Katko

Checklisten zur Datenschutz-Grundverordnung (DS-GVO)

Checklisten zur Datenschutz-Grundverordnung (DS-GVO)

Implementieren, Mitigieren, Auditieren

Herausgegeben von

Dr. Peter Katko
Rechtsanwalt, Partner, licencié en droit, CIPP/E

Bearbeitet von

RAin Sina Biermann, LL.M.; RA Dr. Thomas Blickwedel; RA Daniel Kaiser;
RA Dr. Peter Katko; RAin Monika Menz; Dipl.-Jur. Eric Meyer, Dipl. iur. oec. (univ.);
Dipl.-Inf. Lutz Naake; RA Sebastian Rockstroh; RA Tobias Schall; Laureen Schuldt.

3. Auflage 2026

C.H.BECK

Zitiervorschlag: Katko Checklisten DS-GVO/Bearb. § … Rn. …

beck.de

ISBN PRINT 978 3 406 83847 7

© 2026 Verlag C.H. Beck oHG
Wilhelmstraße 9, 80801 München
info@beck.de
Druck und Bindung: Beltz Grafische Betriebe GmbH
Am Fliegerhorst 8, 99947 Bad Langensalza

Satz: Druckerei C.H.Beck Nördlingen
Umschlag: Martina Busch, Grafikdesign, Homburg Saar

chbeck.de/nachhaltig
produktsicherheit.beck.de

Gedruckt auf säurefreiem, alterungsbeständigem Papier
(hergestellt aus chlorfrei gebleichtem Zellstoff)

Alle urheberrechtlichen Nutzungsrechte bleiben vorbehalten.
Der Verlag behält sich auch das Recht vor, Vervielfältigungen dieses Werkes
zum Zwecke des Text and Data Mining vorzunehmen.

Vorwort zur 3. Auflage

Seit der 2. Auflage dieser Checklisten im Jahr 2023 hat sich in der Welt der digitalen Regulierung viel getan.

Lange Zeit war die DS-GVO die einzige wirklich praxisrelevante EU-Digital-Regulierung. Ein ganzes Bündel von weiteren Regelwerken ist mittlerweile hinzugekommen. Zuvörderst die EU KI-VO; wobei sowohl Training wie auch operative Nutzung der Künstlichen Intelligenz erhebliche DS-GVO Herausforderungen auslösen. Die EY-Law Kollegin Sina Biermann verfasst hierzu nun → § 13 „Künstliche Intelligenz und Datenschutz" – unter Berücksichtigung der Grundprinzipien der EU KI-VO. Wiederum der EU Data Act mit der Pflicht zum Verfügbarmachen von (ggf. auch personenbezogenen) vernetzten Produktdaten hat große Datenschutzrelevanz, die wir nunmehr auch mit diesen Checklisten adressieren. Sebastian Rockstroh ist Autor des neuen Kapitels → § 14 „EU Data Act und Datenschutz", in das er gleichermaßen Erfahrung aus Automobilindustrie wie Gesetzgebungsverfahren einbringt.

Dabei wird die „EU-Digital-Regelungsdichte" mittlerweile als so innovationshemmend gesehen, dass mit dem von der EU-Kommission Ende 2025 vorgestellten Digitalen Omnibus einiges schon wieder geändert werden soll. Positiv insofern, als dass dadurch für die DS-GVO sowie die neuen Cybersecurity-Regulierungen DORA, NIS2 und Cyber Resilience Act eine einheitliche Meldestelle für Sicherheitsvorfälle eingerichtet werden soll. Unter anderem diese Konsolidierung von Meldungen wird unser neuer EY Technology Risk-Autor Lutz Naake in → § 10 „Meldungen und Benachrichtigung von Sicherheitsvorfällen" darstellen. In der DS-GVO selbst soll durch den Digital Omnibus vor allem klargestellt werden, dass pseudonyme Daten bei Verantwortlichen, die keinen realistischen Zugriff auf den „Schlüssel" haben, als anonym gelten. Insofern würde ein maßgebliches Element der EuGH-Entscheidung C-413/23 P „SRB" dann auch normiert. Als weitere neue Autoren begrüßen wir die EY Law-Kollegen Dr. Thomas Blickwedel für das Kapitel→ § 4 „Rechtfertigung und Rechtmäßigkeit" und Laureen Schuldt mit dem Kapitel→ § 15 zur „Vorbereitung auf Untersuchungen durch Aufsichtsbehörden" als neues, sehr praxisrelevantes Thema.

