

# Inhaltsverzeichnis

<b>Abbildungsverzeichnis .....</b>	<b>XXIII</b>
<b>Tabellenverzeichnis .....</b>	<b>XXV</b>
<b>Abkürzungsverzeichnis.....</b>	<b>XXVII</b>
<b>Management Summary.....</b>	<b>XXIX</b>
<b>1 Datenschutz und der betriebliche Einsatz der Biometrie .....</b>	<b>1</b>
1.1 Notwendigkeit einer datenschutzrechtlichen Betrachtung des betrieblichen Einsatzes biometrischer Systeme .....	1
1.2 Aufbau der Arbeit .....	2
<b>2 Grundlagen biometrischer Authentifizierungssysteme .....</b>	<b>3</b>
2.1 Biometrie und biometrische Merkmale .....	3
2.2 Technische Grundlagen biometrischer Systeme.....	5
2.2.1 Prinzipien der Authentizitätsprüfung .....	5
2.2.2 Aufbau eines biometrischen Systems.....	9
2.2.3 Ablauf einer biometrischen Authentifizierung.....	12
2.2.4 Adaptive biometrische Verfahren .....	15
2.2.5 Betriebsarten biometrischer Systeme .....	16
2.2.5.1 Betrieb im Verifikationsmodus .....	16
2.2.5.2 Betrieb im Identifikationsmodus .....	18
2.3 Sicherheit biometrischer Systeme.....	20
2.3.1 Sicherheit durch biometrische Systeme .....	20
2.3.2 Erhöhte Sicherheitsnotwendigkeit beim Systemeinsatz.....	21
2.3.3 Fehlerraten als Gütemaße für die Erkennungsleistung biometrischer Verfahren und Systeme .....	22
2.3.3.1 Grundlegendes zur Ermittlung von Fehlerraten .....	23
2.3.3.2 False Accept Rate (FAR).....	23
2.3.3.3 False Rejection Rate (FRR).....	24
2.3.3.4 Equal Error Rate (EER).....	25

2.3.3.5	Detection Error Trade-off (DET)- und Receiver Operating Characteristic (ROC)-Kurve.....	28
2.3.3.6	Failure to Enrol Rate (FTE).....	30
2.3.3.7	Failure to Acquire Rate (FTA) .....	31
2.3.3.8	False Match Rate (FMR) und False Non-Match Rate (FNMR) vs. FAR und FRR .....	32
2.3.4	Statistische Signifikanz der Fehlerraten .....	34
2.3.5	Versuchsdesign für die Ermittlung der Fehlerraten .....	44
<b>3</b>	<b>Biometrische Systeme auf der Basis des Merkmals Tippverhalten.....</b>	<b>49</b>
3.1	Tippverhalten als biometrisches Merkmal.....	49
3.2	Biometrische Verfahren zur Tippverhaltenserkennung.....	53
3.3	Biometrische Systeme auf der Grundlage des Tippverhaltens.....	57
3.3.1	Repräsentative Systemansätze.....	57
3.3.1.1	Textgebundene Authentifizierungssysteme .....	58
3.3.1.2	Textungebundenen Authentifizierungssysteme .....	61
3.3.2	Psylock-Kernsystem als Basisarchitektur für verschiedene Systemansätze.....	63
<b>4</b>	<b>Datenschutzrechtlich relevante Vorschriften und Konzepte .....</b>	<b>65</b>
4.1	Recht auf informationelle Selbstbestimmung.....	66
4.2	Personenbezug biometrischer Daten.....	68
4.3	Grundsätze und Vorschriften aus dem Bundesdatenschutzgesetz als Ausgangspunkte einer Bewertung .....	71
4.3.1	Notwendigkeit einer Rechtsvorschrift oder einer Einwilligung für die Einsatzlegitimation .....	71
4.3.2	Grundsatz der Zweckbindung .....	72
4.3.3	Grundsatz der Erforderlichkeit.....	72
4.3.4	Grundsatz der Datenvermeidung und der Datensparsamkeit.....	73
4.3.5	Schutz sensibler Daten .....	74
4.3.6	Transparenzgebot, offene Datenerhebung und Grundsatz der Direkterhebung .....	75

