

NOMOSPRAXIS

Dr. Philip Laue | Dr. Judith Nink | Sascha Kremer

Das neue Datenschutzrecht in der betrieblichen Praxis

Dr. Philip Laue, Rechtsanwalt, Unternehmensanwalt im Bereich internationaler Datenschutz bei der Bayer AG | **Dr. Judith Nink**, Rechtsanwältin, Datenschutzbeauftragte und Legal Counsel bei der eyeo GmbH | **Sascha Kremer**, Fachanwalt für IT-Recht und externer Datenschutzbeauftragter, Gründungspartner der LOGIN Partners Rechtsanwälte

Nomos

Inhaltsverzeichnis

Vorwort	5
Literatur	19
§ 1 Einführung	29
A. Allgemeines	29
B. Anwendungsbereich der Datenschutz-Grundverordnung	30
I. Sachlicher Anwendungsbereich	31
1. Verarbeitung von Daten	31
2. Personenbezug der Daten	32
a) Identifizierbarkeit	32
aa) Anonyme Daten	34
bb) Pseudonymisierte Daten	36
cc) Verschlüsselte Daten	39
b) Natürliche Person	40
II. Persönlicher Anwendungsbereich	42
1. Der Verantwortliche	43
a) Natürliche oder juristische Person	43
b) Entscheidung über Zwecke und Mittel der Verarbeitung	45
aa) Entscheidungshoheit aufgrund rechtlicher Zuweisung	45
bb) Entscheidungshoheit aufgrund tatsächlichen Einflusses....	45
c) Gemeinsam Verantwortliche	46
aa) Voraussetzungen	47
bb) Rechtsfolgen	48
2. Auftragsverarbeiter	50
3. Kleinunternehmen sowie kleine und mittlere Unternehmen	51
III. Räumlicher Anwendungsbereich	52
1. Anwendungsbereich der Datenschutz-Grundverordnung	53
a) Niederlassungsprinzip nach Art. 3 Abs. 1	53
aa) Effektive und tatsächliche Ausübung einer Tätigkeit	53
bb) Verarbeitung im Rahmen der Tätigkeit der Niederlassung	54
cc) Ort der Verarbeitung	55
b) Marktortprinzip nach Art. 3 Abs. 2	56
aa) Angebot von Waren und Dienstleistungen	56
bb) Verhaltensbeobachtung	58
cc) Benennung eines Vertreters	59
2. Räumlicher Anwendungsbereich innerhalb der EU	62
a) Sitzlandprinzip	63
b) Territorialitätsprinzip	64

Inhaltsverzeichnis

c) Sonderfall Einwilligung	64
aa) Art. 8 Abs. 1	65
bb) Art. 9 Abs. 2 lit. a	65
d) Rechtswahlklauseln	66
IV. Öffnungsklauseln und besondere Verarbeitungssituationen	67
1. Öffnungsklauseln in Einzelregelungen	68
2. Verarbeitung im Beschäftigungskontext	71
3. Verarbeitung zur wissenschaftlichen Forschung und zu statistischen Zwecken	72
a) Datenminimierung und Widerspruchsrecht	73
b) Privilegierungen	73
4. Delegierte Rechtsakte und Durchführungsrechtsakte der EU-Kommission	75
5. Datenschutz-Grundverordnung und E-Privacy-Richtlinie	76
a) Rechtmäßigkeit der Verarbeitung	76
b) Beschränkungen möglicher Zweckänderungen	76
c) Einwilligung und Widerruf	77
d) Datensicherheit	77
e) Meldepflichten	77
V. Verarbeitungsgrundsätze	77
§2 Zulässigkeit der Verarbeitung	80
A. Allgemeines	80
I. Rechtfertigung der Verarbeitung	80
1. Einwilligung	80
a) Form der Einwilligung	81
b) Opt-In oder Opt-Out?	83
c) Transparenz	85
d) Widerrufsrecht	85
e) Freiwilligkeit der Einwilligung	86
aa) Abhängigkeitsverhältnis	86
bb) Trennungsgebot	88
cc) Koppelungsverbot	88
f) Einwilligung von Kindern	89
g) Anpassungsbedarf für Unternehmen	89
2. Gesetzliche Erlaubnistatbestände	89
a) Vertragserfüllung, Art. 6 Abs. 1 lit. b	90
b) Gesetzliche Verpflichtung, Art. 6 Abs. 1 lit. c und öffentliches Interesse, Art. 6 Abs. 1 lit. e	91
c) Schutz von lebenswichtigen Interessen	93
d) Generalklausel: Berechtigte Interessen	94
e) Zweckänderung, Art. 6 Abs. 4	96
f) Werbung und Adresshandel	97

