DATENSCHUTZ-
BERATER

Pachinger/Beham (Hrsg.)

Datenschutz-Audit

Recht – Organisation – Prozess – IT

Die Autoren:
Pachinger | Beham | Jost | Rusek | Jaksch | Rosinski

Der bewährte Praxisleitfaden nun auch speziell zum deutschen Recht

dfv Mediengruppe

Datenschutz-Berater

Datenschutz-Audit

Recht – Organisation – Prozess – IT

Pachinger/Beham (Hrsg.)

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

HINWEIS/DISCLAIMER:

Die Aufbereitung der einzelnen Kontrollbereiche, Kontrollgruppen und Kontrollen basiert auf den bisherigen Erfahrungen der Herausgeber und Autoren bei der Durchführung von Datenschutz-Audits nach der aktuellen Rechtslage. Die Methodik wurde in Anlehnung an Audits von Managementsystemen entwickelt. Die aus den Verpflichtungen der DSGVO „abgeleiteten" Kontrollen/Maßnahmen sind Möglichkeiten, die Erfüllung der Anforderungen der DSGVO und des BDSG nachzuweisen („Good Practice"). Keinesfalls wird damit gesagt, dass diese Kontrollen/Maßnahmen die ausschließlich relevanten bzw notwendigen sind, um die Erfüllung der Vorgaben der DSGVO und des DSG vollständig nachzuweisen; das vorliegende Werk stellt auch keine Rechts- oder Security-Beratung dar und ersetzt nicht die rechtliche Beratung im Einzelfall. Zu beachten ist daher, dass Datenschutz- und Aufsichtsbehörden oder auch Gerichte im Einzelfall andere oder weitere Nachweise verlangen können. Die Herausgeber und Autoren übernehmen daher keine Haftung für die korrekte Erfüllung von Vorgaben der DSGVO und des BDSG.

Bibliografische Information Der Deutschen Nationalbibliothek

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

ISBN 978-3-8005-1798-5

dfv Mediengruppe

Klimaneutraler Druck in Deutschland

www.ruw.de

Druck: WIRmachenDRUCK GmbH, Backnang

Printed in Germany

„Mit ihrem Werk ‚Datenschutz-Audit' ist den Autoren eine übersichtliche, nachvollziehbare und praxisnahe Darstellung zur Auditierung im Kontext der kommenden DS-GVO gelungen."[1]

Vorwort der Herausgeber und Autoren

Die Datenschutz-Grundverordnung (DSGVO), welche seit 25.5.2018 als einheitliches Regelwerk für die gesamte Europäische Union gilt, brachte gravierende Änderungen für Unternehmen mit sich. Diese lassen sich schlagwortartig in drei Hauptbereiche zusammenfassen: **erhöhte Selbstverantwortung** („Accountability") der Unternehmen und Organisationen beim Datenschutz, **Stärkung der Rechte** der betroffenen Personen und strengere **Vorgaben für Datensicherheit**.

Gleichzeitig erleben wir, dass Datenschutz heutzutage umfassend zu sehen ist und Unternehmen/Organisationen nicht nur in den zentralen Bereichen **Recht, Organisation, Prozess und IT** betrifft, sondern alle Bereiche durchdringt. Dies verlangt eine „ganzheitliche Datenschutzkultur" und eine strategische Integration in alle Geschäftsprozesse unter Berücksichtigung klarer Strukturierung, Priorisierung und Risikoorientierung.

Dieser ganzheitliche und interdisziplinäre Ansatz war Ausgangspunkt und Anstoß für das vorliegende Werk, welches in Österreich bereits in 3., vollständig überarbeiteter Auflage erschienen ist. Als Herausgeber und Autoren möchten wir aus unserer langjährigen Erfahrung und Praxis in den jeweiligen Fachbereichen zeigen, wie man die **Vorgaben der Datenschutz-Grundverordnung** (DSGVO) anhand klar definierter „Kontrollen" und „Maßnahmen" effizient umsetzt und dabei die Verarbeitung personenbezogener Daten im Unternehmen strukturiert, transparent gestaltet, koordiniert und zweckmäßig aufbereitet, um die Rechte von betroffenen Personen hinreichend zu wahren oder aber auch auf einen Datenvorfall vorbereitet zu sein; kurz, wie man einen **Datenschutz-Audit** durchführt, **nomen est omen**.

