

Inhaltsverzeichnis

ABKÜRZUNGSVERZEICHNISXVII

1 EINFÜHRUNG 1

1.1 MOTIVATION 1

1.2 GEGENSTAND DER DISSERTATION.. ... 2

1.2.1 Allgemeine Fragen des Beschäftigtendatenschutzes 2

1.2.2 Anforderungen an Screenings im Beschäftigungsverhältnis auf Basis der Anomalieerkennung 3

1.3 ZIEL DER ARBEIT UND GANG DER DARSTELLUNG 4

2 BEDEUTUNG VON COMPLIANCE IM UNTERNEHMEN 6

2.1 BEGRIFF..... 6

2.2 DAS PROBLEM VON STRAFTATERN IM BETRIEB 9

2.2.1 Innentäter in Unternehmen. 9

2.2.2 Empirische Befunde zur Täterstruktur im betrieblichen Bereich 10

2.2.3 Empirische Erklärungsversuche 12

2.2.4 Zwischenergebnis. 15

2.3 DIE VERPFLICHTUNG DES ARBEITGEBERS ZU COMPLIANCE..... 15

2.3.1 Praktisches Bedürfnis nach Compliance. 15

2.3.2 Rechtliche Verpflichtung zur Einrichtung einer Compliance-Organisation. 17

2.3.2.1 Spezialgesetzliche Regelungen 17

2.3.2.2 Allgemeine Pflicht zu Compliance jenseits spezialgesetzlicher Normen? 20

2.3.2.3 Compliance in der Rechtsprechung 21

2.3.2.3.1 Siemens/Enel, BGH, Urt v 29 8 2008 – 2 StR 587/07 21

2.3.2.3.2 Berliner Stadtwerke, BGH, Urt v 17 7 2009 – 5 StR 394/08 22

2.3.2.3.3 Mobbing-Entscheidung, BGH, Urt. v 20.10 2011 – 4 StR 71/11 22

2.3.2.3.4 Siemens/Neuburger, LG München I, Urt v 10 12 2013 - 5 HK O 1387/10. 23

2.3.3 Compliance-Management-Systeme 24

2.3.4 Mitarbeiterüberwachung als Element effektiver Compliance im Unternehmen..... 25

3 SCREENINGS AUF BASIS DER ANOMALIEERKENNUNG 28

3.1 DER BEGRIFF DES „SCREENINGS“ 28

3.2 PRAKTISCHE NOTWENDIGKEIT UND ABLAUF 29

3.3 GRUNDSÄTZLICHE ANERKENNUNG VON SCREENINGS DURCH GESETZ UND RECHTSPRECHUNG 30

3.4 TECHNISCHE VERFAHREN... .. 32

3.4.1 In der Regel datenschutzneutrale Methoden 32

3.4.2 Datenabgleiche 33

3.4.3 Anomalieerkennungsverfahren in SIEM-Systemen..... 33

3.4.3.1 Anomalie 34

3.4.3.1.1 Begriff.. ... 34

3.4.3.1.2 Arten 35

3.4.3.1.2.1 Punktanomalie. 35

3.4.3.1.2.2 Kontext-Anomalie 35

3.4.3.1.2.3 Kollektive Anomalien 36

3.4.3.2 Verfahren des maschinellen Lernens 36

3.4.3.2.1 Überwachtes Lernen 37

3.4.3.2.2 Halb überwachtes Lernen 37

3.4.3.2.3 Unüberwachtes Lernen 37

3.4.3.3 Praktische und technische Herausforderungen der Anomalieerkennung 38

4 RECHTLICHER RAHMEN FÜR MAßNAHMEN DER MITARBEITERÜBERWACHUNG IM RAHMEN
UNTERNEHMERISCHER COMPLIANCE AUF EBENE DER GRUNDRECHTE SOWIE DER EMRK 40

