

Axel von Walter (Hrsg.)

Datenschutz im Betrieb

Die DSGVO in der Personalarbeit

**Beschäftigten-
Datenschutz**
aktuell

HAUFE.

Urheberrechtsinfo

Alle Inhalte dieses eBooks sind urheberrechtlich geschützt.

Die Herstellung und Verbreitung von Kopien ist nur mit ausdrücklicher Genehmigung des Verlages gestattet.

Datenschutz im Betrieb

Dr. Axel von Walter (Hrsg.)

Datenschutz im Betrieb

Die DS-GVO in der Personalarbeit

1. Auflage

Haufe Group
Freiburg · München · Stuttgart

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.dnb.de> abrufbar.

Print: ISBN 978-3-648-11138-3 Bestell-Nr. 14064-0001

ePub: ISBN 978-3-648-11139-0 Bestell-Nr. 14064-0100

ePDF: ISBN 978-3-648-11140-6 Bestell-Nr. 14064-0150

Dr. Axel von Walter (Hrsg.)

Datenschutz im Betrieb

1. Auflage 2018

© 2018 Haufe-Lexware GmbH & Co. KG, Freiburg

www.haufe.de

info@haufe.de

Produktmanagement: Bernhard Landkammer

Lektorat: Nicole Jähnichen und Alexandra Kittke

Satz: Reemers Publishing Services GmbH, Krefeld

Umschlag: RED GmbH, Krailling

Alle Angaben/Daten nach bestem Wissen, jedoch ohne Gewähr für Vollständigkeit und Richtigkeit. Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

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 Daten- schutzbeauftragten	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	Auskunftsersuchen, 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 Regelungstatbestände	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 Datenminimierung 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 Datenschutzbeauftragten	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-Folgenabschätzung 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 Löschanagements	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

1 Einleitung

Am 25.05.2018 begann für den Datenschutz in Europa ein neues Zeitalter. Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)¹ bildet seitdem den Europäischen Rechtsrahmen und den Maßstab für den Datenschutz in Europa. Auch wenn es weiterhin zahlreiche nationale oder europarechtliche Spezialvorschriften zum Schutz personenbezogener Daten geben wird, ist jetzt die Datenschutz-Grundverordnung (DS-GVO) der Fixstern und stellt für die Grundprinzipien des Datenschutzes einen einheitlichen Standard auf.

Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht, das sich aus Art. 8 Abs. 1 der Charta der Grundrechte der Europäischen Union (EU-Grundrechtecharta)² sowie Art. 16 Abs. 1 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV)³ ergibt. Auch wenn die grundrechtliche Verankerung auf europäischer Ebene noch sehr jung ist, kennen wir das Grundrecht auf informationelle Selbstbestimmung in Deutschland spätestens seit der wichtigen Entscheidung des Bundesverfassungsgerichts aus dem Jahr 1983, die als sogenanntes Volkszählungsurteil bekannt wurde.⁴ Darin erkennt das Bundesverfassungsgericht das *Grundrecht auf informationelle Selbstbestimmung* an. Es soll die Befugnis des Einzelnen gewährleisten, grundsätzlich selbst über die Preisgabe und die Verwendung seiner persönlichen Daten zu bestimmen. In diesem Urteil, das fern des heutigen Digitalzeitalters gefällt wurde, hat das Bundesverfassungsgericht bereits den sich aus dem technischen Fortschritt ergebenden

-
- 1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 v. 04.05.2016, S. 1ff.
 - 2 Charta der Grundrechte der Europäischen Union (2010/C 83/02), ABl. Nr. C 83 v. 30.03.2010, S. 389ff.
 - 3 Konsolidierte Fassungen des Vertrags über die Europäische Union und des Vertrags über die Arbeitsweise der Europäischen Union (2012/C 326/01), ABl. Nr. C 326 v. 26.10.2012, S. 1ff.
 - 4 BVerfG, Urteil v. 15.12.1983, 1 BvR 209/83, BVerfGE 65, 1.