Unser Buch „Datenschutz-Audit" deckt – ganz im Sinne dieser ganzheitlichen Betrachtung des Themas Datenschutz – insbesondere die Bereiche Recht, Organisation, Prozess sowie IT ab und bietet **neuartig** eine **praktisch anwendbare Methodik**, um **Compliance im Datenschutz nachzuweisen** und **Audits durchzuführen**. Wesentlicher Bestandteil ist, die Vorgaben der DSGVO anhand umsetzbarer Kontrollen bzw Maßnahmen einzuhalten. Der komplexe Gesetzestext der **DSGVO** wird in **klar prüfbaren Kontrollen** dargestellt. Ein Unternehmen kann so seiner Selbstverantwortung zur Einhaltung der datenschutzrechtlichen Pflichten und zum Nachweis darüber nachkommen und somit im Worst Case das Risiko von Strafen bzw Sanktionen reduzieren. Die Kontrollen können auch von Auditoren unmittelbar

1 *Bernd Liedke*, ZD-Aktuell 2017, 04260, bereits zur 1. Auflage in Österreich.

zur Prüfung herangezogen werden. Das entwickelte Auditkonzept und die abgeleiteten Kontrollen sind angelehnt an Audits von Managementsystemen bzw bietet vergleichbare sowie reproduzierbare Auditergebnisse. Wir führen seit vielen Jahren Datenschutz-Audits in der Praxis durch und legen unsere Erfahrungen jetzt auf die DSGVO um.

Mit dem vorliegenden Werk wenden wir uns einerseits an all jene, die im Unternehmen bzw in Organisationen mit Datenverarbeitungen zu tun haben oder beim Aufbau eines Datenschutzmanagementsystems (DSMS) mitwirken bzw für die Einhaltung der DSGVO zuständig sind, andererseits aber auch an Auditoren. Das Konzept zum Datenschutz-Audit eignet sich erfahrungsgemäß vor allem auch als **Anleitung** zum **Aufbau** eines **DSMS** und möchte einen aktuellen **Praxisleitfaden** zur Einhaltung/Umsetzung der Pflichten und Vorgaben der **DSGVO** bieten, ganz im Sinne eines **„Code of practice"**.

Aufgrund des guten Feedbacks zu unserem Werk hatten wir schon sehr früh den Wunsch, unser Buch „Datenschutz-Audit" auch in Deutschland herauszubringen.

Die DSGVO gilt zwar unionsweit, enthält aber auch zahlreiche Öffnungsklauseln, die ergänzende Regelungen der Mitgliedstaaten ermöglichen oder notwendig machen. Darauf nehmen die Kontrollgruppen zum nationalen Datenschutzrecht Bezug. Um hier auch jene spezifischen Kontrollen darstellen zu können, die auf die deutsche Rechtslage bzw. spezifische Standardisierung abstellen, ist es uns gelungen, ausgewiesene Experten zu gewinnen.

Als Fachautoren für die deutsche Rechtslage fungieren:

Dr. *Christian Jaksch*, LL.M., arbeitet für den Konzerndatenschutzbeauftragten eines Automobilkonzerns und berät aktuell die neu geschaffene Organisationseinheit für die markenübergreifende Bündelung aller Aktivitäten zur Softwareentwicklung. Er ist Autor von mehreren Fachpublikationen zum Thema Datenschutz und seit 10 Jahren in diesem Bereich tätig.

Dipl.-Ing. (FH) *Arvid Rosinski*, Chief Information Security Officer in der Automobilindustrie, zertifizierter ISO 27001 Lead Auditor und Mitglied der ISACA.

Ein herzlicher Dank sei an dieser Stelle all jenen ausgesprochen, die zur Erstellung dieses Werkes beigetragen haben. Besonders danken wir unseren Autorenkollegen mit deutscher Expertise, die es uns ermöglichten, dieses Werk auch in Deutschland herauszubringen. Frau Manuela Hinterer sei für das Projektmanagement herzlich gedankt. Der Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft, insbesondere Herrn Orth, LL.M., danken wir für die Aufnahme ins Verlagsprogramm, die umsichtige Betreuung und das entgegengebrachte Verständnis.

