

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

RA Dr. Jan-Philipp Günther-Burmeister; RA Daniel Kaiser; RA Dr. Peter Katko;
RA Dr. Stefan Krüger; RAin Monika Menz; Dipl.-Jur. Eric Meyer, Dipl. iur. oec. (univ.);
RAin Ricarda Neukam, LL.M.; Ibrahim H. Sagdic; RA Tobias Schall

2. Auflage 2023



Zitervorschlag: Katko DS-GVO-Checklisten/Bearbeiter

www.beck.de

ISBN 978 3 406 79542 8

© 2023 Verlag C.H. Beck oHG

Wilhelmstraße 9, 80801 München

Druck: Beltz Grafische Betriebe GmbH

Am Fliegerhorst 8, 99947 Bad Langensalza

Satz: 3w+p GmbH, Rimpar

Umschlaggestaltung: Martina Busch, Grafikdesign, Homburg Saar



chbeck.de/nachhaltig

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

Vorwort des Herausgebers zur 2. Auflage

Seit der Erstauflage vorliegenden Werkes im Jahr 2020 haben sich in der Praxis von Datenschutz und DS-GVO eine Reihe von Änderungen durch Urteile und Leitlinien der Aufsichtsbehörden ergeben.

Heraus ragt das EuGH-Urteil zu „Schrems II“.¹ Neben der Unwirksamkeit des „Privacy Shield“ stellte der EuGH im Lichte möglicher Zugriffe durch US-Behörden auch strengere Anforderungen an den Datentransfer unter den EU-Standardvertragsklauseln als Mitigationsinstrument. Dies bedeutete erhebliche formelle und inhaltliche Prüfungsanforderungen für Datenexporteure. Durch die neue Executive Order von Präsident Joe Biden sowie das EU-US Data Privacy Framework wird dies nun relativiert.² Als Folge des Schrems II-Urteils hatte die EU-Kommission zudem neue Standardvertragsklauseln für den internationalen Datentransfer nach Art. 46 Abs. 2 Buchst. c DS-GVO (→ § 5 Rn. 131; → § 11 Rn. 40; → § 12 Rn. 24ff.), aber auch für Auftragsverarbeitungen nach Art. 28 Abs. 7 DS-GVO herausgegeben (→ § 11 Rn. 21; → § 12 Rn. 31).

Die Leitlinien des Europäischen Datenschutzausschusses zur gemeinsamen Verantwortlichkeit lassen die Dokumentationslast gleichermaßen ansteigen (→ § 11 Rn. 132ff.). In Bezug auf Betroffenenrechte hat der BGH klargestellt, dass das Recht auf Auskunft gem. Art. 15 DS-GVO wörtlich zu nehmen ist; in Bezug auf die Ansprüche gegen die dort beklagte Versicherung beinhaltete dies sowohl die Auskunft über die Daten als auch eine Kopie der verarbeiteten Daten (→ § 6 Rn. 2).³ Der EuGH wiederum stellte in Bezug auf die Österreichische Post klar, dass der Verantwortliche auch die einzelnen Empfänger von Daten nennen muss.⁴

Als neue Autoren begrüßen wir herzlich die EY Law-Kollegen Ricarda Neukam, LL.M für → § 4 „Rechtfertigung und Rechtmäßigkeit“ sowie Eric Meyer für → § 9 „Datensicherheit“ sowie → § 12 Drittlandtransfers. Schließlich hat Dr. Jan-Philipp Günther-Burmeister den gänzlich neuen → § 13 „Künstliche Intelligenz und Datenschutz“ verfasst. Die Hambacher Erklärung der Datenschutzkonferenz hatte die Kritikalität der Künstlichen Intelligenz schon mit Mitteln des Datenschutzes adressiert.⁵ Dass mittlerweile die EU-Kommission mit dem Artificial Intelligence Act einen reichlich komplexen Gesetzentwurf vorgelegt hat, unterstreicht die Notwendigkeit von regulatorischen Antworten.⁶

Wieder bedanken wir uns beim Verlag C.H.BECK und Herrn Ulrich Pawlik für die verständnisvolle Unterstützung. Unser besonderer Dank gilt unserem wissenschaftlichen Mitarbeiter Mattis Bieg für die jederzeit kompetente Hilfe.

Dr. Peter Katko

¹ EuGH NJW 2020, 2613 – Schrems II.

² Siehe die gemeinsame Presseerklärung „Gemeinsame Erklärung der Europäischen Kommission und der Vereinigten Staaten zum Transatlantischen Datenschutzrahmen“ vom 25.3.2022, https://ec.europa.eu/commission/presscorner/detail/de/ip_22_2087 (zuletzt abgerufen am 18.11.2022) bzw. <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/> (zuletzt abgerufen am 18.11.2022).

³ BGH ZD 2021, 581.

⁴ EuGH – C-154/21.