4.1 EMRK... 41

4.1.1 Bindungswirkung und Einfluss der EMRK auf das Unionsrecht und auf das nationale Recht. 41

4.1.2 Drittwirkung 42

4.1.3 Art 8 EMRK 42

4.1.4 Eigentumsschutz im Konventionsrecht..... 44

4.2	DIE GRUNDRECHTE DER GRUNDRECHTECHARTA (GRCH) DER EUROPÄISCHEN UNION	45
4.2.1	Grundrechte des Unionsrechts oder deutsche Grundrechte?	45
4.2.1.1	Rechtsprechung des BVerfG	46
4.2.1.2	Rechtsprechung des EuGH	48
4.2.1.3	Zwischenergebnis	50
4.2.2	Drittwirkung	51
4.2.3	Art. 8, 7 GRCh	52
4.2.4	Unternehmerische Freiheit und Eigentumsschutz	53
4.3	ART 16 AEUV	54
4.4	DIE GRUNDRECHTE DES GRUNDGESETZES	54
4.4.1	Drittwirkung	54
4.4.2	Das allgemeine Persönlichkeitsrecht	55
4.4.3	Das Recht auf informationelle Selbstbestimmung	55
4.4.4	Das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme 57	
4.4.5	Das Fernmeldegeheimnis	58
4.4.6	Informationsfreiheit	58
4.4.7	Eigentum und unternehmerische Betätigungsfreiheit	59
5	REGELUNG DES BESCHÄFTIGTENDATENSCHUTZES NACH DER DSGVO	60
5.1	ABRISS ÜBER DIE GESETZGEBERISCHEN BEMÜHUNGEN IM BESCHÄFTIGUNGSDATENSCHUTZ AUF NATIONALER EBENE	60
5.2	ÖFFNUNGSKLAUSEL DES ART. 88 DSGVO	62
5.2.1	Anwendungsbereich	63
5.2.2	Spezifischere Vorschriften	66
5.2.2.1	Meinungsstand	66
5.2.2.2	Stellungnahme	67
5.2.2.2.1	Wortlaut	67
5.2.2.2.2	Systematik	68
5.2.2.2.3	Entstehungsgeschichte	70
5.2.2.2.4	Teleologische Auslegung	70
5.2.2.2.5	Auslegung unter Berücksichtigung des Primärrechts	71
5.2.2.2.5.1	Meinungsstand	71
5.2.2.2.5.2	Bewertung	73
5.2.2.2.6	Zwischenergebnis	74
5.2.3	Gewährleistung des Schutzes der Rechte und Freiheiten	76
5.2.4	Inhaltliche Vorgaben des Art. 88 Abs. 2 DSGVO	77
5.2.4.1	Regelungspflicht?	77
5.2.4.2	Geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und Grundrechte der betroffenen Person	78
5.2.4.2.1	Maßnahmen	78
5.2.4.2.2	Geeignete und besondere Maßnahmen	79
5.2.4.2.3	Wahrung der menschlichen Würde, der berechtigten Interessen und Grundrechte der betroffenen Person	80
5.2.4.3	Die Beispiele in Art. 88 Abs. 2 DSGVO	82
5.2.4.3.1	Transparenz	82
5.2.4.3.1.1	Formale oder inhaltliche Ausgestaltung als Anknüpfungspunkt?	83
5.2.4.3.1.2	Verdeckte Überwachungsmaßnahmen	83
5.2.4.3.1.2.1	Zulässigkeit	83
5.2.4.3.1.2.2	Regelung durch Kollektivvereinbarung	84
5.2.4.3.1.2.3	Zwischenergebnis	86
5.2.4.3.2	Mitarbeiterüberwachung	86
5.2.5	Mitteilungspflicht (Art. 88 Abs. 3 DSGVO)	87
5.2.6	Verhältnis zu anderen Rechtsvorschriften der DSGVO	87
6	ALLGEMEINE ANFORDERUNGEN DER DSGVO UND DES BDSG AN ANOMALIEBASIERTE SCREENINGS VON MITARBEITERN	89
6.1	DIE GRUNDSÄTZE DES DATENSCHUTZRECHTS	89
6.1.1	Rolle der Grundsätze	89
6.1.2	Der Grundsatz der Rechtmäßigkeit der Verarbeitung	91
6.1.3	Der Grundsatz der Verarbeitung nach Treu und Glauben	93
6.1.4	Der Grundsatz der Transparenz der Verarbeitung	95