Wieder bedanken wir uns beim Verlag C.H.BECK und Herrn Ulrich Pawlik für die verständnisvolle Unterstützung. Unser besonderer Dank gilt unseren wissenschaftlichen Mitarbeitern Constantin Kurzidem und Amelie Fichte für die jederzeit kompetente Hilfe.

Dr. Peter Katko

Vorwort der 1. Auflage

Die EU Datenschutz-Grundverordnung (DS-GVO) erwies sich als eines der komplexesten und umstrittensten Akte von EU Gesetzgebung. Unstrittig bedarf das Recht auf Privatheit und informationelle Selbstbestimmung gesetzlichen Schutzes. Ohne Zweifel werden durch die immer stärkere Rolle der Datennutzung in digitalen Prozessen und Geschäftsmodellen erhebliche Risiken für die personenbezogenen Daten jedes einzelnen gesetzt. Doch die Mitigierung dieser Risiken fand mit der DS-GVO verallgemeinernd für sämtliche Unternehmen und öffentliche Stellen statt. Resultat ist eine EU Verordnung mit 173 Erwägungsgründen und 99 Artikeln – und der äußerst fordernden Rechenschaftspflicht. Nicht zuletzt dieses Prinzip der Accountability ist auch der Auslöser für die Erarbeitung vorliegenden Werks. Denn Verantwortliche müssen fortan nachweisen, wie sie die Einhaltung des Datenschutzes sicherstellen. Die daraus resultierende Notwendigkeit der aktiven Implementierung von entsprechenden Maßnahmen fördert das Bedürfnis die Inhalte und Anforderungen der DS-GVO durch Checklisten besser abarbeitbar zu machen.

Im Sinn einer Fokussierung auf das praktisch Relevante haben wir diejenigen Teile der DS-GVO bewusst ausgelassen, die im Alltag der Datenschutzpraxis eher wenig bedeutsam sind. Somit eignen sich die Checklisten für das leichtere Verständnis der Inhalte der DS-GVO, aber insbesondere auch zur Überprüfung der konkreten Implementierung. Nutzer können somit auch die Verantwortlichen der operativen Fachbereiche in Unternehmen und Behörden sein – natürlich genauso wie Datenschutzbeauftragte sowie die Bereiche Interne Revision, Compliance und Recht.

Wir bedanken uns beim Verlag C.H.BECK und insbesondere Herrn Ulrich Pawlik, der unsere Arbeit vertrauensvoll begleitete und uns dieses Werk ermöglichte. Als Autorinnen und Autoren haben wir ein multidisziplinäres Team gewonnen mit umfassender rechtlicher und beraterischer Expertise in der operativen Datenschutzpraxis – wir danken für ihr Engagement. Wir bedanken uns auch bei den wissenschaftlichen Mitarbeitern Jonathan Hoffmann, Justus Helfrich und Aryan Chaprehari, die unsere Arbeit kompetent unterstützten, und bei unserer Assistentin Katharina Beitler, die uns stets wohlwollend zur Seite stand.

Dr. Peter Katko

Inhaltsverzeichnis

Vorwort zur 3. Auflage V
Vorwort der 1. Auflage VI
Abkürzungsverzeichnis XIII
Verzeichnis der (abgekürzt) zitierten Literatur XVII

§ 1. Einleitung 1

A. Zielsetzung und Handhabung der Checklisten 1
I. Ziele und Genese der DS-GVO 1
II. Die DS-GVO als EU–Verordnung 3
III. Öffnungsklauseln – Nationales Datenschutzrecht (BDSG) 3
IV. ePrivacy-Richtlinie 4
B. Die Auslegung der DS-GVO 4
C. Anwendbarkeit der DS-GVO 5

