

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>1</b>
1.1	Gegenstand der Untersuchung	4
1.2	Gang der Untersuchung	8
<b>2</b>	<b>Persönlichkeitsrechte</b>	<b>11</b>
2.1	Persönlichkeit – ihre Bedeutung und ihr Bezug auf das Rechtswesen	11
2.1.1	Bedeutung der Persönlichkeit	11
2.1.2	Grundlegende Regelungen der Persönlichkeitsrechte	12
2.1.2.1	Ausgangspunkt der Persönlichkeitsrechte – Menschenrechte	14
2.1.2.2	Inhalt der Persönlichkeitsrechte	15
2.1.2.3	Zweck und Gegenstand der Persönlichkeitsrechte	16
2.1.2.4	Träger der Persönlichkeitsrechte	17
2.1.2.5	Rechtsnatur der Persönlichkeitsrechte	18
2.1.3	Zivilrechtlicher Persönlichkeitsschutz	18
2.1.3.1	Zivilrechtlicher Persönlichkeitsschutz in der EU	19
2.1.3.2	Zivilrechtlicher Persönlichkeitsschutz in den USA	20

2.1.3.3	Vergleich der zivilrechtlichen Persönlichkeitsschutz in der EU und in den USA .....	22
2.2	Besondere Ausprägung der Persönlichkeitsrechte .....	23
2.2.1	Das Recht auf Privatsphäre .....	23
2.2.1.1	Recht auf Privatsphäre in der EU .....	25
2.2.1.2	Das Recht auf Privatsphäre / „the right to be left alone“ in den USA .....	26
2.2.1.3	Vergleich des Rechts auf Privatsphäre in der EU und in den USA .....	27
2.2.2	Recht auf Datenschutz / „Data Privacy“ bzw. „Data Protection“ .....	28
2.2.2.1	Recht auf Datenschutz in der EU .....	30
2.2.2.2	Recht auf Datenschutz in den USA .....	31
2.2.2.3	Vergleich des Rechts auf Datenschutz und in der EU und in den USA .....	32
2.2.3	Das Recht auf (informationelle) Selbstbestimmung .....	33
2.2.3.1	Das Recht auf informationelle Selbstbestimmung in der EU .....	34
2.2.3.2	Das Recht auf informationeller Selbstbestimmung in den USA .....	35
2.3	Die Zusammenfassung der Persönlichkeitsrechte .....	36
<b>3</b>	<b>(Internationaler) Datentransfer .....</b>	<b>39</b>
3.1	Datentransfer – historische Entwicklung und heutige Ausprägung .....	39
3.2	Internationaler Datentransfer .....	41
3.2.1	Internationaler Datentransfer – ihre Relevanz und ihr Bezug auf das Rechtswesen .....	41
3.2.2	Internationaler Datentransfer – ihr Verhältnis mit den Persönlichkeitsrechten .....	44
3.3	Begrifflichkeiten und Eingrenzung des Untersuchungsgegenstands .....	47
3.3.1	Daten und Informationen .....	48
3.3.1.1	Bedeutung von Daten und Informationen .....	48
3.3.1.2	Arten von Daten .....	48
3.3.1.2.1	Personenbezogene Daten .....	48
3.3.1.2.2	Pseudonymisierte Daten .....	49
3.3.1.2.3	Nicht-personenbezogene Daten .....	49

3.3.2	Detaillierte Beschreibung des Untersuchungsgegenstands .....	51
3.3.2.1	Bedeutung von Datentransfer .....	51
3.3.2.2	Umfang des Datentransfers .....	52
3.4	Rechtliche Voraussetzungen zum internationalen Datentransfer .....	54
3.4.1	Internationaler Datentransfer aus der EU in die USA ...	54
3.4.1.1	Ziel der DSGVO .....	55
3.4.1.2	Räumliche Anwendung der DSGVO .....	55
3.4.1.3	Sachliche Anwendung der DSGVO .....	56
3.4.1.4	Adressanten der DSGVO .....	56
3.4.1.5	Voraussetzungen nach der DSGVO .....	56
3.4.1.5.1	Datentransfer in ein sicheres Land .....	58
3.4.1.5.2	Prüfung allgemeiner Zulässigkeitsvoraussetzungen für die USA .....	59
3.4.1.5.3	Datentransfer in ein unsicheres Land .....	62
3.4.2	Internationaler Datentransfer aus den USA in die EU ...	68
3.4.2.1	Ziel des CLOUD Act .....	71
3.4.2.2	Räumliche Anwendung des CLOUD Act .....	71
3.4.2.3	Sachliche Anwendung des CLOUD Act .....	72
3.4.2.4	Adressaten des CLOUD Act .....	72
3.4.2.5	Voraussetzungen nach dem CLOUD Act .....	73
3.4.2.5.1	CLOUD Act Vereinbarungen .....	76
3.4.2.5.2	Alternative Wege .....	81
3.4.3	Konflikte zwischen den Datenschutzbestimmungen der EU und der USA .....	81
3.4.3.1	Entstehung des CLOUD Act .....	82
3.4.3.2	Problematik .....	83
3.4.4	Internationale Bemühungen .....	86
3.4.4.1	MLAT-Verfahren .....	87
3.4.4.1.1	MLAT-Verfahren in der EU .....	91
3.4.4.1.2	MLAT-Verfahren in den USA .....	92
3.4.4.1.3	Abgrenzung zwischen MLAT-Abkommen und CLOUD Act .....	93
3.4.4.2	Die neue EU-US Data Privacy Framework ....	94