Schutzbedarf für die Persönlichkeit des Einzelnen erkannt und deswegen die informationelle Selbstbestimmung als Abwehrrecht des Einzelnen gegen den Daten sammelnden Staat etabliert. Es hat ausdrücklich darauf hingewiesen, dass die Befugnis, selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden, unter den Bedingungen der automatischen Datenverarbeitung in besonderem Maße des Schutzes bedürfe. Diese Selbstbestimmung sei vor allem deshalb gefährdet, weil bei Entscheidungsprozessen nicht mehr auf manuell zusammengetragene Karteien und Akten zurückgegriffen werden müsse, sondern vielmehr mithilfe der automatischen Datenverarbeitung personenbezogene Daten technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar seien.⁵ Diese Daten können darüber hinaus – vor allem beim Aufbau integrierter Informationssysteme – mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne dass der Betroffene dessen Richtigkeit und Verwendung ausreichend kontrollieren könne.⁶ Die wesentliche Passage in dem Volkszählungsurteil bringt das Ziel und den Zweck des Datenschutzes als Freiheitsschutz auf den Punkt:⁷

»Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. [...]

5 BVerfG, Urteil v. 15.12.1983, 1 BvR 209/83, BVerfGE 65, 1, II. 1 a).

6 BVerfG, Urteil v. 15.12.1983, 1 BvR 209/83, BVerfGE 65, 1, II. 1 a).

7 BVerfG, Urteil v. 15.12.1983, 1 BvR 209/83, BVerfGE 65, 1, II. 1 a).

Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus.»

Die in dem Volkszählungsurteil zum Ausdruck gebrachten Grundsätze helfen auch heute noch, die Leitlinien des Datenschutzrechts zu verstehen und zu interpretieren. Für die Freiheitsrechte des Einzelnen sind die uns aus dem Datenschutzrecht vertrauten Grundsätze, beispielsweise Transparenz, Richtigkeit, Zweckbindung, essenziell. Auch in der betrieblichen Praxis hilft es immer wieder, sich diese Grundsätze zu vergegenwärtigen. Es wird dann klar, dass es beim Datenschutzrecht nicht um Kontrollrechte im Sinne eines erweiterten Eigentumsrechts geht. Vielmehr schützt die informationelle Selbstbestimmung die Freiheit des Einzelnen.

Diese Freiheit des Einzelnen ist nicht unbeschränkt und steht selbstverständlich im Spannungsverhältnis zu den Freiheitsrechten anderer, z. B. des Arbeitgebers. Der Einzelne ist eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit und hat deswegen kein Recht im Sinne einer absoluten Herrschaft über »seine« Daten. Information, auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann.⁸ Das Recht auf Schutz der personenbezogenen Daten muss im Hinblick auf diese gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden⁹.

Die DS-GVO baut auf dem Ansatz der von ihr abgelösten Datenschutzrichtlinie 95/46/EG auf. Sie hat den Anspruch, diesen Ansatz aus den Erfahrungen und der einschlägigen Rechtsprechung der letzten 20 Jahre heraus zu modernisieren. Die DS-GVO enthält eine Reihe neuer Elemente, die einerseits den Schutz der Rechte des Einzelnen stärken sollen, andererseits Unternehmen den Datentransfer im digitalen Binnenmarkt erleichtern werden. Durch