§ 2. Accountability: die Rechenschaftspflicht 7

A. Einführung 7
B. Erläuterungen zur Checkliste 7
I. Das Prinzip der Accountability 7
1. Explizite Verpflichtung zu Rechenschaft und Nachweis in Art. 5 DS-GVO und Art. 24 DS-GVO 7
2. Accountability als übergreifendes Prinzip der DS-GVO im Kontext von Managementprozessen 8
3. Accountability bezüglich der einzelnen Datenschutzgrundsätze gem. Art. 5 DS-GVO 10
II. Sicherstellung der Einhaltung der DS-GVO 12
1. Grundlagen der Sicherstellung 12
2. Vornahme geeigneter technischer und organisatorischer Maßnahmen (TOMs) und Datenschutzvorkehrungen 13
3. Risikobasierter Ansatz: Angemessenheit der Maßnahme 15
4. Komponenten der Konzeptionierung („Plan“) 16
5. Komponenten der Umsetzung („Do“) 19
III. Nachweis der Sicherstellung der Einhaltung der DS-GVO 22
1. Grundlagen zur Nachweispflicht 22
2. Risikobasierter Ansatz: Umfang der Nachweispflicht 23
3. Komponenten des Nachweises 24
IV. Überprüfungspflicht und Anpassung 26
1. Grundlagen der kontinuierlichen Verbesserung 26
2. Komponenten von Überprüfungspflicht und Anpassung („Check“ und „Act“) 28
V. Datenschutzmanagement und Datenschutzorganisation 32
1. Pflicht, ein Datenschutzmanagement zu etablieren und zu unterhalten . 32
2. Elemente eines Datenschutzmanagements und die Datenschutzorganisation 34
3. Komponenten entlang der 7 Elemente des Datenschutzmanagements nach IDW PS 980 n. F. (09.2022) 35
VI. Die Bestellung eines Datenschutzbeauftragten 38
1. Element der Accountability 38

2. Pflicht zur Bestellung des DSB 38
3. Materielle Anforderungen an die Bestellung des DSB 40
4. Anforderungen an den Status des DSB gem. Art. 38 DS-GVO 41
5. Die Aufgaben des DSB 43

§ 3. Der Kernprozess des Datenschutzes – neue Verarbeitungen erfassen, bewerten und überwachen 45

A. Einführung 45
B. Erläuterungen zur Checkliste 45
I. Rechenschaftspflicht (Accountability) und Datenschutz-Kernprozess 45
1. Die allgemeinen Anforderungen an die Implementierung 45
2. Anforderungen an einen Prozess, der sicherstellt, dass neue datenschutzrelevante Verarbeitungen und Projekte erfasst und bewertet werden 46
II. Die Verarbeitung personenbezogener Daten 47
1. Definition von personenbezogenen Daten 47
2. Verarbeitung personenbezogener Daten 48
III. Das Verarbeitungsverzeichnis als Kernstück der Datenschutz-Compliance . 52
1. Die Funktion des Verarbeitungsverzeichnisses 52
2. Das Verarbeitungsverzeichnis des Verantwortlichen 53
3. Das Verarbeitungsverzeichnis des Auftragsverarbeiters (Art. 32 Abs. 2 DS-GVO) 58
4. Weitere Anforderungen an das Verarbeitungsverzeichnis 60
IV. Die Datenschutz-Folgenabschätzung 61
1. Hohes Risiko als Voraussetzung für eine Datenschutz-Folgenabschätzung 61
2. Durchführung, Dokumentation und Methodik der Datenschutz-Folgenabschätzung 70
3. Einbindung von weiteren Akteuren und betroffenen Personen 73
4. Konsultation der Aufsichtsbehörde nach Art. 36 DS-GVO 74
5. Auditierung und Wirksamkeitsprüfung (Art. 35 Abs. 9 DS-GVO) 74
V. Privacy by Design and by Default – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO) .. 75
1. Grundlagen von Privacy by Design and Default 75
2. Privacy by Design (Art. 25 Abs. 1 DS-GVO) 76
3. Privacy by Default (Art. 25 Abs. 2 DS-GVO) 81
4. Zertifizierung von Privacy by Design und by Default 82

§ 4. Rechtfertigung und Rechtmäßigkeit der Verarbeitung personenbezogener Daten 85

A. Einführung 85
B. Erläuterungen zur Checkliste 86
I. Rechtfertigung einer Verarbeitung personenbezogener Daten 86
1. Rechtfertigung durch Einwilligung (Art. 6 Abs. 1 Buchst. a DS-GVO) 86
2. Rechtfertigung durch Vertragsabschluss und Erfüllung vorvertraglicher Maßnahmen (Art. 6 Abs. 1 Buchst. b DS-GVO) 98
3. Rechtfertigung durch Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 Buchst. c DS-GVO) 100
4. Rechtfertigung bei Verarbeitung personenbezogener Daten zum Schutz lebenswichtiger Interessen (Art. 6 Abs. 1 Buchst. d DS-GVO) 101
5. Rechtfertigung bei Verarbeitung personenbezogener Daten zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder zur Ausübung öffentlicher Gewalt (Art. 6 Abs. 1 Buchst. e DS-GVO) 101

