 Völkerrechtliche Verträge 288
3.7.3.3 Persönlicher Anwendungsbereich 288
3.7.3.4 Kollisionsrecht und Internationales Privatrecht 289
3.7.4 Bedeutung für Cloud Computing 289
3.7.4.1 Verhältnis zwischen Softwarehersteller und Cloudprovider 289
3.7.4.2 Verhältnis zwischen Cloudprovider und Cloudnutzer 290
3.7.4.2.1 Rechtmäßige Nutzungshandlungen 291
3.7.4.2.2 Verletzungshandlungen (Unerlaubte Handlungen) 291
3.8 Strafrecht, Strafprozessrecht, Strafverfolgung und Cloudforensik 292
3.8.1 Probleme bei der Strafverfolgung und neue Ermittlungsansätze 292
3.8.1.1 Telekommunikationsüberwachung gemäß § 100a StPO mittels Deep Packet Inspection 296
3.8.1.1.1 Funktionsweise der Deep Packet Inspection 296
3.8.1.1.2 Deep Packet Inspection und deren Relevanz für die IT-Sicherheit 298
3.8.1.1.3 Rechtliche Bedeutung 299
3.8.1.2 Strafrechtliche Regelungen zum Geheimnisschutz 299
3.9 Bezüge zum Recht der Vereinigten Staaten 302
3.9.1 Electronic Discovery 302
3.9.1.1 Beschreibung und Besonderheiten der e-Discovery 302
3.9.1.2 Probleme im Zusammenhang mit Cloud Computing 303
3.9.1.3 Konflikt zwischen US-Recht und deutschem Datenschutzrecht 305
3.9.2 USA PATRIOT Act 308

3.9.3 Auskunfts- und Aufbewahrungspflichten nach dem Sarbanes-Oxley-Act .309
3.10 Empfehlungen zur Rechtsgestaltung 310

4 Gestaltung rechtsverträglicher Cloudsysteme 315
4.1 Notwendigkeit und Maßstab der rechtlichen Gestaltung von Technik 315
4.2 Rechtliche Gestaltung anhand der KORA-Methode 315
4.3 Ableitung von rechtlichen Anforderungen aus grundrechtlichen Vorgaben 316
4.4 Rechtliche Kriterien 319
4.4.1 Techniksicherheit (K1) 319
4.4.2 Vertraulichkeit (K2) 319
4.4.3 Transparenz (K3) 320
4.4.4 Entscheidungsfreiheit (K4) 321
4.4.5 Erforderlichkeit (K5) 322
4.4.6 Zweckbindung (K6) 323
4.4.7 Trennbarkeit (K7) 324
4.4.8 Beherrschbarkeit und Steuerungsfähigkeit (K8) 324
4.4.9 Überprüfbarkeit (K9) 325
4.4.10 Beweissicherung (K10) 326
4.4.11 Integrität (K11) 326
4.4.12 Verfügbarkeit (K12) 327
4.5 Technische Gestaltungsziele 327
4.5.1 Verschlüsselung von Daten und Datenträgern (Z1) 327
4.5.2 Etablierung eines umfassenden Management Interfaces (Z2) 328
4.5.3 Sicherung des Interfaces durch Zugriffsschutzverfahren (Z3) 328
4.5.4 Etablierung und technische Umsetzung des Vieraugenprinzips (Z4) 328
4.5.5 Nutzung von Identitäts- und Zugriffsmanagementsystemen (Z5) 329
4.5.6 Sichere Authentisierung (Z6) 329
4.5.7 Trennung des Nutzertraffic vom administrativen Datenverkehr (Z7) 330
4.5.8 Trennung der virtuellen Nutzersysteme durch sichere Hypervisoren (Z8) .330
4.5.9 Implementierung von Dokumentationsfunktionen (Z9) 330

4.5.10 Keine Weitergabe von administrativen Protokollen (Z10) 331
4.5.11 Kein Zugriff des Providers auf Protokollinhalte der Nutzer (Z11) 331
4.5.12 Sicherung der Protokolldaten durch Zugriffsschutzverfahren (Z12) 331
4.5.13 Sichere Löschung der Protokolldaten (Z13) 331
4.5.14 Sichere Löschung sonstiger Daten (Z14) 331
4.5.15 Bestätigung der Löschung von Daten bei Subunternehmen (Z15) 332
4.5.16 Aufbau von Redundanzen (Z16) 332
4.5.17 Nutzung von Fehlerkorrekturverfahren, Checksummen und Hashwerten (Z17) 332
4.5.18 Technisch unterstützte Auswahl von Subunternehmen (Z18) 334
4.5.19 Regelbasiertes Load Balancing (Z19) 334
4.5.20 Etablierung und Nutzung standardisierter Schnittstellen und APIs (Z20) 335
4.5.21 Fortschreitende Abstraktion und Zusammenfassung zu logischen Geräten (Z21) 335
4.6 Technische Gestaltungsvorschläge 337
4.6.1 Verschlüsselung der beim Datentransport übermittelten Daten (G1) 337
4.6.2 Verschlüsselung während der Speicherung (G2) 338
4.6.3 Sichere Schlüssel- und Passwortverwaltung (G3) 338
4.6.4 Trennung von Schlüsseln und Daten (G4) 339
4.6.5 Nutzung von homomorphen Verschlüsselungsalgorithmen (G5) 339
4.6.6 Trennung der verarbeitenden Rechner von der Cloudinfrastruktur während der Verarbeitung (G6) 340
4.6.7 Einsatz von bewährten und gehärteten Hypervisoren (G7) 341
4.6.8 Verteilung und Replizierung der Daten auf unterschiedliche physische Server (G8) 341
4.6.9 Identifizierung und Authentisierung mittels tauglicher Identifikationsverfahren (G9) 343
4.6.10 Nutzung von geeigneten und erprobten Zugriffs- und Identitätsmanagementsystemen (G10) 343
4.6.11 Bereitstellung von Steuerungs- und Monitoringoberflächen und Data Tracking Tools (G11) 344
4.7 KORA-Methode als disziplinenübergreifende Methode im Cloud-Computing-Kontext 345

5 Schlussbetrachtungen **347**

5.1 Zusammenfassung der Erkenntnisse und Ergebnisse 347

5.2 Ausblick und künftiger Forschungsbedarf 350

Anlage 353

Literaturverzeichnis 356