8 BVerfG, Urteil v. 15.12.1983, 1 BvR 209/83, BVerfGE 65, 1, II. 1 b)

9 Siehe Erwägungsgrund 4 der DS-GVO.

die DS-GVO werden die Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen (»Privacy by Design« und »Privacy by Default«) eingeführt, um Datenschutzinteressen von Anfang an in Geschäftsprozessen und Produkten, wie z.B. bei datenschützenden Voreinstellungen bei Smartphones, zu berücksichtigen. Die Rechte des Einzelnen werden gestärkt, indem neue Transparenzanforderungen eingeführt werden. Außerdem werden die Rechte auf Information, Zugang und Löschung ausgebaut. Einzelpersonen erhalten auch deswegen mehr Kontrolle über die sie betreffenden Daten. Zusätzlich wird das Recht auf Datenübertragbarkeit eingeführt, welches es den Betroffenen ermöglichen soll, von einem Unternehmen die Rück- oder Weiterübertragung personenbezogener Daten zu verlangen, die der Betroffene dem Unternehmen auf Grundlage einer Einwilligung oder eines Vertrages zur Verfügung gestellt hat. Mit der Verordnung erhalten alle Datenschutzaufsichtsbehörden die Befugnis, Geldbußen gegen Verantwortliche und Auftragsverarbeiter zu verhängen, wobei die Geldbußen bis zu 20 Millionen EUR oder bis zu 4 Prozent des weltweiten Jahresumsatzes betragen können. Zusätzlich können Betroffene bei Datenschutzverletzungen Schadenersatz auch für immateriellen Schaden einklagen. Die bislang bestehenden Vorabkontrollpflichten und Meldepflichten werden abgeschafft. Stattdessen gibt es ein für uns in Deutschland neues Instrument, das Risiko vor dem Beginn der Datenverarbeitung zu bewerten. Die Verordnung schreibt eine Datenschutz-Folgenabschätzung vor, wenn die Verarbeitung voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten des Einzelnen führen kann. Unternehmen müssen in diesem Fall vorab die Risiken identifizieren und Abhilfemaßnahmen zur Vermeidung der Risiken implementieren.

Die Verordnung gilt unmittelbar in allen Mitgliedsstaaten, die jedoch die Grundsätze und Bestimmungen der Verordnung in bestimmten Bereichen konkretisieren können. Für die betriebliche Datenschutzpraxis sind insbesondere die Fragen des Datenschutzes bei Beschäftigung und soziale Sicherheit praktisch relevant. Deutschland hat von diesen Konkretisierungsmöglichkeiten bereits Gebrauch gemacht und mit dem ebenfalls am 25.05.2018

in Kraft getretenen BDSG n.F. nationale Regelungen u. a. im Bereich des Beschäftigten-Datenschutzes geschaffen.¹⁰

Auch wenn deutschen Unternehmen viele Prinzipien und Regelungen aus der Datenschutz-Grundverordnung bereits aus der alten Rechtslage – basierend auf der Datenschutzrichtlinie – bekannt sein dürften, begann mit dem 25.05.2018 ein neues Zeitalter. Die bisherige Rechtsprechung der nationalen Gerichte sowie die Verwaltungspraxis der Aufsichtsbehörden der Länder in Deutschland können nicht einfach auf die Datenschutz-Grundverordnung angewendet werden. Da die Verordnung unmittelbar geltendes Europarecht ist, kann es nicht mit rangniedrigerem nationalem Recht ausgelegt werden. Nach der Übergangsphase, die am 25.05.2018 endete, beginnt nun eine Phase der praktischen und europaweiten Findung im europäischen Datenschutzrecht. Denn mit dem Bestreben, europaweit ein möglichst einheitliches Datenschutzregime zu schaffen, ist die Herausforderung verbunden, auch europaweit einheitliche Anwendungs- und Verwaltungspraktiken der Aufsichtsbehörden sicherzustellen. Die Verordnung sieht dazu förmliche Abstimmungsprozesse vor. Das wird seine Zeit benötigen. Deswegen kommen den Leitlinien und Arbeitsunterlagen der bisherigen Datenschutzgruppe nach Art. 29 der Datenschutzrichtlinie (sog. Artikel-29-Datenschutzgruppe) im Hinblick auf die Anwendung der Datenschutz-Grundverordnung besondere Bedeutung zu. Auch wenn es sich dabei um formal nicht bindende Leitlinien handelt, werden die Aufsichtsbehörden der Mitgliedstaaten die darin niedergelegten Grundsätze und Leitlinien bei der praktischen Anwendung der Datenschutz-Grundverordnung berücksichtigen. In der betrieblichen Praxis lohnt es also, mit den Leitlinien der Artikel-29-Datenschutzgruppe zu arbeiten.¹¹

Mit dem Wirksamwerden der Datenschutz-Grundverordnung am 25.05.2018 werden viele Unternehmen in Deutschland noch nicht im Einklang mit den Anforderungen der Verordnung stehen. Unternehmen sollten auch nach dem Startdatum weiterhin mit Hochdruck an der Umsetzung der Anforderungen arbeiten und die Fortschritte dokumentieren.