3. Sonstige Regelungen als Erlaubnis	97
II. Verarbeitung von Daten eines Kindes	98
1. Interessensabwägung, Art. 6 Abs. 1 lit. f	98
2. Einwilligung bei Kindern, Art. 8	99
a) Dienst für die Informationsgesellschaft	100
b) An Kinder gerichtetes Angebot	100
c) Einwilligungsvoraussetzungen	100
aa) Altersgrenzen	100
bb) Dokumentationspflicht	101
cc) Praktische Umsetzung	101
dd) Allgemeines Vertragsrecht	102
ee) Sonstige Einwilligungen von Kindern	103
3. Sonstige Regelungen zum Schutz von Kindern	103
B. Verarbeitung besonderer Datenkategorien (Art. 9)	103
I. Grundsätzliches Verarbeitungsverbot	104
II. Ausnahmen vom Verarbeitungsverbot	105
1. Einwilligung, Abs. 2 lit. a	106
2. Verarbeitung zu Archiv-, historischen, statistischen und wissenschaftlichen Zwecken, Abs. 2 lit. j	107
III. Berufsgeheimnis, Art. 9 Abs. 2 lit. h iVm Abs. 3	107
IV. Öffnungsklausel, Abs. 4	108
C. Daten aus Strafurteilen und Straftaten, Art. 10	108
D. Verarbeitung ohne Identifizierung, Art. 11	109
E. Automatisierte Verarbeitung	110
I. Auf einer automatisierten Verarbeitung beruhende Entscheidungen	HO
1. Anwendungsbereich des Art. 22 Abs. 1	110
2. Erlaubnis automatisierter Entscheidungsfindungen	112
3. Pflichten des Verantwortlichen	113
II. Profiling	113
1. Begriff des Profilings	114
2. Profiling nach der Datenschutz-Grundverordnung	114
a) Scoring	114
b) Erlaubnistatbestände	115
c) Pflichten beim Profiling	115

Inhaltsverzeichnis

§3 Informationspflichten	117
A. Ratio der Informationspflichten	117
B. Inhalt der Informationspflichten	117
I. Gegenstand der Information	118
1. Allgemeine Informationen	118
a) Kontaktdaten, Art. 13 Abs. 1 lit. a / Art. 14 Abs. 1 lit. a	121
b) Darlegung der berechtigten Interessen, Art. 13 Abs. 1 lit. d / Art. 14 Abs. 2 lit. b	121
2. Informationen zur Gewährleistung einer fairen und transparen- ten Verarbeitung	121
a) Widerspruchsrecht, Art. 13 Abs. 2 lit. c / Art. 14 Abs. 2 lit. d ..	123
b) Einwilligung	124
c) Automatisierte Entscheidungsfindung und Profiling	124
d) Zweckänderung	125
3. Keine Direkterhebung	125
II. Ausnahmen von der Informationspflicht	125
III. Zeitpunkt der Information	126
IV. Form der Information (Darstellung)	127
1. Schriftlich und andere Form	127
2. Mündlich	128
3. Piktogramme	128
V. Kosten	128
VI. Überblick Informationspflichten	129
C. Verstöße	130
I. Bußgeld	130
II. Unterlassungsklagengesetz	130
III. Wettbewerbsrecht	131
§4 Rechte der betroffenen Person	133
A. Überblick	133
B. Modalitäten für die Ausübung der Rechte der betroffenen Person	134
I. Identifizierung der betroffenen Person	134
1. Vertretbare Mittel zur Prüfung der Identität	135
2. Keine Vorratsverarbeitung identifizierender Daten	136
II. Verfahren der Ausübung von Rechten der betroffenen Person	136
1. Form der Übermittlung von Mitteilungen	137
2. Erleichterungen bei der Ausübung	137
3. Ablauf und Fristen	138
4. Unentgeltlichkeit und Missbrauchsgebühr	139
C. Auskunftsrecht	140
I. Gegenstand des Auskunftsrechts	140