6. Rechtfertigung aufgrund von berechtigten Interessen (Art. 6 Abs. 1 Buchst. f DS-GVO) ... 101
7. Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 Abs. 1 DS-GVO) ... 104
8. Personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DS-GVO) ... 106
II. Weitere Anforderungen an eine Verarbeitung personenbezogener Daten ... 108
1. Accountability iR.d konkreten Verarbeitung (Rechenschaftspflicht) ... 108
2. Die Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 DS-GVO) ... 108

§ 5. Die Information der betroffenen Personen ... 117

A. Einführung ... 117
B. Erläuterungen zur Checkliste ... 118
I. Vorüberlegungen ... 118
1. Gesetzliche Verantwortlichkeit für die Erteilung der Informationen nach Art. 13 DS-GVO und/oder Art. 14 DS-GVO ... 118
2. Durchführungsverantwortlichkeit für die Erteilung der Informationen nach Art. 13 DS-GVO und/oder Art. 14 DS-GVO im konkreten Fall ... 119
3. Ausnahmen von der Verpflichtung zur (konkreten) Informationserteilung an die betroffene Person ... 120
II. Ausgestaltung der Information der betroffenen Personen ... 130
1. Pflichtinhalte ... 130
2. Anforderungen an die Formulierung und Strukturierung der Pflichtinhalte ... 149
III. Anforderungen an die Implementierung ... 154
1. Zeitpunkt der Erteilung der Datenschutzinformationen ... 154
2. Darreichungsform der Datenschutzinformationen ... 158

§ 6. Auskunft ... 161

A. Einführung ... 161
B. Erläuterungen zur Checkliste ... 162
I. Organisatorische Anforderungen für die Auskunft ... 162
II. Formelle Anforderungen an die Antwort auf einen Antrag auf Auskunft ... 166
1. Form der Beantwortung ... 169
2. Kosten der Auskunft ... 169
III. Materielle Anforderungen an die Auskunft ... 169
1. Erste Stufe des Auskunftsersuchens – Positiv oder Negativattest ... 169
2. Zweite Stufe – Beantwortung des Auskunftsersuchens ... 170
IV. Grenzen der Auskunft ... 177

§ 7. Sonstige Betroffenenrechte ... 181

A. Einführung ... 181
B. Erläuterungen zur Checkliste ... 181
I. Recht auf Berichtigung ... 181
II. Recht auf Datenübertragbarkeit ... 188
1. Vom Recht auf Datenübertragbarkeit erfasste Verarbeitungen ... 188
2. Von der betroffenen Person bereitgestellte Daten ... 191
3. Format der zu übertragenden Daten ... 194

§ 8. Löschen von Daten ... 199
A. Einführung ... 199
B. Erläuterungen zur Checkliste ... 199
I. Speicherbegrenzung – Regelmäßiges Löschen ... 199
1. Löschkonzept ... 200
2. Unstrukturierte Daten ... 208
3. Löschverpflichtung bei Auftragsdatenverarbeitern ... 208
II. Das Betroffenenrecht auf Löschen und das Recht auf Vergessenwerden ... 208
§ 9. Die Sicherheit der Verarbeitung sowie technische und organisatorische Maßnahmen ... 215
A. Einführung ... 215
B. Erläuterungen zur Checkliste ... 216
I. Die Sicherheit der Verarbeitung nach Art. 32 DS-GVO ... 216
1. Allgemeines ... 216
2. Wurde ein Datensicherheitskonzept entwickelt? ... 229
3. Berechtigung – „Need-to-Know-Prinzip" ... 232
II. Praxishinweise für die Umsetzung ... 234
§ 10. Meldungen und Benachrichtigung von Sicherheitsvorfällen ... 237
A. Einführung ... 237
B. Erläuterungen zur Checkliste ... 237
I. Organisationspflichten des Verantwortlichen (Rechenschaftspflicht und Implementierung) ... 237
1. Allgemeine Anforderungen an die Implementierung ... 238
2. Risikoprognose ... 243
3. Besondere Anforderungen an die Implementierung ... 245
4. Dokumentationspflichten des Verantwortlichen nach Art. 33 Abs. 5 DS-GVO ... 253
II. Ausschlusstatbestände für die Benachrichtigung von betroffenen Personen (Art. 34 Abs. 3 DS-GVO) ... 255
C. Synergien der Meldepflichten regulatorischer Rahmenwerke ... 257
I. Ausgangspunkt und Zielrichtung ... 257
II. Gemeinsame Strukturelemente ... 257
III. Integrierter Meldeprozess im Security Operations Center ... 260
IV. Nationale Entwicklung und Bündelungstendenz ... 261
V. Beispiele zur praktischen Verzahnung ... 261
VI. Bewertung und Ausblick ... 262
§ 11. Auftragsverarbeitung und gemeinsame Verantwortlichkeit ... 265
A. Einführung ... 265
B. Erläuterungen zur Checkliste ... 266
I. Auftragsverarbeitung ... 266
1. Vorliegen einer Auftragsverarbeitung ... 267
2. (Vertrags-)Rechtliche Bindung des Auftragsverarbeiters in Bezug auf den Verantwortlichen ... 269
3. Implementierung von Kontroll- und Steuerungsmechanismen ... 285
II. Gemeinsame Verantwortlichkeit ... 288
1. Vorliegen einer gemeinsamen Verantwortlichkeit ... 289
2. Vereinbarung über die gemeinsame Verantwortlichkeit ... 293
3. Anforderungen an die Implementierung ... 300