¹⁰ Bundesdatenschutzgesetz (BDSG) vom 30.06.2017, BGBl. I S. 2097.

¹¹ Die Unterlagen sind online verfügbar unter: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360&tpa_id=6936, letzter Zugriff: 12.03.2018.

2 Neue Aufgaben für HR-Fach- und Führungskräfte

Marco Ferme und Dr. Franziska von Kummer

2.1 Besonders betroffen von den neuen Regelungen: das Personalwesen

Die DS-GVO bringt zahlreiche neue Aufgaben und Verantwortlichkeiten mit sich, die nicht nur Personen an der Unternehmensspitze betreffen. Auch Fach- und Führungskräfte im HR-Bereich müssen eine Einhaltung der datenschutzrechtlichen Vorgaben gewährleisten. Da u.a. nach Art. 82 Abs. 2 DS-GVO auch natürliche Personen für Schäden haften, die durch eine nicht der Verordnung entsprechende Verarbeitung verursacht werden, ist jedem Entscheider, der mit personenbezogenen Daten zu tun hat (vgl. hierzu näher Kapitel 6.4), dringend anzuraten, sich mit den Rahmenbedingungen vertraut zu machen.

In der Praxis beobachten wir, dass die Risiken exorbitant hoher Bußgelder – bis zu 20 Mio. EUR bzw., wenn höher, bis zu 4 Prozent des globalen Umsatzes (Art. 83 Abs. 5 DS-GVO) – zwar bereits bekannt sind, sie aber eher als eine abstrakte Gefahr wahrgenommen werden. Die verbreitete Meinung, dass es sich bei der DS-GVO um ein Thema handelt, mit dem sich »andere« (gedacht wird hierbei an den Datenschutzbeauftragten) beschäftigen müssten, ist gefährlich. Tatsächlich ist auch der Personalbereich nicht davor gefeit, Bußgelder für das Unternehmen und daneben etwaige Schadensersatzforderungen auszulösen. Auch Personalverantwortliche sollten die Thematik daher nicht unterschätzen.

Gerade im Personalwesen sind viele Prozesse anfällig für Datenschutzverstöße – man denke nur an Recruiting oder auch die Überwachung von Mitarbeitern, wobei Letzteres gar nicht die berühmte Videoüberwachung, E-Mail-Kontrolle oder das Thema der Keylogger betreffen muss (zu aktuellen Entscheidungen hierzu vgl. Kapitel 12.3). Jedes Arbeitszeitkonto geht mit ei-

ner Datenverarbeitung einher; jedes Verfahren des Betrieblichen Eingliederungsmanagements (BEM) betrifft besonders sensible Daten. Auch darf man nicht annehmen, dass etwaige Datenverluste nur ein Problem sind, welches die IT zu klären hätte – so können beispielsweise der auf einer Dienstreise abhandengekommene Firmenlaptop oder das verlorene Diensthandy eine Reihe von Informationspflichten nach sich ziehen, wenn dort – wie eigentlich immer – personenbezogene Daten gespeichert sind. In solchen Fällen ist es wichtig, unverzüglich die notwendigen Maßnahmen zu ergreifen und zu beachten, dass binnen 72 Stunden eine Meldung an die Datenschutzbehörde zu erfolgen hat.

HR-Fach- und Führungskräfte sind in ihrem Bereich verantwortlich für die Anpassung von Strukturen und Prozessen und müssen verinnerlichen, dass sie jeden »Handschlag« unter datenschutzrechtlichen Gesichtspunkten analysieren und mögliche datenschutzrechtliche Folgen bedenken müssen.

Zunächst bedarf es dabei einer Bestandsaufnahme, wo eigentlich überall in welcher Form, auf welcher Grundlage und zu welchem Zweck personenbezogene Daten verarbeitet werden und wie der Zugriff auf diese Informationen überwacht und kontrolliert wird. Daraus lässt sich ableiten, in welchen Bereichen Handlungsbedarf besteht. Die besonders praxisrelevanten Themenfelder sollen nachstehend kurz angesprochen werden.