September 2021 *Die Herausgeber und Autoren*

Vorwort von Jörg Asma

Die seit dem 25.5.2018 in der EU geltende Datenschutz-Grundverordnung hat eine einheitliche Linie für den Datenschutz verbindlich für die gesamte EU definiert. Die Schaffung und In Kraft Setzung dieses Regelwerks wird häufig sehr kontrovers zwischen den Anspruchsgruppen diskutiert. Unternehmen und Organisationen weisen insbesondere auf gestiegene Anforderungen, daraus resultierende höhere Kosten und komplexere organisatorische Maßnahmen hin.

Schaut man aber genau auf die Argumente der Kritiker, so wird sehr schnell klar, dass hier Grundprinzipien, wie insbesondere unser Recht auf informationelle Selbstbestimmung zur Diskussion gestellt werden und angesichts zunehmender Digitalisierung dem technischen Fortschritt geopfert werden sollen. Ja, mit wachsender Digitalisierung wird es zunehmend schwierig, das Recht auf Vergessen oder eine Beauskunftung umzusetzen. Gleichwohl sind dies aber Grundrechte europäischer Bürger und unsere Europäische Datenschutz-Grundverordnung kann gar nicht so falsch sein, wenn global diskutiert wird, ob die Forderungen der DSGVO nicht sogar weltweites Menschenrecht sein sollten.

Die aktuelle Corona--Pandemie bringt diesen Zwist zwischen Befürwortern und Gegnern der DSGVO sehr deutlich an den Tag: Die global entstehenden Corona-Apps werden zunächst in der guten Absicht erstellt, Kontaktketten zu identifizieren und unterbrechen zu können, was dem Wohl der Menschen in den jeweiligen Nationalstaaten zugutekommt. Gleichzeitig wurde der Ruf der Geheimdienste laut, diese Kontaktdaten und Kontaktketten auch für die nationalen Geheimdienste bereitzustellen. So wurden die Corona-Apps in einigen Ländern eher zu trojanischen Pferden, die nun auch der Überwachung der Bürger dient. Die Europäischen Staaten konnten weitestgehend dieser Versuchung widerstehen.

Für Organisationen und Unternehmen ist, wie man anhand dieser Tendenzen sehen kann, etwas sehr Gutes und vor allem Berechenbares entstanden: Ein Datenschutz, der nicht als zahnloses Papiertigerchen ein eher tristes Dasein fristet, sondern eine fundierte und berechenbare Grundlage, die auch über die Grenzen von Europa hinaus in rechtsstaatlichen Ländern bewundernd anerkannt wird. Unternehmen und Organisationen wissen sehr genau, dass sie sich auf einen einheitlichen Datenschutz innerhalb Europas verlassen können und keine unterschiedlichen Auslegungen fürchten müssen, die letztlich komplexitätstreibend sind.

Menschen in Europa können sich nun ebenso sicher sein, dass ihre Grundrechte nicht dem technischen Fortschrittswillen, dem Gewinnstreben von Organisationen und Unternehmen oder gar monopolistisch anmutenden

globalen Techgiganten geopfert werden, sondern ihre Rechte durchsetzen können.

Das vorliegende Buch ist eine praktische Hilfe für Organisationen und Unternehmen, den komplexen Gesetzestext der Datenschutz-Grundverordnung in eine sehr praktisch anwendbare Methode, nämlich abgeleitete Kontrollen und Maßnahmen, die auditierbar sind, abgeleitet zu bekommen.

Es gilt auch insbesondere der Grundsatz, dass alles, was ich prüfen kann, auch zum Aufbau dessen nutzen kann. So wendet sich das vorliegende Buch zwar vermeintlich an den Auditor, jedoch sollte das hierin beschriebene Kontrollsystem auch jedem als Grundlage dienen, der ein Datenschutzmanagementsystem aufbauen, verbessern oder betreiben möchte.

Das vorliegende Werk profitiert maßgeblich von den praktischen Erfahrungen der Autoren und der Anwendung dieser Kontrollen in den letzten drei Jahren, so dass eine Qualitätskontrolle und Verbesserung im Sinne eines stetigen Qualitätsregelkreises auch hier Anwendung gefunden haben.

Nutzen Sie die Chance, von den Erfahrungen der Autoren zu profitieren und ich hoffe, dass es für Sie als Leser zu Ihrer Standardlektüre für den Datenschutz wird.

