

Johanna M. Hofmann

Dynamische Zertifizierung

Datenschutzrechtliche Zertifizierung nach der Datenschutz-
Grundverordnung am Beispiel des Cloud Computing



Nomos

Inhaltsverzeichnis

Tabellenverzeichnis	19
Danksagung	21
Abkürzungsverzeichnis	23
1 Einleitung	29
1.1 Das Problem	30
1.1.1 Vermittlungsprobleme zwischen Technik und Recht	31
1.1.2 Mehrdimensionale Intransparenz	34
1.1.3 Mehrdimensionaler Kontrollverlust	37
1.1.4 Mangelhafte Nachweisbarkeit	38
1.1.5 Beschränkte Abhilfe durch herkömmliche Zertifizierungsverfahren	40
1.2 Die Lösung	42
1.3 Gegenstand der Untersuchung und deren Grenzen	44
1.4 Gang der Untersuchung	47
2 Grundlagen des Cloud Computing	49
2.1 Definition	49
2.2 Beteiligte	51
2.3 Bereitstellungsmodelle	52
2.4 Dienstmodelle	53
2.5 Zwischenergebnis	54
3 Cloudrelevante Rechtsfragen	57
3.1 Begriffliche Abgrenzung von Daten und Informationen	57
3.1.1 Das Datum	58
3.1.2 Die Information	59

3.2 Die Grundrechte und Verfassungswerte als Maßstab der Technikgestaltung	60
3.2.1 Nationale Grundrechte und Prinzipien	62
3.2.1.1 Recht auf informationelle Selbstbestimmung	63
3.2.1.2 Recht auf Integrität und Vertraulichkeit informationstechnischer Systeme	65
3.2.1.3 Grundrecht auf Eigentum	67
3.2.1.4 Berufsfreiheit	68
3.2.1.5 Fernmeldegeheimnis	68
3.2.1.6 Meinungs-, Forschungs- und Rundfunkfreiheit	69
3.2.1.7 Allgemeine Handlungsfreiheit	70
3.2.2 Unionsgrundrechte und allgemeine Grundsätze	70
3.2.2.1 Recht auf Achtung des Privat- und Familienlebens sowie der Kommunikation	73
3.2.2.2 Schutz personenbezogener Daten	75
3.2.2.3 Grundrecht auf Eigentum	77
3.2.2.4 Unternehmerische Freiheit	78
3.2.2.5 Freiheit der Meinungsäußerung, Informations- und Medienfreiheit	79
3.2.2.6 Allgemeine Handlungsfreiheit	80
3.2.2.7 Freier Datenverkehr	80
3.3 Materielles Datenschutz- und Datensicherheitsrecht	81
3.3.1 Datenschutz und Datensicherheit	81
3.3.1.1 Schutzrichtungen	81
3.3.1.2 Interessenlagen	85
3.3.1.3 Schutzgrade	85
3.3.2 Anwendbarkeit des Datenschutz- und Datensicherheitsrechts	86
3.3.2.1 Internationale Regelungen	86
3.3.2.2 Europäische Regelungen	88
3.3.2.2.1 Primärrecht	88
3.3.2.2.2 Datenschutz-Grundverordnung	89
3.3.2.2.2.1 Sachlicher Anwendungsbereich	94
3.3.2.2.2.2 Räumlicher Anwendungsbereich	98
3.3.2.2.2.3 Persönlicher Anwendungsbereich	100
3.3.2.2.3 Cybersicherheitsrichtlinie	102

3.3.2.2.4	Durchführungsverordnung zur Cybersicherheitsrichtlinie	103
3.3.2.2.5	Ausblick auf die ePrivacy-Verordnung	104
3.3.2.2.6	Ausblick auf die Verordnung über nicht- personenbezogene Daten	107
3.3.2.3	Nationales Recht	108
3.3.2.3.1	Anwendungsbereich des Bundesdatenschutzgesetzes	112
3.3.2.3.2	Anwendungsbereich des Telekommunikationsgesetzes	113
3.3.2.3.3	Anwendungsbereich des Telemediengesetzes	115
3.3.2.3.4	Anwendungsbereich des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik	117
3.3.2.3.5	Anwendbarer bereichsspezifischer Datenschutz	118
3.3.2.4	Zusammenfassung der anwendbaren Regelungen aus Unions- und nationalem deutschen Recht	119
3.3.3	Zulässiges Cloud Computing nach dem Unionsrecht	120
3.3.3.1	Cloud Computing unter der Datenschutz- Grundverordnung	120
3.3.3.1.1	Zulässige Datenverarbeitung im Auftrag	122
3.3.3.1.2	Rechtmäßige Auftragserteilung	126
3.3.3.1.2.1	Format	126
3.3.3.1.2.2	Regelungsgegenstand	129
3.3.3.1.3	Verantwortungsverteilung	130
3.3.3.1.3.1	Verantwortung des Cloud- Kunden	132
3.3.3.1.3.2	Verantwortung des Cloud- Anbieters	132
3.3.3.1.3.3	Verantwortung des weiteren Auftragsverarbeiters	134
3.3.3.1.3.4	Gemeinsame Verantwortung	135
3.3.3.1.4	Pflichten der Beteiligten bei der Auftragsverarbeitung	136
3.3.3.1.4.1	Pflichten aller an der Auftragsverarbeitung Beteiligten	136