6.1.5 Der Grundsatz der Zweckbindung 97

6.1.5.1 Verarbeitung für festgelegte Zwecke 97

6.1.5.2 Eindeutige Zwecke 98

6.1.5.3 Legitime Zwecke 99

6.1.5.4 Bedeutung für die Rechtsgrundlage 100

6.1.5.5 Zweckänderung 100

6.1.5.5.1 Fiktion des Art. 5 Abs. 1 lit. b Hs. 2 DSGVO 101

6.1.5.5.2 Vereinbarkeitsprüfung 102

6.1.5.5.2.1 Einwilligung 102

6.1.5.5.2.2 Nationale Erlaubnistatbestände zur zweckändernden Weiterverarbeitung 102

6.1.5.5.2.3 Die Kriterien des Art. 6 Abs. 4 DSGVO 104

6.1.5.5.2.3.1 Verbindung zwischen den Zwecken 104

6.1.5.5.2.3.2 Zusammenhang 104

6.1.5.5.2.3.3 Art der Daten 105

6.1.5.5.2.3.4 Folgen für betroffene Personen 105

6.1.5.5.2.3.5 Geeignete Garantien 105

6.1.6 Der Grundsatz der Datenminimierung, Art. 5 Abs. 1 lit. c DSGVO 105

6.1.6.1 Dem Zweck angemessen und erheblich 106

6.1.6.2 Auf das notwendige Maß begrenzt 107

6.1.6.3 Zusammenspiel mit Art. 25 DSGVO 108

6.1.7 Der Grundsatz der Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO) 108

6.1.8 Grundsatz der Integrität und Vertraulichkeit gemäß Art. 5 Abs. 1 lit. f DSGVO 109

6.1.9 Zwischenergebnis 110

6.2 RECHTSGRUNDLAGEN FÜR SCREENINGS AUF BASIS DER ANOMALIEERKENNUNG IM BESCHÄFTIGUNGSVERHÄLTNIS 113

6.2.1 Einwilligung 113

6.2.1.1 Anwendbarkeit des § 26 Abs. 2 BDSG auf Compliance-Sachverhalte? 113

6.2.1.2 Anforderungen 114

6.2.1.2.1 Einwilligung der betroffenen Person 114

6.2.1.2.2 Freiwillige Abgabe 115

6.2.1.2.2.1 Abhängigkeitsverhältnis 116

6.2.1.2.2.2 Überrumpelung 120

6.2.1.2.2.3 Androhen von Nachteilen oder Versprechen hoher Vorteile 120

6.2.1.2.2.4 Kopplungsverbot 120

6.2.1.2.3 Abgabe für den bestimmten Fall 122

6.2.1.2.4 Informierte Einwilligung 122

6.2.1.2.5 Form 124

6.2.1.2.5.1 Zulässige Abweichung von den Regelungen der DSGVO 125

6.2.1.2.5.2 Die Begriffe der Schriftform und der elektronischen Form 126

6.2.1.2.6 Verarbeitung besonderer Kategorien personenbezogener Daten 127

6.2.1.2.7 Unmissverständlich 127

6.2.1.2.8 Jederzeitige Widerruflichkeit 128

6.2.1.2.8.1 Form 128

6.2.1.2.8.2 Begründung 128

6.2.1.2.8.3 Wirkung 129

6.2.1.3 Regelung der Einwilligung durch Kollektivvereinbarung 129

6.2.1.4 AGB 130