Ein herzlicher Dank gebührt insbesondere allen, die an der Erstellung dieses Werkes mitgewirkt haben.

Jörg Asma

Partner PwC Deutschland, Cybersecurity & Privacy

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abs	Absatz
ACL	Access Control List
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
Art	Artikel (Artikelnennungen ohne nähere Angaben beziehen sich auf die DSGVO)
BDSG	Bundesdatenschutzgesetz
BIA	Business Impact Analyse
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs	Bundestagsdrucksache
BVwG	Bundesverwaltungsgericht
CMDB	Configuration Management Database
CNIL	Commission Nationale de l'Informatique et des Libertés
COBIT	Control Objectives for Information and Related Technology
COO	Chief Operating Officer
dh	das heißt
DPIA	Data Protection Impact Assessment
DS	Datenschutz
DSB	Datenschutzbeauftragter
DSFA	Datenschutz-Folgenabschätzung
DSG 2000	Datenschutzgesetz 2000 (Österreich)
DSG	Datenschutzgesetz (Österreich)
DSGVO	Datenschutz-Grundverordnung
DSMS	Datenschutzmanagementsystem
DSRL	Datenschutzrichtlinie (RL 95/46/EG)
ErwGr	Erwägungsgrund (Erwägungsgründe ohne nähere Angaben beziehen sich auf die DSGVO)
etc	et cetera
EU	Europäische Union
GAPP	Generally Accepted Privacy Principles
GDPR	General Data Protection Regulation
ggf	gegebenenfalls
GL	Geschäftsleitung
Hs	Halbsatz
IAPP	International Association of Privacy Professionals

iHv	in Höhe von
IKS	Internes Kontrollsystem
insb	insbesonders
ISAE	International Standards for Assurance Engagements
iSd	im Sinne des/der
ISO	International Organization for Standardization
ITIL	IT Infrastructure Library
KPI	Key Performance Indikatoren
KVP	Kontinuierlicher Verbesserungsprozess
LAN	Local Area Network
lit	litera/Buchstabe
MAC	Media-Access-Control
MS	Mitgliedstaat
NDA	Vertraulichkeitsvereinbarung, Geheimhaltungsvereinbarung
Nr	Nummer
OLA	Operational Level Agreement
PIA	Privacy Impact Assessment
PIMS	Privacy Information Management System
PMO	Project Management Office
ROPI	Recht, Organisation, Prozess, IT
RPO	Recovery Point Objective
RTO	Recovery Time Objective
S.	Seite
SAS	Statement on Auditing Standards
SLA	Service Level Agreements
TIA	Transfer Impact Assessment
TLS	Transport Layer Security
TOM	Technische und organisatorische Maßnahmen
vgl	vergleiche
VLAN	Virtual Local Area Network
wg	wegen
WLAN	Wireless Local Area Network
zB	zum Beispiel

Literaturverzeichnis

Das vorliegende Buch „Datenschutz-Audit“ verfolgt einen interdisziplinären Ansatz, nämlich die Kombination der „Kontrollbereiche“ Recht, Organisation, Prozess und IT, und beinhaltet Kontrollen/Maßnahmen, die aus den Vorgaben und Verpflichtungen der DSGVO abgeleitet wurden, wobei die Erfahrungen und das Wissen der Herausgeber und Autoren wesentlich mit eingeflossen sind. Aufgrund dieses Ansatzes wird auf ein ausführliches Literaturverzeichnis verzichtet. Einige den Herausgebern und Autoren wichtig erscheinende Werke werden im Folgenden dennoch angeführt.

CNIL (Commission Nationale de l’Informatique et des Libertés) (2015). Privacy Impact Assessment: Methodology (how to carry out a PIA), https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf (zuletzt abgerufen am 4.6.2021)

CNIL (Commission Nationale de l’Informatique et des Libertés) (2018). Privacy Impact Assessment: Tools (templates and knowledge bases), https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Tools.pdf (zuletzt abgerufen am 4.6.2021)

CNIL (Commission Nationale de l’Informatique et des Libertés) (2018). Measures for the Privacy Risk Treatment, https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-3-GoodPractices.pdf (zuletzt abgerufen am 4.6.2021)

Eßer/Kramer/v. Lewinski (Hrsg), DSGVO BDSG, 7. Auflage 2020

Gietl/Lobinger, Leitfaden für Qualitätsauditoren: Planung und Durchführung von Audits nach ISO 9001:2015, 6. Auflage 2019