II. Bereitstellung von Kopien personenbezogener Daten	142
1. Unentgeltlichkeit und Bereitstellung mehrerer Kopien	142
2. Konkretisierung des Auskunftsverlangens	142
3. Bereitstellung in einem gängigen elektronischen Format	142
4. Beachtung der Rechte Dritter	143
III. Auskunft aus Patientenakten	145
D. Recht auf Berichtigung	145
I. Berichtigung unrichtiger personenbezogener Daten	145
II. Vervollständigung richtiger personenbezogener Daten	146
III. Darlegungs- und Beweislast	146
E. Recht auf Löschung und Recht auf Vergessenwerden	146
I. Voraussetzungen für das Recht auf Löschung	147
1. Lösungsgründe im Überblick	147
2. Entfallen des Verarbeitungszwecks	148
3. Widerruf der Einwilligung	148
4. Unrechtmäßige Verarbeitung	148
5. Von Kindern erhobene Daten	149
II. Folgen des Rechts auf Löschung	149
1. Löschung personenbezogener Daten	149
2. Recht auf Vergessenwerden im engeren Sinn	150
3. Mitteilung an Empfänger und Auskunftsrecht	151
III. Ausnahmen vom Recht auf Löschung	151
IV. Darlegungs- und Beweislast	152
F. Recht auf Einschränkung der Verarbeitung	152
I. Voraussetzungen des Rechts auf Einschränkung	152
II. Folgen des Rechts auf Einschränkung	153
III. Darlegungs- und Beweislast	153
G. Recht auf Datenübertragbarkeit	154
I. Ratio	155
II. Anwendungsbereich	155
III. Direktübermittlung an anderen Verantwortlichen	156
IV. Technische Anforderungen	157
H. Widerspruchsrecht	157
I. Voraussetzungen für Widerspruchsrecht	158
1. Allgemeines Widerspruchsrecht aus besonderer Situation	158
2. Widerspruchsrecht bei Direktwerbung	158
3. Ausübung mittels automatisierter Verfahren	159
II. Folgen des Widerspruchs	159
III. Darlegungs- und Beweislast	160

§5 Verarbeitung durch Dritte und im Ausland	161
A. Allgemeines	161
I. Begriff der Auftragsverarbeitung	161
1. Bislang geltendes nationales Recht	161
a) Privilegierung der Auftragsverarbeitung	161
b) Abgrenzung zur Funktionsübertragung	162
2. Auftragsverarbeitung nach der Datenschutz-Grundverordnung ..	163
a) Pflichten des Auftragsverarbeiters	163
b) Auftragsverarbeitung in Drittländern	165
II. Rechtfertigung	165
III. Auswahl des Auftragsverarbeiters	166
IV. Formelle Anforderungen der Auftragsverarbeitung	167
V. Inhalt eines Vertrags zur Auftragsverarbeitung	168
1. Weisungen	169
2. Vertraulichkeit	170
3. Einsatz von Unterauftragnehmern	170
4. Beendigung des Auftrags	173
5. Kontrollen	173
VI. Konsequenzen bei Verstößen	174
VII. Umgang mit Altverträgen	174
B. Internationale Verarbeitung	175
I. Allgemeines	176
II. Angemessenheitsbeschluss, Art. 45	176
1. Allgemeines	176
2. Selbstverpflichtungen	178
a) EU-U.S. Privacy Shield	178
aa) Inhalt	178
bb) Compliance	179
b) Safe Harbor (unwirksam)	179
III. Geeignete Garantien, Art. 46	180
1. Binding Corporate Rules, Art. 47	180
a) Inhaltliche Anforderungen	181
b) Genehmigungsverfahren	182
2. Standarddatenschutzklauseln	183
3. Genehmigte Verhaltensregeln und Zertifizierungsverfahren	184
4. Genehmigte sonstige Verträge	185
IV. Urteile und Entscheidungen aus Drittländern, Art. 48	185
V. Ausnahmen, Art. 49	187
1. Einwilligung	188
2. Vertragliche Pflichten	188
3. Auffangtatbestand Art. 49 Abs. 1 Satz 2	189