6.2.1.5 Rückgriff auf andere Rechtsgrundlagen? 131

6.2.1.6 Praktische Untauglichkeit 132

6.2.2 Kollektivvereinbarungen 133

6.2.2.1 Betriebsvereinbarungen als taugliche Rechtsgrundlage 133

6.2.2.2 Tarifvertrag 135

6.2.2.3 Inhaltliche Anforderungen 136

6.2.3 Zulässigkeit von Screenings nach § 26 Abs. 1 BDSG 137

6.2.3.1 Vereinbarkeit des § 26 Abs. 1 BDSG mit Art. 88 DSGVO 138

6.2.3.1.1 Meinungsstand zur Unionsrechtskonformität des § 26 Abs. 1 BDSG 138

6.2.3.1.2 Unionsrechtskonformität des § 26 BDSG 140

6.2.3.2 Europarechtskonforme Erweiterung des sachlichen Anwendungsbereichs 141

6.2.3.3 Das Verhältnis der beiden Sätze des § 26 Abs. 1 BDSG zueinander 143

6.2.3.3.1 Präventive Maßnahmen 144

6.2.3.3.2 Abgrenzungsschwierigkeiten insbesondere bei Screenings von Beschäftigtendaten 147

6.2.3.3.3 Rechtsprechung zu Terrorlistenscreenings 149

6.2.3.3.4 Versuch der Einordnung von Anomalieerkennung 151

6.2.3.3.5 Rechtsgrundlage zur Aufdeckung von Pflichtverletzungen 152

6.2.3.3.6 Weniger eingriffsintensive Maßnahmen 154

6.2.3.3.7	Maßnahmen gegenüber unverdächtigen Beschäftigten	155
6.2.3.4	Verhältnis zu Art. 6 DSGVO.....	155
6.2.3.5	Verhältnis zu Art. 10 DSGVO.....	156
6.2.3.6	Erforderlich.....	158
6.2.3.6.1	Legitimes Ziel.....	159
6.2.3.6.2	Geeignetheit.....	160
6.2.3.6.3	Erforderlichkeit.....	160
6.2.3.6.4	Interessenabwägung.....	161
6.2.3.7	Repressive Maßnahmen der Aufdeckung von Straftaten.....	162
6.2.3.7.1	Verdacht.....	163
6.2.3.7.2	Im Beschäftigungsverhältnis begangene Straftat.....	163
6.2.3.7.3	Zur Aufdeckung von Straftaten	163
6.2.3.7.4	Dokumentationspflicht	163
6.2.3.8	Aspekte der Interessenabwägung des § 26 Abs. 1 BDSG und Gestaltungsvorschläge	164
6.2.3.8.1	Keine anlasslose Dauerüberwachung.....	164
6.2.3.8.2	Nur ausnahmsweise heimliche Überwachung	167
6.2.3.8.3	Anzahl der überwachten Personen und Streubreite	167
6.2.3.8.4	Räumliche und zeitliche Begrenzung	168
6.2.3.8.5	Art der Daten.....	168
6.2.3.8.6	Dauer.....	169
6.2.3.8.7	Art der Durchführung.....	169
6.2.3.8.8	Zahl der an dem Eingriff beteiligten Personen	169
6.2.3.8.9	Drohende Nachteile	170