3.3.3.1.4.2	Weitergehende Pflichten des Verantwortlichen	138
3.3.3.1.4.3	Weitergehende Pflichten des Auftragsverarbeiters	141
3.3.3.1.4.4	Weitergehende Pflichten des weiteren Auftragsverarbeiters	142
3.3.3.1.5	Beteiligung außereuropäischer Datenverarbeiter	143
3.3.3.2	Durchführungsverordnung für die Cybersicherheitsrichtlinie	147
3.3.3.3	Ausblick auf die ePrivacy-Verordnung	147
3.3.3.4	Verordnung über nicht-personenbezogene Daten	149
3.3.4	Zulässiges Cloud Computing nach deutschem Recht	149
3.3.4.1	Nationales bereichsspezifisches Datenschutzrecht mit Cloudrelevanz	149
3.3.4.2	Nationales Datensicherheitsrecht mit Cloudrelevanz	150
3.3.4.3	Regelungen des Bundesdatenschutzgesetzes	152
3.4	Geheimnisschutzrecht	153
3.5	Technische Normung	157
3.6	Zwischenfazit	160
4	Grundlagen datenschutzrechtlicher Konformitätsbewertung	162
4.1	Geschichtlicher Hintergrund der Konformitätsbewertung	165
4.2	Begriffsklärung bei der Konformitätsbewertung	170
4.2.1	Zertifikat	170
4.2.2	Zertifizierung	171
4.2.2.1	Datenschutzrechtliche Zertifizierungsverfahren	171
4.2.2.2	Zertifizierer	174
4.2.2.3	Überwachung des Gegenstands	174
4.2.3	Datenschutzsiegel	175
4.2.4	Gütesiegel	175
4.2.5	Gütezeichen	176
4.2.6	Testat	177
4.2.7	Audit und Auditierung	177
4.2.8	Akkreditierung	179
4.3	Beteiligte am Zertifizierungsverfahren	181

4.4	Interessen der Beteiligten an einer Zertifizierung des Cloud-Anbieters	183
4.4.1	Interessen der Zertifizierer	184
4.4.2	Interessen des Cloud-Anbieters	184
4.4.3	Interessen des Cloud-Kunden	186
4.4.3.1	Vertrauen in den Cloud-Anbieter	187
4.4.3.2	Vertrauensverlagerung auf den Zertifizierer	189
4.4.4	Interessen der Kontrollstelle	191
4.4.5	Interessen der betroffenen Personen	192
4.5	Zwischenergebnis und Ablauf eines Zertifizierungsverfahrens	192
5	Zertifizierungsrelevante Rechtsfragen	194
5.1	Zertifizierungsrelevante Unionsregelungen	194
5.1.1	Grundrechte und allgemeine Prinzipien des Unionsrechts	194
5.1.1.1	Recht auf ordnungsgemäße Verwaltung	197
5.1.1.2	Gleichheitsgrundsatz	199
5.1.1.3	Rechtsstaatlichkeit	200
5.1.1.4	Recht auf wirksamen Rechtsbehelf	201
5.1.1.5	Verbraucherschutz	201
5.1.1.6	Berufsfreiheit	202
5.1.2	Zertifizierungsrelevante Regelungen der Datenschutz-Grundverordnung	203
5.1.2.1	Zertifizierungszuständigkeit	204
5.1.2.1.1	Zuständigkeit der Aufsichtsbehörde	205
5.1.2.1.1.1	Grenzüberschreitender Bezug	206
5.1.2.1.1.2	Kein grenzüberschreitender Bezug	207
5.1.2.1.1.3	Zuständigkeitsverschiebung durch das Näheprinzip	207
5.1.2.1.1.4	Zwischenergebnis	208
5.1.2.1.2	Zuständigkeit der akkreditierten Stelle und Akkreditierung	209
5.1.2.1.3	Zertifizierungszuständigkeit bei Drittstaatendatenverarbeitern	212
5.1.2.1.3.1	Zuständige Aufsichtsbehörde durch Analogie?	213