§ 12. Drittlandtransfers 303
A. Einführung 303
B. Erläuterungen zur Checkliste 304
I. Vorliegen eines Drittlandtransfers 304
II. Zulässigkeit eines Drittlandtransfers 306
§ 13. Künstliche Intelligenz und Datenschutz 327
A. Einführung 327
B. Erläuterungen zur Checkliste 328
I. Vorliegen eines KI-Systems iSd KI-VO 329
II. Risikobasierte Klassifizierung von KI-Systemen 330
III. Phasen der Verarbeitung über den KI-Lebenszyklus 333
1. KI-Lebenszyklus 333
2. Datenschutzrechtliche Phasen der Verarbeitung 335
IV. Das Zusammenspiel der Verantwortlichkeiten unter der KI-VO und der DS-GVO 337
1. Verantwortliche Akteure nach der KI-VO 337
2. Datenschutzrechtliche Verantwortlichkeit 338
V. Rechtsgrundlagen iRd verschiedenen Verarbeitungsphasen 342
VI. Keine automatisierte Letztentscheidungen im Einzelfall mit Rechtswirkung nach Art. 22 DS–GVO 345
1. Allgemeines 345
2. Ausschließliche automatisierte Entscheidung im Einzelfall 346
3. Rechtliche Wirkung oder erhebliche Beeinträchtigung 348
4. Zulässigkeit automatisierter Entscheidungen 348
5. Angemessene Maßnahmen 350
6. Informationspflichten 352
7. DSFA 353
8. Sonderfall: Besondere Kategorien personenbezogener Daten 354
VII. Einsatz von KI-Anwendungen von Anbietern außerhalb der Europäischen Union 354
VIII. Sonstige allgemeine datenschutzrechtliche Vorgaben im Zusammenhang mit KI-Anwendungen 355
1. Datenschutz-Grundsätze 355
2. Data privacy by Design/Data privacy by default 356
3. Die DSFA als strategisches Instrument zur Risikobeherrschung 356
IX. Weitere Hinweise und aktuelle Entwicklungen 357
§ 14. Die Datenbereitstellungspflichten nach Art. 4 f. EU Data Act und die DS-GVO 359
A. Einführung 360
I. Hintergrund 360
II. Die Datenbereitstellung nach Art. 4, 5 DA 360
1. Dateninhaber 361
2. Nutzer 361
3. Dritter (Datenempfänger) 361
4. Ohne Weiteres verfügbare Daten 362
B. Erläuterung der Checkliste 363
I. Besondere datenschutzrechtliche Herausforderungen im Rahmen des Data Acts 363
1. Die Bereitstellung nach Art. 4 f. als Verarbeitung personenbezogener Daten 364
2. Was folgt daraus? 368

II. Prozessschritte DS-GVO im Kontext des Data Acts 369
1. Rollendefinition 369
2. Prüfung des Vorliegens einer Rechtsgrundlage 371
3. Nutzer 372
4. Dateninhaber 377
5. Dritter 384
6. Prüfung der Rechtsgrundlage des Nutzers oder des Dritten durch den Dateninhaber 385
7. Die Informations-/Transparenzpflichten 386

§ 15. Vorbereitung auf Untersuchungen durch Aufsichtsbehörden 389

A. Einführung 389
B. Erläuterungen zur Checkliste 391
I. Rechtsgrundlagen (Art. 58 DS-GVO) 391
1. Untersuchungsbefugnisse 391
2. Abhilfe- und Sanktionsbefugnisse 391
3. Genehmigungs- und Beratungsbefugnisse 392
II. Maßnahmen zur Vorbereitung 392
III. Reaktion und Maßnahmen im Fall von Datenschutzverstößen 397

Anhang: Zusammengefasste Checklisten 403

Sachverzeichnis 431