6.2.3.8.10	Unterscheidung zwischen Treffern und Nicht-Treffern sowie Bedeutung der Veranlassung	170
6.2.3.8.11	Fazit.....	172
6.2.4	Videüberwachung im Kontext von Screenings	174
6.2.4.1	Die Rechtsprechung des EGMR zur Videüberwachung	175
6.2.4.1.1	Rs. Kopke/Deutschland	175
6.2.4.1.2	Rs. Bărbulescu/Rumänien	177
6.2.4.1.2.1	Entscheidung.....	177
6.2.4.1.2.2	Die Bedeutung der Unterrichtungspflicht	179
6.2.4.1.3	Rs. Antović und Mirković/Montenegro	179
6.2.4.1.4	Rs. Lopez Ribalda.....	180
6.2.4.1.4.1	Die Entscheidung der 3. Kammer des EGMR, Urt. v. 9.1.2018 - 1874/13, 8567/13	181
6.2.4.1.4.2	Die Entscheidung der Großen Kammer des EGMR vom 17.10.2019 – 1874/13, 8567/13	183
6.2.4.1.4.3	Zwischenergebnis.....	186
6.2.4.1.5	Konsequenzen der Rechtsprechung des EGMR.....	187
6.2.4.2	Die Zulässigkeit der Videüberwachung im Beschäftigungsverhältnis.....	189
6.2.4.2.1	§ 4 BDSG als Rechtsgrundlage für die offene Videüberwachung im öffentlichen Bereich auch im Beschäftigungsverhältnis?.....	189
6.2.4.2.2	Ausschließliche Anwendbarkeit des § 26 BDSG?	190
6.2.4.2.3	Die Zulässigkeit präventiver Videüberwachung	192
6.2.4.2.4	Rechtmäßigkeitsgrundsätze	192
6.2.5	Sensible Daten	196
6.2.5.1	Unionsrechtskonformität des § 26 Abs. 3 BDSG.....	197
6.2.5.2	Verarbeitungszwecke	197
6.2.6	Verarbeitung der Daten Dritter	201
6.3	BETROFFENENRECHTE	201
6.3.1	Art. 12 DSGVO	201
6.3.2	Die Informationspflichten nach Art. 13, 14 DSGVO	202
6.3.2.1	Informationspflichten bei Erhebung personenbezogener Daten bei der betroffenen Person nach Art. 13 DSGVO	203
6.3.2.1.1	Erhebung bei der betroffenen Person.....	204
6.3.2.1.1.1	Keine Kenntnis oder Mitwirkung nach teilweise vertretener Ansicht erforderlich	204
6.3.2.1.1.2	Kenntnis oder Mitwirkungshandlung erforderlich	205
6.3.2.1.1.3	Zwischenergebnis.....	208
6.3.2.1.2	Zweckänderung	209
6.3.2.1.3	Ausnahmen	211
6.3.2.1.4	Beschränkungen durch Kollektivvereinbarungen auf der Grundlage von Art. 88 DSGVO?	212
6.3.2.2	Datenerhebung nach Art. 14 DSGVO.....	213
6.3.2.2.1	Informationspflichten	213
6.3.2.2.2	Ausnahmetatbestände des Art. 14 Abs. 5 DSGVO	214
6.3.2.2.3	Geheimhaltungspflicht nach § 29 Abs. 1 S. 1 BDSG.....	215
6.3.2.2.4	Ausnahmetatbestände des § 33 Abs. 1 BDSG	216