4.3.7	Technische und organisatorische Schutzmaßnahmen .....	76
4.4	Weitere relevante Vorschriften und Gegebenheiten .....	77
4.4.1	Grundgesetzlich motivierte Aspekte .....	77
4.4.1.1	Grundsatz der Gleichheit .....	77
4.4.1.2	Gefahr der Schaffung eines einheitlichen Personenkennzeichens .....	78
4.4.2	Legitimationsgrundlagen mit datenschutzrechtlicher Relevanz für den betrieblichen Systemeinsatz .....	80
4.4.2.1	Einwilligung oder Rechtsvorschrift als Ausgangsbasis einer Legitimation .....	80
4.4.2.2	Allgemeine Normierung des Persönlichkeitsschutzes in § 75 Abs. 2 Satz 1 BetrVG .....	82
4.4.2.3	Mitbestimmung des Betriebsrats gemäß § 87 Abs. 1 Satz 6 BetrVG .....	84
4.4.2.4	Legitimation des betrieblichen Einsatzes biometrischer Systeme auf der Grundlage des § 32 Abs. 1 Satz 1 BDSG .....	89
4.5	Position und Mitwirken des betrieblichen Datenschutzbeauftragten bei der Einführung biometrischer Systeme .....	93
4.5.1	Rolle des betrieblichen Datenschutzbeauftragten .....	94
4.5.2	Position und Verantwortlichkeit des Datenschutzbeauftragten bei der Einführung biometrischer Systeme im Unternehmen .....	96
4.5.3	Zusammenarbeit mit dem Betriebsrat .....	97
<b>5</b>	<b>Biometriespezifisches Gefährdungspotenzial und Schutzmaßnahmen...</b>	<b>101</b>
5.1	Allgemeine Risiken für den Einsatz biometrischer Systeme .....	102
5.2	Spezielle Risiken für den Einsatz biometrischer Systeme .....	103
5.2.1	Unrechtmäßige Aneignung der Nutzeridentität .....	103
5.2.2	Missbräuchliche Verwendung von Zusatzinformationen .....	105
5.2.3	Gefahr der lebenslangen Merkmalskompromittierung .....	106
5.2.4	Überwachungseignung biometrischer Systeme .....	107
5.2.5	Bildung von Personenprofilen .....	108

5.2.6	Zwang zur Nutzung biometrischer Systeme .....	109
5.3	Schutzmaßnahmen gegen das bestehende Gefährdungspotenzial.....	110
5.3.1	Technische Schutzmaßnahmen .....	110
5.3.1.1	Schutzmaßnahmen gegen den Datendiebstahl .....	110
5.3.1.2	Absicherung der Funktionsfähigkeit des Systems.....	114
5.3.1.3	Absicherung gestohlener oder verlorener biometrischer Daten.....	117
5.3.2	Gesetzliche Schutzmaßnahmen.....	120
5.3.3	Vertragliche Schutzmaßnahmen.....	121
5.4	Vertrauensbildende Maßnahmen als datenschutzförderliches Instrumentarium.....	122
5.4.1	Transparenz gegenüber den Systemnutzern.....	122
5.4.2	Überprüfung und Zertifizierung durch unabhängige Dritte .....	124
5.4.3	Selbstbeschränkung des Systembetreibers .....	126
5.4.4	Freiwilligkeit der Systemnutzung .....	127
5.5	Biometrie und Privacy Enhancing Technology (PET) .....	128
<b>6</b>	<b>Bewertungskriterien für eine datenschutzrechtliche Evaluation .....</b>	<b>131</b>
6.1	Prüfkriterien für eine Bewertung biometrischer Merkmale .....	133
6.1.1	Informationsgehalt des biometrischen Merkmals .....	133
6.1.2	Zeitliche Variabilität des biometrischen Merkmals .....	134
6.1.3	Ausspähbarkeit des biometrischen Merkmals.....	135
6.1.4	Willentliche Beeinflussbarkeit des biometrischen Merkmals....	136
6.2	Prüfkriterien für eine Bewertung biometrischer Systeme .....	137
6.2.1	Notwendigkeit des Systemeinsatzes.....	137
6.2.2	Berücksichtigung des vorab zu definierenden Verwendungszwecks im Systemdesign .....	138
6.2.3	Berücksichtigung der Erforderlichkeit im Systemdesign .....	139
6.2.4	Betriebsart des Systems: Identifikation versus Verifikation.....	140
6.2.5	Verzicht auf die Anlage einer zentralen Referenzdatenbank.....	141