5.1.2.1.3.1.1	Keine Bestimmung über den „engeren Bezug“	214
5.1.2.1.3.1.2	Keine Bestimmung anhand der übermittelnden Stelle	215
5.1.2.1.3.1.3	Bestimmung über den Vertreter	216
5.1.2.1.3.2	Zuständigkeit der akkreditierten Stelle	217
5.1.2.2	Gegenstand der Zertifizierung	218
5.1.2.2.1	Verfahrensbezogenheit	218
5.1.2.2.2	Kein „Mehr“ an Datenschutz erforderlich	219
5.1.2.2.3	Mittelbare Überprüfung von Diensten und Produkten	221
5.1.2.2.4	De facto Zertifizierung von Cloud-Diensten im Einzelfall	223
5.1.2.3	Prüfung anhand genehmigter Kriterienkataloge	224
5.1.2.3.1	Abstraktheit	225
5.1.2.3.2	Vorschlag	226
5.1.2.3.3	Billigungsverfahren	227
5.1.2.4	Zertifizierungsumfang	227
5.1.2.5	Erst- und Rezertifizierung	228
5.1.2.6	Rechtsfolgen von Zertifizierungen	231
5.1.2.7	Rechtsnatur von Zertifizierungen	232
5.1.2.7.1	Handlungsformen der Grundverordnung	232
5.1.2.7.2	Handlungsformen des nationalen Rechts	234
5.1.2.7.3	Privatrechtliche Zertifizierung	235
5.1.2.7.4	Rechtscharakter der Zertifizierung	238
5.1.2.8	Ansprüche im Zusammenhang mit dem Zertifizierungsverfahren	238
5.1.2.8.1	Anspruch auf Durchführung eines Zertifizierungsverfahrens	239
5.1.2.8.2	Anspruch auf Prüfung anhand eines festgelegten Verfahrens	240
5.1.2.8.3	Anspruch auf Prüfung anhand von genehmigten Prüfkatalogen	241
5.1.2.8.4	Anspruch auf Erteilung einer Zertifizierung	242

5.1.2.8.5	Anspruch auf erneute Zertifizierung nach Ablauf der Höchstfrist	243
5.1.2.8.6	Kein Anspruch auf Unterlassen nachträglicher Überwachung	244
5.1.2.8.7	Anspruch auf angemessene Würdigung des Zertifikats	246
5.1.2.8.8	Zwischenergebnis	247
5.1.2.9	Pflichten der Beteiligten	247
5.1.2.10	Werbung mit einem Zertifikat	250
5.1.2.11	Beweiswert eines Zertifikats	252
5.1.2.12	Handlungsbedarf	253
5.1.3	Weitere zertifizierungsrelevante Unionsregelungen	253
5.1.3.1	Europäische Akkreditierungsverordnung	254
5.1.3.2	Unionsregelungen zur IT- und datensicherheitsrechtlichen Zertifizierung	255
5.2	Nationales Zertifizierungsrecht	257
5.2.1	Verfassungsrechtliche Grundlagen	257
5.2.1.1	Grundrecht auf Eigentum	259
5.2.1.2	Berufsfreiheit	259
5.2.1.3	Meinungsfreiheit	261
5.2.1.4	Allgemeine Handlungsfreiheit	261
5.2.1.5	Rechtsstaatsprinzip	262
5.2.1.6	Demokratieprinzip	267
5.2.1.7	Sozialstaatsprinzip	268
5.2.2	Einfachgesetzliche Grundlagen des Zertifizierungsverfahrens	268
5.2.2.1	Nationales Akkreditierungsrecht	269
5.2.2.2	Nationale Regelungen zur IT-Sicherheit	270
5.2.2.3	Nationales Wettbewerbsrecht	272
5.2.2.3.1	Zulässige Werbung mit Genehmigung	274
5.2.2.3.2	Zulässige Werbung mit Bestätigung	276
5.2.2.3.3	Keine Irreführung bei wahren Angaben	278
5.2.2.3.4	Keine Werbung mit einer Selbstverständlichkeit	278
5.2.2.3.5.1	Informationsinteresse aufgrund Unkenntnis	280
5.2.2.3.5.2	Informationsinteresse aufgrund Misstrauens	282
5.2.2.3.5.3	Weitere Gesichtspunkte	283
5.2.2.3.5.4	Zwischenergebnis	284