2.2 Sensibilität im Umgang mit Bewerberdaten

Im Umgang mit Bewerberdaten gilt es, die internen Recruiting-Prozesse kritisch mit Blick auf die DS-GVO-Compliance zu hinterfragen. Bei Bewerbungsvorgängen werden zahlreiche besonders geschützte personenbezogene Daten erhoben. Wer mit diesen Daten in Berührung kommt, muss daher dafür Sorge tragen, dass hierbei alles datenschutzkonform abläuft.

Das Problem ist dabei weniger die Frage einer wirksamen Einwilligung, denn der Bewerber übermittelt zunächst zahlreiche Daten von sich aus (vgl. jedoch zur Problematik der wirksamen Einwilligung im laufenden Beschäftigungsverhältnis Kapitel 7). Doch schwieriger wird es bereits dann, wenn Unternehmen zur Person des Bewerbers recherchieren und z.B. »Funds-

chen« auf Facebook mit dem Bewerberprofil verknüpfen. Auch ein Bewerberinterview über Skype ist datenschutzrechtlich bedenklich, zumal meist nicht einmal der Interviewer selbst weiß, wo entsprechende Daten gespeichert werden – nämlich nicht nur beim Unternehmen selbst und nicht nur im räumlichen Geltungsbereich der DS-GVO, sondern oftmals auch in Clouds und auf Servern, die sich beispielsweise auch in den USA befinden können. Doch auch das klassisch »analog« geführte Interview ist datenschutzrechtlich relevant, weil die an den Bewerber gerichteten Fragen ebenfalls zu einer Datenerhebung führen. Bei den so eingeholten Informationen sind ebenfalls die bereits am Anfang der DS-GVO stehenden Grundsätze der Zweckbindung (Art. 5 Abs. 1b) und Datenminimierung (Art. 5 Abs. 1c) einzuhalten. Hiernach sind Daten nicht auf Vorrat zu sammeln, sondern die Verwendungszwecke müssen von vornherein festgelegt, eindeutig und legitim sein. Ferner muss das Ausmaß der Verarbeitung personenbezogener Daten auf das für die Verarbeitungszwecke Notwendige beschränkt sein.

Unternehmen müssen in diesem Zusammenhang insbesondere offenlegen, welche persönlichen Daten zu welchem Zweck gespeichert und weitergegeben werden und wer Zugriff auf diese Informationen hat. Den Bewerbern stehen entsprechende Fragerechte zu. Ebenso ist zu überlegen, an welche Personen – nämlich möglichst wenige – Bewerberdaten zirkuliert werden, welche Fragen den Bewerbern zulässigerweise gestellt werden dürfen und wie nach Abschluss des Bewerbungsprozesses mit den Daten umzugehen ist.

Soweit im Unternehmen ein Bewerbermanagement-System genutzt wird, ist darauf zu achten, dass nur restriktive Zugriffe eingeräumt und etwaige automatisierte Prozesse kritisch hinterfragt werden. Von technischer Seite ist u. a. abzuklären, ob die von der Software vorgesehenen Verschlüsselungsstandards noch den neuen Anforderungen genügen. Etwa genutzte Cloud-Lösungen sind ebenfalls kritisch auf ihre Datenschutzkonformität zu hinterfragen. Soweit Anbieter (insbesondere EU-externe) sich das Recht einer eigenen Weiterverarbeitung vorbehalten, entspricht es nicht den Kriterien der DS-GVO, dem Anbieter durch Nutzung der Cloud-Lösung Zugriff auf die Daten zu ermöglichen.



Achtung

Werden Cloud-Lösungen genutzt, ist genau zu prüfen, ob die Nutzungsbedingungen des Anbieters ihrerseits den Anforderungen der DS-GVO entsprechen und ob bei dem Cloud-Anbieter und im Sitzland des Cloud-Anbieters ein ausreichendes Datenschutzniveau besteht (siehe dazu näher das Kapitel 16).