6.2.6	Umsetzung eines datenschutzfreundlichen Speicherkonzepts ...	142
6.2.7	Reduktion des Personenbezugs bei den biometrischen Daten ...	142
6.2.8	Technische Sicherheit und Zuverlässigkeit des Systems .....	143
6.2.9	Umgang mit sensiblen Daten im biometrischen System.....	144
6.2.10	Transparenz des Systems und der Sicherheitsmechanismen .....	145
6.2.11	Gewährleistung hinreichender Mechanismen für die technische und die organisatorische Sicherheit.....	147
6.2.12	Angebot effektiver Alternativverfahren .....	149
<b>7</b>	<b>Evaluation ausgewählter Tippverhalten basierender Systeme .....</b>	<b>151</b>
7.1	Detaillierte Evaluation des Merkmals Tippverhalten .....	152
7.1.1	Informationsgehalt des Tippverhaltens .....	152
7.1.2	Zeitliche Variabilität des Tippverhaltens .....	153
7.1.3	Ausspähbarkeit des Tippverhaltens .....	153
7.1.4	Willentliche Beeinflussbarkeit des Tippverhaltens .....	154
7.1.5	Zusammenfassung der Evaluationsergebnisse des biometrischen Merkmals Tippverhalten.....	155
7.2	Vergleichende Gegenüberstellung mit weiteren Merkmalen .....	156
7.3	Evaluation textgebundener Authentifizierungssysteme .....	161
7.3.1	Notwendigkeit des Systemeinsatzes.....	161
7.3.2	Berücksichtigung des vorab zu definierenden Verwendungszwecks im Systemdesign.....	163
7.3.3	Berücksichtigung des Grundsatzes der Erforderlichkeit im Systemdesign .....	164
7.3.4	Betriebsart textgebundener Systemansätze .....	164
7.3.5	Verzicht auf eine zentrale Referenzdatenbank.....	165
7.3.6	Umsetzung eines datenschutzfreundlichen Speicherkonzepts ...	167
7.3.7	Reduktion des Personenbezugs bei den Tippverhaltensdaten....	169
7.3.8	Technische Sicherheit und Zuverlässigkeit textgebundener Authentifizierungssysteme .....	170

7.3.8.1	Aufbau des Testszenarios und Beschreibung der Testdatenbasis.....	171
7.3.8.2	Ergebnisse des Performancetests.....	173
7.3.8.3	Vergleich mit weiteren marktgängigen biometrischen Systemen.....	179
7.3.8.4	Bewertung der Sicherheit der Systemarchitektur.....	181
7.3.8.5	Abschließende Beurteilung des Sicherheitsniveaus.....	183
7.3.9	Umgang mit sensiblen Daten in textgebundenen Authentifizierungssystemen.....	183
7.3.10	Transparenz textgebundener Authentifizierungssysteme und deren Sicherheitsmechanismen.....	184
7.3.11	Gewährleistung hinreichender Mechanismen für die technische und die organisatorische Sicherheit.....	185
7.3.12	Angebot effektiver Alternativverfahren.....	186
7.3.13	Zusammenfassung der Evaluationsergebnisse textgebundener Systemansätze.....	186
7.4	Evaluation textungebundener Authentifizierungssysteme.....	188
7.4.1	Notwendigkeit des Systemeinsatzes.....	188
7.4.2	Berücksichtigung des vorab zu definierenden Verwendungszwecks im Systemdesign.....	190
7.4.3	Berücksichtigung des Grundsatzes der Erforderlichkeit im Systemdesign.....	192
7.4.4	Betriebsart textungebundener Systemansätze.....	193
7.4.5	Verzicht auf eine zentrale Referenzdatenbank.....	194
7.4.6	Umsetzung eines datenschutzfreundlichen Speicherkonzepts... ..	196
7.4.7	Reduktion des Personenbezugs bei den Tippverhaltensdaten....	196
7.4.8	Technische Sicherheit und Zuverlässigkeit textungebundener Authentifizierungssysteme.....	198
7.4.9	Umgang mit sensiblen Daten in textungebundenen Authentifizierungssystemen.....	199
7.4.10	Transparenz textungebundener Authentifizierungssysteme und deren Sicherheitsmechanismen.....	200

7.4.11 Gewährleistung hinreichender Mechanismen für die technische und die organisatorische Sicherheit.....	201
7.4.12 Angebot effektiver Alternativverfahren .....	202
7.4.13 Zusammenfassung der Evaluationsergebnisse textungebundener Systemansätze .....	202
<b>8 Legitimationsgrundlage für den Systemeinsatz im Unternehmen.....</b>	<b>207</b>
8.1 Systeme zur Tippverhaltenserkennung und der Schutz der Persönlichkeitsrechte von Betriebsangehörigen .....	207
8.2 Mitbestimmung des Betriebsrats beim Einsatz von Systemen zur Tippverhaltenserkennung.....	210
8.3 Systeme zur Tippverhaltenserkennung und die im Bundesdatenschutzgesetz manifestierten Legitimationsgrundlagen .....	214
<b>9 Abschließende Wertung und Ausblick .....</b>	<b>217</b>
<b>Literaturverzeichnis .....</b>	<b>221</b>



**Quelle:**

Florian Dotzler: *Datenschutzrechtliche Aspekte und der Einsatz biometrischer Systeme in Unternehmen. Eine exemplarische Betrachtung von Systemen auf der Grundlage des biometrischen Merkmals Tippverhalten*, Kölner Wissenschaftsverlag, Köln, 2010.

© 2010 Kölner Wissenschaftsverlag und Florian Dotzler