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

C.H.BECK

Zitiervorschlag: Katko DS-GVO-Checklisten/Bearbeiter

www.beck.de

ISBN 978 3 406 79542 8

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. 24 ff.), 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. 132 ff.). 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

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

§ 4. Rechtfertigung und Rechtmäßigkeit der Verarbeitung personenbezogener Daten

§ 5. Die Information der betroffenen Personen

§ 6. Auskunft

§ 7. Sonstige Betroffenenrechte

§ 8. Löschen von Daten

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

§ 10. Meldungen und Benachrichtigung von Sicherheitsvorfällen

§ 11. Auftragsverarbeitung und gemeinsame Verantwortlichkeit

§ 12. Drittlandtransfers

§ 13 Künstliche Intelligenz und Datenschutz