6.3.3 *Recht auf Auskunft (Art. 15 DSGVO)* 217

6.3.4 *Recht auf Berichtigung (Art. 16 DSGVO)* 218

6.3.5 *Recht auf Löschung (Art. 17 DSGVO)*..... 219

 6.3.5.1 *Loschpflichten nach Art. 17 Abs. 1 DSGVO*..... 219

 6.3.5.1.1 *Loschungstatbestände* 219

 6.3.5.1.1.1 *Zweckfortfall, Art. 17 Abs. 1 lit. a DSGVO*..... 220

 6.3.5.1.1.2 *Widerruf der Einwilligung, Art. 17 Abs. 1 lit. b DSGVO*..... 220

 6.3.5.1.1.3 *Unrechtmäßige Verarbeitung, Art. 17 Abs. 1 lit. d DSGVO*..... 221

 6.3.5.1.2 *Ausnahmetatbestände*..... 221

 6.3.5.1.2.1 *Erfüllung einer Rechtspflicht oder öffentlicher Aufgaben (Art. 17 Abs. 3 lit. b DSGVO)* 221

 6.3.5.1.2.2 *Rechtsansprüche (Art. 17 Abs. 3 lit. e DSGVO)*..... 221

 6.3.5.1.3 *Die Löschung* 222

 6.3.5.1.4 *Unverzüglich*..... 224

 6.3.5.1.5 *Praktische Umsetzung durch Löschkonzepte* 225

 6.3.5.1.6 *Umsetzung durch Black Box* 226

 6.3.6 *Widerspruchsrecht, Art. 21 DSGVO* 226

6.4 *PRIVACY BY DESIGN AND BY DEFAULT (ART. 25 DSGVO)* 227

 6.4.1 *Datenschutz durch Technikgestaltung (Art. 25 Abs. 1 DSGVO)*..... 228

 6.4.1.1 *Schutzgut*..... 229

 6.4.1.2 *Der Risikobegriff* 229

 6.4.1.3 *Risikoanalyse*..... 229

 6.4.1.3.1 *Risikoidentifikation*..... 230

 6.4.1.3.1.1 *Art, Umfang, Umstände und Zwecke der Verarbeitung* 230

 6.4.1.3.1.2 *Risikoszenarien*..... 231

 6.4.1.3.1.3 *Bestimmung der Schwere möglicher Schäden* 232

 6.4.1.3.1.4 *Eintrittswahrscheinlichkeit*.. 234

 6.4.1.3.2 *Risikobewertung* 234

 6.4.1.4 *Stand der Technik*..... 235

 6.4.1.5 *Implementierungskosten* 236

 6.4.1.6 *Technische und organisatorische Maßnahmen*..... 236

 6.4.2 *Privacy by Default (Art. 25 Abs. 2 DSGVO)* 238

 6.4.3 *Zertifizierungsverfahren als Nachweis (Art. 25 Abs. 3 DSGVO)* 239

6.5 *VERZEICHNIS VON VERARBEITUNGSTATIGKEITEN (ART. 30 DSGVO)* 239

6.6 *SICHERHEIT DER VERARBEITUNG (ART. 32 DSGVO)* 240

 6.6.1 *Das Verhältnis von Datenschutz und Sicherheit der Verarbeitung*..... 241

 6.6.2 *Abgrenzung zu Art. 25 DSGVO* 241

 6.6.3 *Die Anforderungen an die Datensicherheit nach Art. 32 DSGVO* 242

 6.6.3.1 *Dem Risiko angemessenes Schutzniveau* 242

 6.6.3.2 *Maßnahmen* 243

 6.6.3.3 *Praktische Umsetzung* 244

6.7 *DATENSCHUTZ-FOLGENABSCHÄTZUNG, ART. 35-DSGVO* 245

 6.7.1 *Erforderlichkeit einer Datenschutz-Folgenabschätzung*..... 247

 6.7.1.1 *Neue Technologien*..... 247

 6.7.1.2 *Hohes Risiko* 248

 6.7.1.2.1.1 *Risikoanalyse*.. 248

 6.7.1.2.1.2 *Fälle zwingender Datenschutz-Folgenabschätzung (Art. 35 Abs. 3 DSGVO)* . 250

 6.7.1.2.1.2.1 *Automatisierte, systematische und umfassende Bewertung persönlicher Aspekte*..... 250

 6.7.1.2.1.2.2 *Umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten* 251

 6.7.1.2.1.2.3 *Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche* 252

 6.7.1.3 *Positiv- und Negativlisten der Aufsichtsbehörden* 253

 6.7.2 *Inhaltliche Anforderungen*..... 253

 6.7.3 *Beteiligung der betroffenen Personen*..... 254

6.8 *BETEILIGUNG DES DATENSCHUTZBEAUFTRAGTEN* 255

 6.8.1 *Benennung eines Datenschutzbeauftragten* 255

 6.8.1.1 *Pflicht zur Benennung auf der Grundlage von Art. 37 Abs. 1 lit. a DSGVO*..... 256

 6.8.1.2 *Pflicht zur Benennung auf der Grundlage von Art. 37 Abs. 1 lit. b und c DSGVO* 256

