

Dr. Axel von Walter (Hrsg.)

Datenschutz im Betrieb

Die DS-GVO in der Personalarbeit

1. Auflage

Inhaltsverzeichnis

1	Einleitung	15
2	Neue Aufgaben für HR-Fach- und Führungskräfte	21
2.1	Besonders betroffen von den neuen Regelungen: das Personalwesen	21
2.2	Sensibilität im Umgang mit Bewerberdaten	22
2.3	Aufgaben im laufenden Beschäftigungsverhältnis	25
2.4	Aufgaben nach Beendigung des Beschäftigungsverhältnisses	27
2.5	Zur Rolle des Betriebsrats	28
2.6	Instruktion von Mitarbeitern	30
3	Der Datenschutzbeauftragte	33
3.1	Die Pflicht zur Benennung eines Datenschutzbeauftragten	33
3.2	Benennung und Abberufung eines Datenschutzbeauftragten	36
3.2.1	Die Formalien der Benennung	36
3.2.2	Benennung für mehrere Organisationen	38
3.2.3	Abberufung	39
3.3	Anforderungen an den Datenschutzbeauftragten	39
3.4	Die Stellung des Datenschutzbeauftragten im Unternehmen	42
3.5	Aufgaben und Pflichten des Datenschutzbeauftragten	45
3.6	Alternative Rollen im Unternehmen neben oder statt dem Datenschutzbeauftragten	47
3.7	Musterschreiben: Benennung eines Datenschutzbeauftragten	48
4	Dokumentationspflichten und das Verarbeitungsverzeichnis	51
4.1	Die Nachweis- und Dokumentationspflichten in der DS-GVO	51
4.2	Das Verarbeitungsverzeichnis	52
4.2.1	Form des Verzeichnisses	54
4.2.2	Inhalt des Verzeichnisses	55
4.3	Erstellung und Pflege des Verarbeitungsverzeichnisses	60
5	Die Rechte der betroffenen Personen	63
5.1	Informationspflichten	63
5.1.1	Informationspflichten bei Direkterhebung	64
5.1.2	Informationspflichten bei Dritterhebung	64

5.1.3	Überblick über die mitzuteilenden und bereitzustellenden Informationen	64
5.1.4	Informationspflichten bei Zweckänderung und Übermittlung	71
5.1.5	Form der Informationspflicht	71
5.1.6	Ausnahmen	73
5.2	Individualrechte des Betroffenen zur Sicherung der informationellen Selbstbestimmung	74
5.2.1	Auskunftersuchen, Art. 15 DS-GVO	75
5.2.2	Das Recht auf Berichtigung, Art. 16 DS-GVO	78
5.2.3	Das Recht auf Löschung, Art. 17 DS-GVO	79
5.2.4	Das Recht auf Einschränkung der Verarbeitung, Art. 18 DS-GVO	80
5.2.5	Anfragen auf Datenübertragung (Art. 20 DS-GVO)	81
5.2.6	Das Widerspruchsrecht, Art. 21 DS-GVO	83
5.3	Das Vorgehen bei Betroffenen-Anfragen	84
5.3.1	Vorüberlegungen	85
5.3.2	Eingang der Anfrage des Betroffenen	85
5.3.3	Prüfung der Anfrage	86
5.3.4	Information an die Betroffenen und Speicherung der Anfrage	89
5.4	Musterschreiben und Formulare	89
5.4.1	Formular für die interne Vorbereitung der Auskunftserteilung	89
5.4.2	Muster für Antwortschreiben	90
6	Beschäftigtendatenschutz	97
6.1	Begriff und Zweck des Beschäftigtendatenschutzes	97
6.2	Rechtliche Grundlagen des Beschäftigtendatenschutzes	97
6.3	Beschäftigtenbegriff	98
6.4	Begriff der personenbezogenen Daten	98
6.5	Begriff der Verarbeitung	100
6.6	Erlaubnistatbestände zur Verarbeitung von Beschäftigtendaten	101
6.7	Beschäftigtendatenschutz im Bewerbungsverfahren	103
6.7.1	Welche Daten darf der Arbeitgeber erheben?	103
6.7.2	Was muss der Arbeitgeber wann löschen?	106
6.8	Beschäftigtendatenschutz im Arbeitsverhältnis	107
6.8.1	Welche Daten darf der Arbeitnehmer verarbeiten?	107
6.8.2	Besonderheiten der Videoüberwachung	110