3.4.4.3	Weitere internationale Bemühungen .....	102
3.4.5	Digitaler Datentransfer bei gleichzeitigem Zusammenspiel von EU- und US-Vorschriften .....	104
3.4.5.1	Lösung I: Rechtliche Schritte .....	106
3.4.5.1.1	Einheitliches MLAT-Abkommen und einfaches MLAT-Verfahren .....	106
3.4.5.1.2	„Verhandlung ähnlicher Beschränkungen“ .....	108
3.4.5.1.3	Melde- und Konsultationspflicht ....	109
3.4.5.2	Lösung II: Organisatorische Gestaltung einer Organisation .....	109
3.4.5.2.1	Duplizierte hierarchische Trennung und Segmentierung .....	109
3.4.5.2.2	Umgang mit dem Dienstleister ....	111
3.4.5.3	Lösung III: Technische Gestaltung der Organisation .....	111
3.4.5.3.1	Verwaltung des Verschlüsselungsschlüssels .....	112
3.4.5.3.2	Zugang und Segmentierung .....	112
3.4.5.4	Lösung IV: Praktische Schritte .....	113
3.5	Die Zusammenfassung des (internationalen) Datentransfers ....	114
<b>4</b>	<b>Präventive Maßnahmen</b> .....	119
4.1	Präventive Maßnahmen – Platzierung und Relevanz .....	119
4.1.1	Einführung .....	119
4.1.2	Primäre Schutzziele der Informationssicherheit .....	123
4.1.2.1	Vertraulichkeit .....	123
4.1.2.2	Integrität .....	123
4.1.2.3	Verfügbarkeit .....	124
4.1.2.4	Belastbarkeit .....	125
4.1.3	Weitere Eigenschaften bzw. Schutzziele der Informationssicherheit .....	125
4.1.3.1	Authentizität / „Authenticity“ und Authentifizierung / „Authentication“ .....	125
4.1.3.2	Nichtabstreitbarkeit / „Non-Repudiation“ und Verbindlichkeit .....	126
4.1.3.3	Verlässlichkeit / „Reliability“ .....	127

4.1.3.4	Zurechenbarkeit / „Accountability“ .....	127
4.2	Risiko-Beurteilung .....	128
4.2.1	Internationaler Standard .....	128
4.2.2	Risiko-Beurteilung des rechtmäßigen Zugangs durch ausländische Behörden .....	129
4.2.3	Risiko-Beurteilung nach dem EU-Datenschutzrecht .....	133
4.2.4	Risiko-Beurteilung nach dem US-Datenschutzrecht .....	137
4.2.5	Vergleich der Risiko-Beurteilung in der EU und in den USA .....	140
4.3	Präventive rechtliche Maßnahmen .....	141
4.3.1	Präventive rechtliche Maßnahmen nach dem europäischen Recht .....	141
4.3.1.1	Privacy by Design und Privacy by Default .....	143
4.3.1.2	Sicherheit der Verarbeitung nach EU-Vorschriften .....	145
4.3.1.3	Mindestanforderungen nach EU-Vorschriften .....	147
4.3.1.3.1	Pseudonymisierung: Art. 32 Abs. 1 lit. a) DSGVO .....	147
4.3.1.3.2	Verschlüsselung: Art. 32 Abs. 1 lit. a) DSGVO .....	148
4.3.1.3.3	Verfügbarkeit / Backup: Art. 32 Abs. 1 lit. c) DSGVO .....	149
4.3.1.3.4	Gewährleistung der Sicherheit der Verarbeitung: Art. 32 Abs. 1 lit. d) DSGVO .....	149
4.3.1.3.5	Genehmigte Verhaltensregeln: Art. 32 Abs. 3 DSGVO .....	150
4.3.1.3.6	Genehmigte Zertifizierungen: Art. 32 Abs. 3 DSGVO .....	150
4.3.1.3.7	Mitarbeiteranweisungen: Art. 32 Abs. 4 DSGVO .....	152
4.3.2	Präventive rechtliche Maßnahmen nach dem amerikanischen Recht .....	153
4.3.2.1	Privacy by Design, Privacy by Default .....	154
4.3.2.2	Sicherheit der Verarbeitung nach US-Vorschriften .....	156
4.3.2.3	Mindestanforderungen nach US-Vorschriften .....	157