Die Grenzen der zulässigen Aufbewahrungsfristen sind ebenso zu beachten wie die Bindung an den Speicherungszweck. Hiernach ist der Zeitraum der Aufbewahrung beschränkt – eine Speicherung über die Dauer von mehr als einem halben Jahr ist auch mit Blick auf laufende AGG-Fristen (mögliche Diskriminierungsklagen, für die nach §15 Abs. 4 Satz 1 AGG eine zweimonatige Geltendmachungsfrist ab Zugang der Absage gilt) nicht zu rechtfertigen. Danach hat eine Löschung zu erfolgen, schon aufgrund der Vorgaben zur Datenminimierung. Bereits eine nicht ausreichende Löschung nach Abschluss des – für den Kandidaten erfolglosen – Bewerbungsprozesses kann Bußgelder auslösen. Und nicht erst die Erfahrungen mit dem AGG haben gezeigt, dass es durchaus Personen gibt, die zielgerichtet nach solchen Verstößen suchen. Dass eine datenschutzgerechte Vernichtung nicht vorliegt, wenn – überspitzt gesagt – die Bewerbungsunterlagen als Paket im Papierkorb entsorgt werden, versteht sich von selbst.

Auch der erfolgreiche Bewerber kann, bei strenger Betrachtung der Zweckbindung, bereits Lösungsansprüche haben, soweit Daten übermittelt wurden, die für die konkrete Beschäftigung nicht (mehr) erforderlich sind. Die Erforderlichkeit dürfte beispielsweise bei Schul- und Ausbildungszeugnissen und ggf. auch dem Bewerbungsanschreiben fehlen.

Für eine länger andauernde Speicherung ist das ausdrückliche Einverständnis des Bewerbers erforderlich, seine Daten in einem Kandidatenpool länger zu verwahren. Es ist daher sicherzustellen, dass bei Nichtvorliegen einer solchen Erklärung die Lösungsfristen beachtet werden und die Daten nicht auf irgendeinem Laufwerk »versickern«, auf welchem sie auch Jahre später noch zu finden sein werden. Zu denken ist dabei nicht nur an eine Compliance an sich, sondern auch an deren Nachweisbarkeit, sodass beispielsweise Prozesse entwickelt werden müssen, wie eine etwa angeforderte Datenlöschung (vgl. hierzu Kapitel 17.1) bewiesen werden kann.

Insgesamt müssen die Prozesse im Bereich Recruiting daher grundlegend überprüft und ggf. angepasst werden. Die Einführung und Vermittlung von datenschutzkonformen Standards schützt davor, dass zu viele Akteure »irgendwas« tun und dabei nicht auf Datenschutzkonformität achten.

2.3 Aufgaben im laufenden Beschäftigungsverhältnis

Auch über laufende Prozesse müssen sich Personalverantwortliche Gedanken machen. So gilt es insbesondere, die Grundlagen für Datenverarbeitungen im laufenden Beschäftigungsverhältnis einer kritischen Prüfung zu unterziehen. Zahlreiche Einwilligungserklärungen und auch Betriebsvereinbarungen, die in der Zeit vor Geltung der DS-GVO eine zulässige Grundlage für die Datenverarbeitung darstellten, genügen heute nicht mehr den Standards. Dies bedeutet nicht nur, dass etwa vorhandene Muster, die die Personalabteilung über die Zeit hinweg zusammengestellt hat, für die Zukunft angepasst werden müssen, sondern entzieht ggf. auch in bestehenden Beschäftigungsverhältnissen zahlreichen Datenverarbeitungsprozessen die Erlaubnisgrundlage.