⁵ Datenschutzkonferenz, Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder Hambacher Schloss vom 3.4.2019 (Hambacher Erklärung zur Künstlichen Intelligenz).

⁶ European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, COM/2021/206 final.

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 des Herausgebers zur 2. Auflage	V
Abkürzungsverzeichnis	XIII
Verzeichnis der (abgekürzt) zitierten Literatur	XVII

§ 1. Einleitung

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

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	14
4. Komponenten der Konzeptionierung („Plan“)	15
5. Komponenten der Umsetzung („Do“)	19
III. Nachweis der Sicherstellung der Einhaltung der DS-GVO	21
1. Grundlagen zur Nachweispflicht	21
2. Risikobasierter Ansatz: Umfang der Nachweispflicht	22
3. Komponenten des Nachweises	23
IV. Überprüfungspflicht und Anpassung	25
1. Grundlagen der kontinuierlichen Verbesserung	25
2. Komponenten von Überprüfungspflicht und Anpassung („Check“ und „Act“)	27
V. Datenschutzmanagement und Datenschutzorganisation	30
1. Pflicht, ein Datenschutzmanagement zu etablieren und zu unterhalten	30
2. Elemente eines Datenschutzmanagements und die Datenschutzorganisation	32
3. Komponenten entlang der 7 Elemente des Datenschutzmanagements nach IDW PS 980	33
VI. Die Bestellung eines Datenschutzbeauftragten	36
1. Element der Accountability	36

2. Pflicht zur Bestellung des DSB	36
3. Materielle Anforderungen an die Bestellung des DSB	38
4. Anforderungen an den Status des DSB gem. Art. 38 DS-GVO	39
5. Die Aufgaben des DSB	40
§ 3. Der Kernprozess des Datenschutzes – neue Verarbeitungen erfassen, bewerten und überwachen	
A. Einführung	43
B. Erläuterungen zur Checkliste	43
I. Rechenschaftspflicht (Accountability) und Datenschutz-Kernprozess	43
1. Die allgemeinen Anforderungen an die Implementierung	43
2. Anforderungen an einen Prozess, der sicherstellt, dass neue datenschutzrelevante Verarbeitungen und Projekte erfasst und bewertet werden	44
II. Das Verarbeitungsverzeichnis als Kernstück der Datenschutz-Compliance	45
1. Die Funktion des Verarbeitungsverzeichnisses	45
2. Das Verarbeitungsverzeichnis des Verantwortlichen	46
3. Das Verarbeitungsverzeichnis des Auftragsverarbeiters (Art. 32 Abs. 2 DS-GVO)	51
4. Weitere Anforderungen an das Verarbeitungsverzeichnis	53
III. Die Datenschutz-Folgenabschätzung	53
1. Hohes Risiko als Voraussetzung für eine Datenschutz-Folgenabschätzung	54
2. Durchführung, Dokumentation und Methodik der Datenschutz-Folgenabschätzung	61
3. Einbindung von weiteren Akteuren und betroffenen Personen	63
4. Konsultation der Aufsichtsbehörde nach Art. 36 DS-GVO	64
5. Auditierung und Wirksamkeitsprüfung (Art. 35 Abs. 9 DS-GVO)	65
IV. Privacy by Design and by Default – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO)	65
1. Grundlagen von Privacy by Design and Default	66
2. Privacy by Design (Art. 25 Abs. 1 DS-GVO)	66
3. Privacy by Default (Art. 25 Abs. 2 DS-GVO)	71
4. Zertifizierung von Privacy by Design und by Default	72
§ 4. Rechtfertigung und Rechtmäßigkeit der Verarbeitung personenbezogener Daten	
A. Einführung	75
B. Erläuterungen zur Checkliste	76
I. Rechtfertigung einer Verarbeitung personenbezogener Daten	76
1. Rechtfertigung durch Einwilligung (Art. 6 Abs. 1 Buchst. a DS-GVO)	76
2. Rechtfertigung durch Vertragsabschluss und Erfüllung vorvertraglicher Maßnahmen (Art. 6 Abs. 1 Buchst. b DS-GVO)	87
3. Rechtfertigung durch Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 Buchst. c DS-GVO)	88
4. Rechtfertigung bei Verarbeitung personenbezogener Daten zum Schutz lebenswichtiger Interessen (Art. 6 Abs. 1 Buchst. d DS-GVO)	89
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)	89