4.3.2.3.1	Pseudonymisierung: 1798.140 (aa) CPRA .....	157
4.3.2.3.2	Verschlüsselung: CLOUD Act / SCA, CCPA / CPRA .....	157
4.3.2.3.3	Verfügbarkeit / Backup: Abschn. 103 (a) (1), § 2713 CLOUD Act / 18 U.S.C. § 2704 (a) (1)-(3) SCA .....	157
4.3.2.3.4	Gewährleistung der Sicherheit der Verarbeitung: 1798.140 (j) (1) (C) CPRA .....	158
4.3.2.3.5	Verhaltensregeln: CLOUD Act / SCA, CCPA / CPRA .....	159
4.3.2.3.6	Genehmigte Zertifizierungen: 1798.140 (j) (1) (A) und (B) CPRA .....	159
4.3.2.3.7	Mitarbeiteranweisungen: CLOUD Act, CCPA .....	160
4.3.3	Vergleich der präventiven rechtlichen Maßnahmen .....	160
4.4	Präventive normative Maßnahmen .....	161
4.4.1	Organisatorische Maßnahmen / „Organizational Controls“ .....	162
4.4.1.1	Erkenntnisse zur Bedrohungslage .....	162
4.4.1.2	Übertragung oder Transport von Informationen .....	162
4.4.1.3	Zugangssteuerung .....	163
4.4.1.4	Informationssicherheit bei der Verwendung von Cloud-Diensten .....	164
4.4.2	Personenbezogene Maßnahmen / „People Controls“ .....	164
4.4.2.1	Sensibilisierung, Ausbildung und Schulung für Informationssicherheit .....	164
4.4.2.2	Disziplinarverfahren .....	165
4.4.3	Technische Maßnahmen / „Technological Controls“ .....	166
4.4.3.1	Einschränkung des Zugangs zu Informationen .....	166
4.4.3.2	Konfigurationsmanagement .....	167
4.4.3.3	Vermeidung von Datenabfluss .....	168
4.4.3.4	Datensicherung / „Backup“ .....	169

4.4.3.5	Einsatz von Kryptographie / Verschlüsselung .....	170
4.4.4	Die PDCA-Methodik: Plan-Do-Check-Act .....	174
4.4.4.1	Plan / Planung .....	175
4.4.4.2	Do / Umsetzung .....	175
4.4.4.3	Check / Überprüfung .....	175
4.4.4.4	Act / Verbesserung .....	176
4.5	Zusammenfassung der präventiven Maßnahmen .....	176
<b>5</b>	<b>Nachgelagerte Maßnahmen .....</b>	<b>181</b>
5.1	Cyber-Bedrohungen – gefährlicher denn je .....	181
5.1.1	Einführung und Relevanz .....	181
5.1.2	Gefährdungen der Informationssicherheit .....	184
5.1.3	Cyber-Attacken .....	186
5.2	Incident Response .....	190
5.2.1	Incident Response Team .....	191
5.2.2	Incident Response Plan .....	195
5.3	Incident Response Steps .....	197
5.3.1	Erfassung und Bewertung des Angriffs / „Identification“ .....	197
5.3.1.1	Datenschutzverletzung .....	198
5.3.1.2	Informationssicherheitsvorfall .....	200
5.3.2	Schadensbegrenzung / „Minimization“ und -beseitigung .....	201
5.3.3	Dokumentation .....	202
5.3.4	Benachrichtigung bzw. Meldung / „Notification“ .....	202
5.3.4.1	Notification nach dem europäischen Recht .....	204
5.3.4.2	Notification nach dem amerikanischen Recht .....	205
5.3.5	Beweissicherung .....	208
5.3.6	Analyse der Ursachen und möglicher Maßnahmen / „Lessons learned“ .....	209
5.3.7	Rückkehr zum Normalbetrieb / „Remediation“ .....	210
5.4	Zusammenfassung der nachgelagerten Maßnahmen .....	212
<b>6</b>	<b>Das Ergebnis .....</b>	<b>215</b>
	<b>Literaturverzeichnis .....</b>	<b>221</b>