Die DS-GVO legt zwar zugrunde, dass auch im Beschäftigungsverhältnis eine Einwilligung eine zulässige Grundlage für eine Datenverarbeitung darstellen kann – vielfach wird jedoch empfohlen, sich nicht allein auf diese Erlaubnisgrundlage zu verlassen. Sie ist fehleranfällig und u.U. nicht nachhaltig. Ersteres liegt bereits daran, dass die Einwilligung freiwillig erfolgen und auf informierter Grundlage erklärt werden muss. Fehler können hier dazu führen, dass die Freiwilligkeit infrage gestellt wird oder der Betroffene geltend macht, nicht über alle entscheidungserheblichen Informationen verfügt zu haben, als er die Einwilligung erteilte. Hauptaufgabe wird insoweit sein, die Arbeitsverträge entsprechend anzupassen und auf Klauseln zu verzichten, die die Einwilligungserklärung direkt mit der Vertragsunterzeichnung verknüpfen. Doch auch bei ordnungsgemäßer Vorbereitung und nicht zu beanstandender Einwilligungserklärung kann sich die jederzeitige Widerruflichkeit der Einwilligung als Problem darstellen. Datenverarbeitungen sollten daher nicht mehr ausschließlich auf dieser Grundlage erfolgen. Generell ergibt sich das Erfordernis, neue Einwilligungen einzuholen, wobei diese jeweils von dem Verwendungszweck abhängen und wegen des Gebots der

»informierten Einwilligung« (vgl. §26 Abs. 2 Satz 4 BDSG n.F.) die Erstellung der Vorlage einen gewissen Aufwand mit sich bringt.

Auch die in der Korrespondenz mit Beschäftigten genutzten Kommunikationsmedien sollten überprüft werden. So ist beispielsweise ein »üblicher« Austausch über WhatsApp genau besehen an den Maßstäben der Auftrags(daten)verarbeitung (vgl. näher dazu das Kapitel 13) zu messen und insbesondere dann heikel, wenn es den Gepflogenheiten in der Praxis des Beschäftigungsverhältnisses entspricht, dass hierüber u.a. Krankmeldungen übermittelt werden. Automatische Backups solcher und ähnlicher Messenger-Dienste, die unverschlüsselt in Clouds gespeichert werden, dürften nicht den Kriterien der DS-GVO entsprechen. Vor diesem Hintergrund sollten auch die Berührungspunkte des gelebten Beschäftigungsverhältnisses mit Diensten wie Facebook, Twitter oder Instagram – insbesondere bei Pflege von Unternehmensprofilen – auf ihre Datenschutzkonformität überprüft werden. In der Praxis empfiehlt sich außerdem – auch unter Berücksichtigung der zu erwartenden Vorgaben der zukünftigen ePrivacy-Verordnung – sich nicht noch stärkeren Restriktionen zu unterwerfen, indem die private Nutzung von betrieblichen Kommunikationsmitteln erlaubt wird.

Weiterhin sollten sich Personalverantwortliche damit vertraut machen, welche Betroffenenrechte es nach Art. 12 ff., 23 DS-GVO i.V.m. §§32 ff. BDSG n.F. gibt und wie auf entsprechende Anforderungen zu reagieren ist. Bestimmte Datenverarbeitungen, die durchaus verbreitet sind, können gerade unter Geltung der DS-GVO zu hinterfragen sein. Zu denken ist hier beispielsweise an eine auf einer »Alt-Einwilligung« beruhenden Veröffentlichung von Kontaktdaten und Profilbildern auf der Firmenwebsite, soweit es sich um Mitarbeiter handelt, die keine sog. Funktionsträger sind.

Für die Reaktion auf ein Verlangen auf Herausgabe bzw. Löschung von Daten gelten kurze Fristen. Die Praxis zeigt, dass solche Anfragen als unangenehm empfunden werden und bestenfalls erst einmal liegenbleiben, bis man vielleicht nach einigen Tagen die Rechtsabteilung oder den Datenschutzbeauftragten einbezieht. Hier gilt es, zeitnah umzudenken und entsprechenden Aufforderungen die gebotene Priorität beizumessen.

2.4 Aufgaben nach Beendigung des Beschäftigungsverhältnisses

Die Beendigung eines Beschäftigungsverhältnisses ist ebenfalls mit zahlreichen datenschutzrechtlichen Fragestellungen verbunden. Gerade bei einer weniger einvernehmlichen Beendigung dürften diejenigen Fälle, die mit unmittelbar geäußerten datenschutzrechtlichen Löschanforderungen einhergehen, zukünftig zunehmen. Die Umsetzung des »Rechts auf Vergessenwerden« (Art. 17 DS-GVO) erweist sich dabei als ausgesprochen schwierig. Je nach Daten ist zu differenzieren, inwieweit einer Aufforderung zur Löschung nachgekommen werden kann bzw. muss.