6.8.3	Compliance-Maßnahmen	114
6.8.4	Was muss der Arbeitgeber wann löschen?	117
6.9	Einhaltung der Grundsätze der DS-GVO	118
6.10	Rechtsfolgen bei Verstößen gegen den Beschäftigtendatenschutz	118
7	Einwilligung im Beschäftigungsverhältnis	121
7.1	Rechtliche Grundlagen der Einwilligung im Beschäftigtenverhältnis	121
7.2	Freiwilligkeit der Einwilligung im Beschäftigtenverhältnis	121
7.3	Schriftform der Einwilligung	124
7.4	Pflicht zur Aufklärung über den Zweck der Datenverarbeitung	125
7.5	Widerrufsrecht	126
7.6	Alternativen zur Einwilligung im Beschäftigungsverhältnis	126
8	Die Betriebsvereinbarung und andere Kollektivvereinbarungen	129
8.1	Betriebsvereinbarungen und Tarifverträge als datenschutzrechtliche Erlaubnisgrundlage nach der DS-GVO	129
8.1.1	Datenschutzrechtliche Erlaubnisgrundlage nach BDSG a.F.	129
8.1.2	Auch datenschutzrechtliche Erlaubnisgrundlage nach der DS-GVO	130
8.2	Kann durch eine Kollektivvereinbarung das Schutzniveau der DS-GVO abgesenkt werden?	131
8.2.1	Abweichung vom datenschutzrechtlichen Schutzniveau nach BDSG a.F.	131
8.2.2	Keine wesentliche Unterschreitung des Schutzniveaus der DS-GVO	132
8.2.3	Handlungsspielräume der DS-GVO durch Kollektivvereinbarungen gestalten	132
8.3	Doppelfunktion von Betriebsvereinbarungen in der Praxis	133
8.3.1	Mitbestimmungstatbestand des §87 Abs. 1 Nr. 6 BetrVG	133
8.3.2	Gleichzeitig datenschutzrechtliche Erlaubnisgrundlage nach der DS-GVO	135
8.4	Inhaltliche Anforderungen der DS-GVO an Betriebsvereinbarungen	136
8.4.1	Transparenz und Prinzipien des Art. 5 DS-GVO	136
8.4.2	Rechenschaftspflicht	139
8.4.3	Übermittlung personenbezogener Daten innerhalb der Unternehmensgruppe	140
8.4.4	Überwachungssysteme am Arbeitsplatz	142

8.5	Handlungsempfehlungen für die Formulierung einer Betriebsvereinbarung nach der DS-GVO	144
8.5.1	Allgemein zwingend notwendige Regeln	144
8.5.2	Im besonderen Fall notwendige bzw. mögliche Regelungs- tatbestände	145
8.6	Verhandlungstaktik bei der Anpassung von Betriebsvereinbarungen	147
9	Arbeitnehmerüberlassung	149
10	Digitale Personalakte	151
10.1	Personalakte – eine Begriffsdefinition	151
10.2	Grundsätze bei der Führung von Personalakten	152
10.2.1	Grundsatz der Vollständigkeit vs. Grundsatz der Daten- minimierung und Speicherbegrenzung	153
10.2.2	Grundsatz der Richtigkeit	157
10.2.3	Grundsatz der Transparenz	157
10.2.4	Grundsatz der Integrität und Vertraulichkeit	158
10.3	Schritt für Schritt zur digitalen Personalakte	159
10.3.1	Schritt 1: Bestandsaufnahme	159
10.3.2	Schritt 2: Auswahl des Dienstleisters bzw. Systems	160
10.3.3	Schritt 3: Frühzeitige Beteiligung des Datenschutz- beauftragten	160
10.3.4	Schritt 4: Beteiligung des Betriebsrats	161
10.3.5	Schritt 5: Privacy by Design und Privacy by Default	161
10.3.6	Schritt 6: Einführung eines Löschkonzepts	162
10.3.7	Schritt 7: Prüfen, ob Erfordernis einer Datenschutz-Folgen- abschätzung besteht, und ggf. Durchführung der Datenschutz- Folgenabschätzung	162
10.3.8	Schritt 8: Entscheidung über das Führen einer Rumpfakte	162
10.3.9	Schritt 9: Organisation der digitalen Personalakte – konzernweite Datenverarbeitung	165
10.3.10	Schritt 10: Sicheres Vernichten aller (irrelevanten) Dokumente	165
11	Datenschutz und elektronische Kommunikation	167
11.1	Die Verwendung von E-Mail und Internet am Arbeitsplatz	167
11.2	Regelungsmöglichkeiten für den Arbeitnehmer	168