§6 Datenschutzbeauftragter	191
A. Rolle des Datenschutzbeauftragten	191
B. Benennung des Datenschutzbeauftragten	192
I. Benennungspflicht	193
1. Benennungspflicht nach der Datenschutz-Grundverordnung	193
2. Benennungspflicht nach dem Recht der Union oder der Mitgliedsstaaten	194
3. Datenschutzbeauftragte im Konzern	195
a) Benennung durch beteiligte Unternehmen	195
b) Leichte Erreichbarkeit aus allen Niederlassungen	196
4. Interner und externer Datenschutzbeauftragter	197
5. Veröffentlichung und Mitteilung der Kontaktdaten	198
6. Fortgeltung von nach dem BDSG erfolgten Bestellungen	199
II. Voraussetzungen für die Bestellung	200
1. Berufliche Qualifikation, Fachwissen und Fähigkeiten	200
2. Zuverlässigkeit	200
C. Stellung des Datenschutzbeauftragten	201
I. Unterstützungspflicht des Verantwortlichen oder Auftragsverarbeiters	202
II. Unabhängigkeit des Datenschutzbeauftragten	203
1. Weisungsfreiheit	203
2. Benachteiligungsverbot	204
3. Berichtspflicht gegenüber höchster Managementebene	205
III. Wahrung der Geheimhaltung oder Vertraulichkeit	205
IV. Ansprechpartner für betroffene Personen	206
D. Aufgaben des Datenschutzbeauftragten	206
I. Unterrichtung und Beratung	207
II. Überwachung des Datenschutzes	207
III. Zusammenarbeit mit der Aufsichtsbehörde	209
IV. Risikoangemessenheit der Aufgabenerfüllung	210
E. Haftung des Datenschutzbeauftragten	210
§7 Technischer und organisatorischer Datenschutz	212
A. Datensicherheit	212
I. Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen	213
1. Regelungsadressaten	214
2. Inhaltliche Anforderungen	214
a) Datenschutz durch Technik	214
b) Datenschutzfreundliche Voreinstellungen	216

Inhaltsverzeichnis

II. Sicherheit bei der Verarbeitung	217
1. Regelungsadressaten	217
2. Inhaltliche Anforderungen	218
III. Praktische Umsetzung	219
B. Informationspflichten bei Datenschutzverletzungen	221
I. Meldepflicht gegenüber Aufsichtsbehörden	222
1. Meldepflichtige Ereignisse	222
2. Meldefrist	223
3. Inhalt und Form der Meldung und sonstige Dokumentationspflichten	224
4. Unterstützungspflicht des Auftragsverarbeiters	225
II. Benachrichtigungspflicht gegenüber betroffenen Personen	227
1. Benachrichtigungspflichtige Ereignisse	228
2. Benachrichtigungsfrist	229
3. Inhalt und Form der Benachrichtigung	230
4. Ausnahmen von der Benachrichtigungspflicht	230
C. Datenschutz-Folgenabschätzung	233
I. Regelungsadressaten	234
II. Voraussetzung der Folgenabschätzung	234
1. Voraussichtlich hohes Risiko	235
a) Gesetzliche Regelbeispiele	235
b) Listen der zuständigen Aufsichtsbehörden	236
2. Befreiung von der Folgenabschätzung für bestimmte Verarbeitungszwecke	238
III. Durchführung der Folgenabschätzung	239
1. Zusammenfassung gleichartiger Verarbeitungen	240
2. Dokumentation	240
3. Verhaltensregeln	241
4. Einbindung des Datenschutzbeauftragten	241
5. Einbindung der zuständigen Aufsichtsbehörde	242
6. Einbindung der betroffenen Personen oder ihrer Vertreter	244
a) Gegebenenfalls	245
b) Keine entgegenstehenden kommerziellen Interessen oder Sicherheitsinteressen	246
7. Überprüfung	246
D. Verzeichnis von Verarbeitungstätigkeiten	248
I. Bisherige Rechtslage	249
II. Aufzeichnungspflichten nach der Datenschutz-Grundverordnung	249
1. Verzeichnis des Verantwortlichen	251
2. Verzeichnis des Auftragsverarbeiters	253