Um in diesem Kontext beurteilen zu können, welche datenschutzrechtlichen Pflichten bestehen, ist es wichtig, sich zu vergegenwärtigen,

- inwieweit personenbezogene Daten das Beschäftigungsverhältnis überdauern,
- zu welchen Zwecken sie gespeichert worden waren,
- ob ein Aufbewahrungsinteresse vom Speicherzweck gedeckt ist und
- welche Daten demgegenüber in welchem zeitlichen Abstand zur Beendigung des Anstellungsverhältnisses zu löschen sind.

Grundsätzlich entfällt der wesentliche Zweck der Speicherung mit Beendigung des Arbeitsverhältnisses. Anlässlich der Beendigung hat eine Bestandsanalyse zu erfolgen, wo überall Daten mit der Person des ausgeschiedenen Arbeitnehmers verknüpft sind und inwieweit diese auch ohne ausdrückliche Aufforderung zu löschen sind. Bei Bildern dürfte beispielsweise von einer automatischen Löschungspflicht auszugehen sein¹ und das Kunsturhebergesetz nicht (mehr) als Argument für eine Unwiderruflichkeit der Einwilligung ausreichen.

Als schwieriger erweist sich dabei der Umgang mit dem dienstlichen E-Mail-Konto, da sich der Arbeitgeber hier einerseits Löschanforderungen, andererseits Aufforderungen zur Herausgabe von Daten ausgesetzt sehen kann.

¹ So Fischer, NZA 2018, S. 8 (11).



Wichtig

Es empfiehlt sich, das E-Mail-Konto zunächst nur zu deaktivieren und zu sperren und mit Blick auf möglicherweise noch erfolgende Ansprüche auf Herausgabe von Daten vorerst nicht zu löschen, weil dies wiederum Schadensersatzpflichten auslösen könnte.

Eine automatische Weiterleitung aller an die E-Mail-Adresse eingehenden Nachrichten dürfte datenschutzrechtlich unzulässig sein, insbesondere wenn die private Nutzung des Postfachs faktisch geduldet ist.

Soweit dienstlich genutzte Arbeitsmittel abgegeben werden, sollte der Betroffene vorsorglich auf Löschungsmöglichkeiten (insbesondere bei Diensthandy und Laptop, aber z.B. auch beim Navigationssystem des privat genutzten Dienstwagens) hingewiesen werden.

Festzuhalten ist, dass einer Löschungsaufforderung jedenfalls zunächst nicht vollständig nachgekommen werden kann, was auch Art. 17 Abs. 3 DSGVO anerkennt, indem er u.a. die Geltendmachung/Ausübung/Verteidigung von Rechtsansprüchen als Einwand anerkennt. Ebenso ist eine fortgesetzte Speicherung unter Verweis auf rechtliche Verpflichtungen (zu denken ist hier beispielsweise an die zweijährigen Aufbewahrungsfristen für die über acht Stunden pro Tag hinausgehende Arbeitszeit oder für bestimmte Steuerunterlagen und Lohnabrechnungsunterlagen, die sechs Jahre aufzubewahren sind) ein Löschungshindernis.

Naturgemäß kann es hier noch keine Faustregeln geben; wichtig ist aber für Personalverantwortliche, eine entsprechende Sensibilität im Umgang mit Daten zu entwickeln und sich insbesondere in Konfliktfällen der Brisanz des Themas bewusst zu sein.

2.5 Zur Rolle des Betriebsrats

Personalverantwortliche müssen in datenschutzrechtlichen Fragen auch darauf achten, dass im Zusammenwirken mit dem Betriebsrat keine Rechtsverstöße begangen werden. Dies betrifft insbesondere die Verhandlung von Betriebsvereinbarungen, aber auch die Preisgabe von Daten an den Betriebsrat.