11.2.1	Keine Regelung zur Privatnutzung	168
11.2.2	Sonderfall betriebliche Übung	168
11.2.3	Ausdrückliche Regelung zur Privatnutzung	169
11.3	Kontrollmöglichkeiten	170
11.3.1	Kontrollen bei Verbot der privaten Nutzung	170
11.3.2	Kontrollen bei Erlaubnis der privaten Nutzung	172
11.4	Handlungsempfehlungen und Checkliste	176
11.4.1	Die einfachste Lösung: Verbot der privaten Nutzung	176
11.4.2	Klare Regelung notwendig: Erlaubnis der privaten Nutzung	177
12	Interne Untersuchungen und Aufdeckung von Pflichtverletzungen	179
12.1	Einleitung	179
12.2	Insbesondere: Videoüberwachung	180
12.3	Aktuelle Entscheidungen	180
12.3.1	Unzulässigkeit von Keylogger-Software	180
12.3.2	Überwachungsmaßnahmen durch Detektive	183
12.3.3	Mitbestimmung des Betriebsrats bei Einrichtung einer Facebook-Seite	185
13	Auftragsverarbeitung	187
13.1	Einführung	187
13.2	Der Auftragsverarbeiter	192
13.2.1	Stellung des Auftragsverarbeiters	192
13.2.2	Neue Pflichten des Auftragsverarbeiters	194
13.3	Auswahl des Auftragsverarbeiters	196
13.4	Vertrag zwischen Verantwortlichem und Auftragsverarbeiter	198
13.4.1	Erforderlichkeit eines Vertrags	198
13.4.2	Notwendige Vertragsinhalte	199
13.4.3	Umsetzung dieser Vertragsinhalte	208
13.5	Unterauftragnehmer	209
13.5.1	Genehmigung	209
13.5.2	Anforderungen an den Unterauftrag	212
13.5.3	Haftung für den Unterauftragsverarbeiter	213
13.6	Form	214
13.7	Internationale Auftragsverarbeitung	215
13.8	Einstandspflichten, Haftung und Sanktionen	218

13.8.1	Einstandspflichten des Auftragsverarbeiters	218
13.8.2	Haftung	219
13.8.3	Sanktionsmöglichkeiten der Aufsichtsbehörde	223
13.9	Fortgeltung bestehender Verträge	224
13.10	Checkliste: ADV-Vertrag	227
14	Konzerndatenschutz	229
14.1	Grundlagen	229
14.1.1	Begriff des Konzerns	229
14.1.2	Fehlendes »Konzernprivileg« im Datenschutzrecht	229
14.2	Rechtsgrundlage für die konzerninterne Übermittlung und weitere Verarbeitung von personenbezogenen Daten	230
14.2.1	Auftragsverarbeitung	230
14.2.2	Konzerninterne Übermittlung	232
14.3	Gemeinsame Verantwortlichkeit gem. Art. 26 DS-GVO	240
14.4	Fallgruppen	241
14.4.1	Konzernweites Kontakt-Verzeichnis	241
14.4.2	Zentralisierung der Personalverwaltung	242
14.4.3	Matrix-Strukturen	242
14.4.4	Skill-Datenbanken	242
14.4.5	Konzernweites Recruiting	243
14.5	Datenübermittlung an Konzernunternehmen in Drittländern	243
14.6	Checkliste	244
15	Outsourcing	247
15.1	Generelle Voraussetzungen	247
15.1.1	Auftragsdatenverarbeitung	247
15.1.2	Funktionsübertragung	247
15.1.3	Berufsgeheimnisträger	248
15.1.4	Einbeziehung des Datenschutzbeauftragten und des Betriebsrates	248
15.2	Übermittlung an Outsourcing-Unternehmen in Drittländer	249
15.3	Auswahl des Outsourcing-Anbieters	249
15.4	Fragenkatalog für Outsourcing-Projekte	251

16	Internationaler Datenverkehr	253
16.1	Die »Zwei Stufen«-Prüfung bei internationalen Datentransfers	253
16.2	Datentransfer in Drittländer auf Grundlage eines Angemessenheitsbeschlusses	254
16.3	EU-US Privacy Shield	254
16.4	Datenübermittlung auf Grundlage von Standarddatenschutzklauseln gem. Art. 46 Abs. 2c und d DS-GVO	255
16.5	Verbindliche interne Datenschutzvorschriften gem. Art. 47 DS-GVO ..	257
16.6	Genehmigte Verhaltensregeln und Zertifizierungsmechanismen	258
16.7	Genehmigungsbedürftige vertragliche Regelungen	259
16.8	Gesetzliche Erlaubnistatbestände	259
17	Löschkonzept	263
17.1	Im Fokus: Löschverpflichtung	263
17.2	Das Prinzip der Speicherbegrenzung und die Löschverpflichtung	263
17.3	Technische und organisatorische Maßnahmen zur Speicherbegrenzung	264
17.4	Das Löschkonzept	265
17.5	Beispiel: Löschregeln im Personalbereich	266
18	Direktmarketing	275
18.1	Bestehende Kundenbeziehung	275
18.1.1	Überblick	275
18.1.2	Details	276
18.2	Einwilligung	277
18.2.1	Gültigkeit von Alt-Einwilligungen – Übergangsregelungen	278
18.2.2	Anforderungen nach der DS-GVO	279
18.3	Rechtfertigung durch gesetzlichen Erlaubnistatbestand	285
18.4	Keine Sonderregelungen bei Geschäftskontakten	286
19	Industrie 4.0 im Kontext des Datenschutzes	289
19.1	Beschäftigtendatenschutz	289
19.2	Datentransfers in Drittstaaten	293
19.3	Datensicherheit	296
19.4	Exkurs: Data Ownership	297