6. Rechtfertigung aufgrund von berechtigten Interessen (Art. 6 Abs. 1 Buchst. f DS-GVO)	89
7. Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 Abs. 1 DS-GVO)	92
8. Personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DS-GVO)	93
II. Weitere Anforderungen an eine Verarbeitung personenbezogener Daten	95
1. Accountability im Rahmen der konkreten Verarbeitung (Rechenschaftspflicht)	95
2. Die Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 DS-GVO)	96
§ 5. Die Information der betroffenen Personen	
A. Einführung	1
B. Erläuterungen zur Checkliste	2
I. Vorüberlegungen	2
1. Gesetzliche Verantwortlichkeit für die Erteilung der Informationen nach Art. 13 DS-GVO und/oder Art. 14 DS-GVO	2
2. Durchführungsverantwortlichkeit für die Erteilung der Informationen nach Art. 13 DS-GVO und/oder Art. 14 DS-GVO im konkreten Fall	3
3. Ausnahmen von der Verpflichtung zur (konkreten) Informationserteilung an die betroffene Person	4
II. Ausgestaltung der Information der betroffenen Personen	13
1. Pflichtinhalte	13
2. Anforderungen an die Formulierung und Strukturierung der Pflichtinhalte	28
III. Anforderungen an die Implementierung	33
1. Zeitpunkt der Erteilung der Datenschutzinformationen	33
2. Darreichungsform der Datenschutzinformationen	36
§ 6. Auskunft	
A. Einführung	145
B. Erläuterungen zur Checkliste	146
I. Organisatorische Anforderungen für die Auskunft	146
II. Formelle Anforderungen an die Antwort auf einen Antrag auf Auskunft	150
1. Form der Beantwortung	152
2. Kosten der Auskunft	153
III. Materielle Anforderungen an die Auskunft	153
1. Erste Stufe des Auskunftersuchens – Positiv oder Negativattest	153
2. Zweite Stufe – Beantwortung des Auskunftersuchens	154
IV. Grenzen der Auskunft	160
§ 7. Sonstige Betroffenenrechte	
A. Einführung	163
B. Erläuterungen zur Checkliste	163
I. Recht auf Berichtigung	163
II. Recht auf Datenübertragbarkeit	169

§ 8. Löschen von Daten

A. Einführung	179
B. Erläuterungen zur Checkliste	180
I. Speicherbegrenzung – Regelmäßiges Löschen	180
II. Das Betroffenenrecht auf Löschen und das Recht auf Vergessenwerden	188

§ 9. Die Sicherheit der Verarbeitung sowie technische und organisatorische Maßnahmen

A. Einführung	195
B. Erläuterungen zur Checkliste	196
I. Die Sicherheit der Verarbeitung nach Art. 32 DS-GVO	196
1. Allgemeines	196
2. Wurde ein Datensicherheitskonzept entwickelt?	208
3. Berechtigung – „Need-to-Know-Prinzip“	210
II. Praxishinweise für die Umsetzung	212

§ 10. Meldungen und Benachrichtigung von Sicherheitsvorfällen

A. Einführung	215
B. Erläuterungen zur Checkliste	215
I. Organisationspflichten des Verantwortlichen (Rechenschaftspflicht und Implementierung)	215
1. Allgemeine Anforderungen an die Implementierung	216
2. Risikoprognose	219
3. Besondere Anforderungen an die Implementierung	222
4. Dokumentationspflichten des Verantwortlichen nach Art. 33 Abs. 5 DS-GVO	225
II. Ausschlussstatbestände für die Benachrichtigung von betroffenen Personen (Art. 34 Abs. 3 DS-GVO)	227

§ 11. Auftragsverarbeitung und gemeinsame Verantwortlichkeit

A. Einführung	1
B. Erläuterungen zur Checkliste	2
I. Auftragsverarbeitung	2
1. Vorliegen einer Auftragsverarbeitung	3
2. (Vertrags-)Rechtliche Bindung des Auftragsverarbeiters in Bezug auf den Verantwortlichen	4
3. Implementierung von Kontroll- und Steuerungsmechanismen	18
II. Gemeinsame Verantwortlichkeit	22
1. Vorliegen einer gemeinsamen Verantwortlichkeit	22
2. Vereinbarung über die gemeinsame Verantwortlichkeit	25
3. Anforderungen an die Implementierung	31

§ 12. Drittlandtransfers

A. Einführung	265
B. Erläuterungen zur Checkliste	266
I. Vorliegen eines Drittlandtransfers	266
II. Zulässigkeit eines Drittlandtransfers	268

§ 13 Künstliche Intelligenz und Datenschutz

A. Einführung	285
B. Erläuterungen zur Checkliste	286
I. Automatisierte Entscheidungen im Einzelfall nach Art. 22 DS-GVO	286
1. Allgemeines	286
2. Ausschließliche automatisierte Entscheidung im Einzelfall	286
3. Rechtliche Wirkung oder erhebliche Beeinträchtigung	288
4. Zulässigkeit automatisierter Entscheidungen	288
5. Angemessene Maßnahmen	290
6. Informationspflichten	291
7. DSFA	292
8. Sonderfall: Besondere Kategorien personenbezogener Daten	293
II. Sonstiger Einsatz von KI	294
III. Weitere Hinweise und aktuelle Entwicklungen	294
Anhang: Zusammengefasste Checklisten	297
Sachverzeichnis	329