§ 8 Selbstregulierung	255
A. Verhaltensregeln (Codes of Conduct)	255
I. Vorlageberechtigte Stellen	256
II. Gegenstand von Verhaltensregeln	256
III. Genehmigungsverfahren	257
1. Nationale Verhaltensregeln	258
2. Multinationale Verhaltensregeln	258
IV. Überprüfung durch private Kontrollstellen	258
V. Rechtsfolgen	260
1. Bindungswirkung für Aufsichtsbehörden	261
2. Nachweiserleichterungen für Pflichten aus der Datenschutz- Grundverordnung	261
3. Rechtsfolgen von Verstößen gegen Verhaltensregeln	262
B. Datenschutzzertifizierungen	263
I. Zertifizierungsgegenstand	264
II. Zertifizierungsmaßstab	264
III. Zertifizierungsverfahren	265
IV. Zertifizierungsstelle	266
V. Rechtsfolgen	267
1. Nachweiserleichterungen für Pflichten aus der Datenschutz- Grundverordnung	267
2. Rechtsfolgen von Verstößen	268
§ 9 Beschäftigtendatenschutz	270
A. Allgemeines	270
B. Anforderungen an mitgliedstaatliche Vorschriften	270
C. Hinweise für Arbeitgeber	272
§ 10 Zusammenarbeit mit Aufsichtsbehörden	274
A. Allgemeines	274
B. Stellung der Aufsichtsbehörden	275
I. Unabhängigkeit der Aufsichtsbehörden	275
II. Mehrere Aufsichtsbehörden in einem Mitgliedstaat	276
C. Aufgaben der Aufsichtsbehörden	277
I. Übersicht wesentlicher Aufgaben	277
II. Beschwerderecht der betroffenen Person	279
III. Unentgeltlichkeit der Aufgabenerfüllung	279
D. Befugnisse der Aufsichtsbehörden	280
I. Untersuchungsbefugnisse	281
II. Abhilfebefugnisse	282

Inhaltsverzeichnis

III. Genehmigungsbefugnisse und beratende Befugnisse	283
E. Zuständigkeit und Zusammenarbeit der Aufsichtsbehörden	284
I. Zuständigkeit der Aufsichtsbehörden	284
1. Zuständigkeit der federführenden Aufsichtsbehörde	285
a) Feststellung der federführenden Aufsichtsbehörde	285
b) Mehrere Niederlassungen oder eine Niederlassung in der Union	286
c) Abweichende Zuständigkeit bei Angelegenheiten in einem Mitgliedstaat	288
2. One-Stop-Shop	288
II. Zusammenarbeit in konkreten Angelegenheiten	289
1. Vorgehen in Verantwortung der federführenden Aufsichtsbehörde	289
2. Amtshilfe und gemeinsame Maßnahmen	293
3. Dringlichkeitsmaßnahmen	293
III. Kohärenzverfahren	294
1. Stellungnahmen durch den Ausschuss	295
2. Streitbeilegung durch den Ausschuss	296
F. Zusammenarbeit von Verantwortlichen und Auftragsverarbeitern mit Aufsichtsbehörden	297
G. Europäischer Datenschutzausschuss	298
§ 11 Haftung, Sanktionen und Rechtsbehelfe	301
A. Haftung	301
I. Verletzungshandlung	301
II. Schaden	302
III. Anspruchsberechtigter	302
IV. Ersatzpflichtige	303
V. Exkulpationsmöglichkeit	304
VI. Gesamtschuldnerische Haftung	305
VII. Sonstige Ansprüche	306
B. Sanktionen	307
I. Bußgelder	307
1. Ermessen der Aufsichtsbehörden	307
2. Kategorien von bußgeldbewehrten Verstößen	308
3. Geldbußen bei Unternehmensgruppen	309
II. Sanktionen der Mitgliedstaaten	310
C. Rechtsbehelfe	311
I. Rechtsbehelfe betroffener Personen	311
1. Beschwerderecht	311

2. Klagerecht	312
a) Klagen gegen Aufsichtsbehörden	312
b) Klagen gegen Verantwortliche oder Auftragsverarbeiter	312
II. Rechtsbehelfe von Verantwortlichen, Auftragsverarbeitern, ua	313
III. Rechtsbehelfe von Verbänden	313
1. Vertretung von betroffenen Personen	313
2. Datenschutzverbandsklage	314
IV. Aussetzung des Verfahrens	315
V. Rechtsbehelfe gegen Beschlüsse des Ausschusses	316
 Stichwortverzeichnis	 317