20	Verarbeitung personenbezogener Daten Minderjähriger im Internet	299
20.1	Strengere Schutzanforderungen bei Kindern	299
20.2	Allgemeine Anforderungen an die Einwilligung	300
20.3	Wirksamkeit von alten Einwilligungserklärungen	302
20.4	Besondere Anforderungen an die Einwilligung bei Kindern	303
20.5	Entbehrlichkeit der Einwilligung bei notwendiger Datenverarbeitung	305
	20.5.1 Berechtigte Interessen	305
	20.5.2 Erfüllung eines Vertrags	306
21	IT-Sicherheit im Unternehmen	309
21.1	Ausgangslage	309
21.2	Typisches Angriffsszenario	310
21.3	Datenverarbeitung als wesentlicher Teil der IT-Sicherheit	310
21.4	Rechtlicher Rahmen	312
	21.4.1 Anwendbarkeit des Datenschutzrechts	312
	21.4.2 Gesetzliche Anforderungen an die IT-Sicherheit	313
	21.4.3 Zulässige Verarbeitung und Speicherdauer von Daten	316
21.5	Praktische Umsetzung/Checkliste	326
22	Datenschutz-Folgenabschätzung	329
22.1	Zielsetzung	329
22.2	Erforderlichkeit der Datenschutz-Folgenabschätzung	330
	22.2.1 Grundsatz	331
	22.2.2 Konkretisierung durch Regelbeispiele	333
	22.2.3 Kriterien für ein »hohes Risiko« nach der Artikel-29-Datenschutzgruppe	336
	22.2.4 Orientierung an Listen der Aufsichtsbehörden	338
	22.2.5 Zwischenergebnis	339
22.3	Durchführung der Datenschutz-Folgenabschätzung	339
	22.3.1 Die Vorbereitungsphase	340
	22.3.2 Die Bewertungsphase	343
	22.3.3 Die Maßnahmenphase	346
22.4	Einbeziehung des Datenschutzbeauftragten	348
22.5	Einbeziehung der Betroffenen	348
22.6	Konsultation der Aufsichtsbehörde	349
22.7	Altfälle: Bewertung von vorhandenen Verarbeitungsprozessen	350

22.8	Überprüfung und Wiederholung der Datenschutz-Folgenabschätzung .	351
22.9	Sanktionen	352
23	Datenschutzrisikomanagement	353
23.1	Einführung	353
23.2	Rahmenbedingungen eines Compliance- und Datenschutz- Management-Systems	355
23.3	Bestandsaufnahme als Vorbereitungsmaßnahme	356
23.4	Umsetzung	358
23.4.1	Beschreibung der Datenverarbeitungsprozesse	359
23.4.2	Im Fokus: Beschäftigtendatenschutz	361
23.4.3	Stärkung der Rolle des Datenschutzbeauftragten	362
23.4.4	Anpassung der IT-Struktur	363
23.4.5	Implementierung eines Löschmodernents	365
23.4.6	Kollektivrechtliche Aspekte	367
23.4.7	Kommunikation und Training	367
24	Datenschutzaudit und Zertifizierung	369
24.1	Das Datenschutz-Management-System	369
24.2	Audit, Übung, Wartung	370
24.3	Strategie definieren, Maßnahmen planen	372
24.4	Strategien und Maßnahmen implementieren	376
24.5	Umsetzung kontrollieren	376
24.6	Etablierung von Datenschutzorganisation und Datenschutz-Kultur ..	377
24.7	Projektmanagement	378
24.8	Datenschutzsiegel	378
25	Datenschutzschulung und Sensibilisierung	381
25.1	Relevante Schulungsinhalte	381
25.1.1	Besondere Arten personenbezogener Daten	381
25.1.2	Einwilligung des Betroffenen	382
25.1.3	Neue Rechte des Betroffenen	383
25.1.4	Verzeichnis für Verarbeitungstätigkeiten	383
25.1.5	Benachrichtigungspflicht bei Sicherheitspannen	383
25.2	Durchführung der Schulungsmaßnahmen und Sensibilisierung der Mitarbeiter	384

Die Autoren	387
Abkürzungsverzeichnis	391
Literaturverzeichnis	397
Stichwortverzeichnis	401