5.2.2.3.5	Unzulässige Werbung mit einer „veralteten“ Zertifizierung	284
5.2.2.3.6	Täuschung über eine Auszeichnung	286
5.2.2.3.7	Verheimlichen wesentlicher Informationen	287
5.2.2.3.8	Keine Vertrauensausnutzung	288
5.2.2.3.9	Zwischenergebnis zur lauterkeitsrechtlichen Bedeutung	289
5.3	Zusammenfassung der Schwächen der nichtdynamischen Zertifizierung	290
5.3.1	Fehlende Dynamik auf einem höchst dynamischen Gebiet	291
5.3.2	Die sogenannte „Erwartungslücke“	294
5.3.3	Rechtspolitisch verbesserungswürdiges Vertrauenssubstitut	296
6	Dynamik	297
6.1	Begriff der Dynamik	299
6.2	Bedeutung der Dynamik	299
6.3	Dynamik und Recht im Allgemeinen	302
6.4	Relevante Grundrechte und Verfassungsprinzipien im Besonderen	303
6.4.1	Recht auf informationelle Selbstbestimmung und auf Datenschutz	303
6.4.2	Wirtschaftsgrundrechte der Beteiligten	304
6.4.3	Rechtsstaatsprinzip	305
6.5	Dynamik im Datenschutzrecht	307
6.6	Dynamik und Lauterkeitsrecht	308
6.7	Chancen und Risiken der Dynamik	309
6.7.1	Chancen der Dynamik	309
6.7.1.1	Chancen für den Cloud-Kunden	310
6.7.1.2	Chancen für den Cloud-Anbieter	312
6.7.1.3	Chancen für den weiteren Auftragsverarbeiter	313
6.7.1.4	Chancen für betroffene Personen	314
6.7.1.5	Chancen für die Prüfer	314
6.7.1.6	Chancen für die Aufsichtsbehörde	315

6.7.2 Auszugleichende Risiken	316
6.7.2.1 Allgemeine Risiken für die Rechtssicherheit	317
6.7.2.2 Risiken für den Cloud-Anbieter	318
6.7.2.3 Risiken für die betroffenen Personen	319
6.7.2.4 Risiken für die Zertifizierer und Auditoren	320
6.7.2.5 Risiken für die Aufsichtsbehörde	321
6.8 Grenzen der dynamischen Zertifizierung	321
6.9 Struktur des dynamischen Zertifizierungsverfahrens	323
7 Rechtsverträgliche Technikgestaltung	326
7.1 Verfassungsrechtliche Vorgaben	328
7.2 Rechtliche Anforderungen	329
7.3 Rechtliche Kriterien	337
7.3.1 Rechtliche Kriterien für den Betrieb eines Cloud-Dienstes	338
7.3.2 Rechtliche Kriterien an einen Zertifizierungsdienst	371
7.3.3 Rechtliche Kriterien für einen dynamischen Zertifizierungsdienst	390
7.4 Technische Gestaltungsziele	398
7.4.1 Allgemeine Prinzipien für die Technikgestaltung	399
7.4.2 Zwingende Ziele zur Sicherheit eines Cloud-Dienstes	401
7.4.3 Technische Ziele zur Effizienz- und Qualitätssteigerung	425
7.4.4 Technische Ziele zur Organisation eines Cloud-Dienstes	431
7.4.5 Technische Ziele für die Funktionalität eines dynamischen Zertifizierungsdienstes	442
7.4.6 Technische Ziele für die Sicherheit des dynamischen Zertifizierungsdienstes	444
7.4.7 Technische Ziele für die Transparenz eines dynamischen Zertifizierungsdienstes	449
8 Technikadäquate Rechtsfortbildung	452
8.1 Regelungsbedürfnis bei der Zertifizierung	453
8.2 Zuständigkeit	456
8.2.1 Unionsgesetzgeber	457
8.2.2 Europäische Kommission	458
8.2.2.1 Delegierte Rechtsakte	459
8.2.2.1.1 Dynamik der Kriterienkataloge	459
8.2.2.1.2 Begriffsdefinitionen und Abgrenzungen	461

8.2.2.1.3 Voraussetzungen der Zertifizierung von Drittstaatenanbietern	461
8.2.2.2 Durchführungsrechtsakte	461
8.2.2.3 Standardvertragsklauseln	462
8.2.3 Europäischer Datenschutzausschuss	463
8.2.4 Nationaler Gesetzgeber	464
8.2.4.1 Rollentrennung innerhalb der Aufsichtsbehörde	464
8.2.4.2 Nebeneinander öffentlicher und privater Stellen	466
8.2.4.3 Überprüfung-, Widerruf- und Erteilungsverfahren	466
8.2.5 Zuständige Aufsichtsbehörde	467
8.3 Zusammenfassung der Rechtsgestaltung	468
9 Schlussbetrachtungen	469
Literatur	473