 6.8.1.2.1 *Kerntätigkeit*..... 256

 6.8.1.2.1.1 *Meinungsstand zur Verarbeitung von Beschäftigtendaten*..... 257

 6.8.1.2.1.2 *Stellungnahme* 258

 6.8.2 *Bestellpflicht nach § 38 Abs. 1 BDSG* 259

6.9 *AUSSCHLIEßLICH AUTOMATISIERTE VERARBEITUNG*..... 259

 6.9.1 *Ausschließlichkeit* 260

6.9.2	Profiling	262
6.9.3	Kein Erfassen bloßer Zutrittskontrollen	263
6.9.4	Rechtliche Wirkung oder erhebliche Beeinträchtigung	264
6.9.5	Zwischenergebnis	265
6.10	ANONYMISIERUNG UND PSEUDONYMISIERUNG IM BETRIEB	265
6.10.1	Anonymisierung	265
6.10.1.1	Unterscheidung zwischen anonymen und anonymisierten Informationen	265
6.10.1.2	Der Begriff der personenbezogenen Daten	266
6.10.1.2.1	Die Identifizierbarkeit als zentrales Merkmal	266
6.10.1.2.2	Absolutes oder relatives Begriffsverständnis	267
6.10.1.2.2.1	Relative Theorie	268
6.10.1.2.2.2	Absolute Theorie	268
6.10.1.2.2.3	EuGH, Urteil vom 19.10.2016 (Rs. C-582/14 – Breyer/Bundesrepublik Deutschland)	269
6.10.1.2.2.4	Relatives Begriffsverständnis der DSGVO	270
6.10.1.2.2.5	Zwischenergebnis	272
6.10.1.2.3	Arten der Anonymisierung	272
6.10.1.2.4	Abgrenzung zu Pseudonymisierung	273
6.10.2	Pseudonymisierung	274
6.10.2.1.1	Bedeutung der Pseudonymisierung	274
6.10.2.1.2	Pseudonymisierte Daten als personenbezogene Daten	275
6.10.2.1.3	Anforderungen an eine Pseudonymisierung	277
6.10.2.1.3.1	Keine Zuordnung der Daten zu einer bestimmten Person ohne Hinzuziehung zusätzlicher Informationen	278
6.10.2.1.3.2	Gesonderte Aufbewahrung	279
6.10.2.1.3.3	Technische und organisatorische Maßnahmen zur Nichtzuordnung	280
6.10.2.1.3.4	Umsetzung im Unternehmen	281
6.10.2.1.4	Treuhändermodelle und deren rechtliche Bewertung	281
6.10.2.1.4.1	Technische Umsetzung	282
6.10.2.1.4.2	Stellung des Betriebsrats	282
6.10.2.1.4.2.1	Keine eigene Verantwortlichkeit des Betriebs- bzw. Personalrats	282
6.10.2.1.4.2.2	Kontrolle der Beschäftigtenvertretung durch den Datenschutzbeauftragten	285
6.10.2.1.4.2.3	Spannungsverhältnis zwischen Betriebsverfassungsrecht und Datenschutzrecht	287
6.10.2.1.4.2.4	Überwachungsaufgabe	287
6.10.2.1.4.2.5	Verschwiegenheitsverpflichtung der Mitglieder des Betriebsrats	289
6.10.2.1.4.3	Fachabteilungen als Treuhänder	290
6.10.2.1.4.4	Der Datenschutzbeauftragte als Treuhänder	290
6.10.2.1.4.4.1	Unabhängige Stellung	291
6.10.2.1.4.4.1.1	Weisungsfreiheit	291
6.10.2.1.4.4.1.2	Schutz vor Abberufung	291
6.10.2.1.4.4.1.3	Verschwiegenheitsverpflichtung	292
6.10.2.1.4.4.1.4	Zwischenergebnis	293
6.10.2.1.4.4.2	Übernahme und Zuweisung von Aufgaben	293
6.10.2.1.4.4.2.1	Die Zulässigkeit von Prüfaufträgen gegenüber dem Datenschutzbeauftragten	293
6.10.2.1.4.4.2.2	Die Aufnahme entsprechender Klauseln in Kollektivvereinbarungen	297
6.10.2.1.5	Zwischenergebnis	299
6.10.2.1.6	Entschlüsselungsquorum	299
6.10.2.1.7	Offenlegung	299
6.10.2.1.8	Verwahrung	300
6.10.2.1.9	Pseudonymwahl	300
7	BEWEISVERWERTUNG VOR DEN ARBEITSGERICHTEN	301
8	MITBESTIMMUNG DES BETRIEBSRATS	304
8.1	MITBESTIMMUNG NACH § 87 Abs. 1 Nr. 1 BetrVG	304
8.2	MITBESTIMMUNG NACH § 87 Abs. 1 Nr. 6 BetrVG	304
9	FAZIT	306
9.1	BEDEUTUNG VON COMPLIANCE IM UNTERNEHMEN	306
9.2	SCREENINGS AUF BASIS DER ANOMALIEERKENNUNG IN UNTERNEHMEN	307
9.3	RECHTLICHER RAHMEN FÜR SCREENINGS AUF BASIS DER ANOMALIEERKENNUNG IM UNTERNEHMEN AUF EBENE DER GRUNDRECHTE SOWIE DER EMRK	308
9.4	ANFORDERUNGEN DES BESCHAFTIGTENDATENSCHUTZES	308
9.5	ALLGEMEINE ANFORDERUNGEN DER DSGVO UND DES BDSG	309

XVI	Inhaltsverzeichnis
10	EXKURS 314
	LITERATURVERZEICHNIS..... 315