Hinsch, Die neue ISO 9001: 2015 – Ein Praxis-Ratgeber für die Normenumstellung, 2015

ISO 19011: Leitfaden zur Auditierung von Managementsystemen, 2011

Jaksch, Datenschutzrechtliche Fragen des IT-gestützten Arbeitsplatzes – Grundrechtsschutz in einem Konzern vor dem Hintergrund neuer Technologien, 2020

Jaksch, Der Grundsatz der Zweckbindung und Zweckvereinbarkeit im Rahmen von Weiterverarbeitungen personenbezogener Daten, in: Jahnel (Hrsg), Jahrbuch Datenschutzrecht 2019, 2019, S. 141

Jaksch/Alt, Die Rolle des Datenschutzbeauftragten und der Datenschutz-Organisation bei der Implementierung des vernetzten Fahrzeuges, in: Roßnagel/Hornung (Hrsg), Grundrechtsschutz im Smart Car, 2019, S. 181

Jaksch/von Daacke, Datenschutzbeauftragter und Datenschutz-Organisation unter der DSGVO, DuD 12/2018, 758

Jaksch, Die Bestellungspflichten eines Datenschutzbeauftragten gemäß DSGVO, ZIIR 2/2017, 140

Karper, Datenschutzsiegel und Zertifizierungen nach der DSGVO, PinG Privacy in Germany 05.16, 201, http://www.pingdigital.de/PinG.05.2016.201 (zuletzt abgerufen am 4.6.2021)

Kramer, IT-Arbeitsrecht, 2. Auflage 2019

Kühling/Buchner (Hrsg), DS-GVO BDSG, 3. Auflage 2020

Pachinger, Auf dem schwierigen Weg zum „EU-Datenschutz", jusIT 2013/87, 181

Pachinger, DSGVO: Aus Zustimmung wird Einwilligung, ecolex 09/2017, 898

Pachinger, Zeit wird knapp: Sechs Monate bis zum neuen Datenschutz, Die Presse 2017/11/20

Pachinger, Datenschutzverträge, in: *Pachinger* (Hrsg), Datenschutz. Recht und Praxis, 2019, S. 153, 172 ff

Pachinger, KODEX Datenschutz, 5. Auflage 2021

Pachinger, Datenschutz-Verträge, Verantwortlicher – Auftragsverarbeiter – Joint Controller, 2021

White Paper Datenschutz-Folgenabschätzung des Forum Privatheit, https://www.forum-privatheit.de/wp-content/uploads/Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf, 3. Auflage, Nov 2017 (zuletzt abgerufen am 4.6.2021)

Leitlinien der Artikel-29-Datenschutzgruppe[1]

WP 242 rev.01, Leitlinie zum Recht auf Datenübertragbarkeit (13.12.2016).

WP 243 rev.01, Leitlinie in Bezug auf Datenschutzbeauftragte („DSB") (13.12.2016).

WP 244 rev.01, Leitlinie für die Bestimmung der federführenden Aufsichtsbehörde eines Verantwortlichen oder Auftragsverarbeiters (13.12.2016).

WP 248 rev.01, Leitlinien zur Datenschutz-Folgenabschätzungen (DFSA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt" (4.4.2017)

WP 250 rev. 01, Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679 (3.10.2017).

WP 251 rev.01, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679 (3.10.2017).

WP 253, Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679 (3.10.2017).

WP 259 rev. 01, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679 (28.11.2017).

1 Abgerufen unter www.dsb.gv.at (Stand 27.9.2021).

WP 260 rev. 01, Leitlinien für Transparenz gemäß der Verordnung 2016/679 (29.11.2017).

Guidelines European Data Protection Board[2]

Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation (25.5.2018).

Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679 (25.5.2018).

Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) (16.11.2018).

Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) (4.6.2019).

Leitlinien 1/2019 über Verhaltensregeln und Überwachungsstellen gemäß der Verordnung (EU) 2016/679 (4.6.2019).

Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects (8.10.2019).

Guidelines 3/2019 on processing of personal data through video devices (29.1.2020).

Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications (28.1.2020).

Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies (18.1.2020).

Leitlinien 3/2020 für die Verarbeitung von Gesundheitsdaten für wissenschaftliche Forschungszwecke im Zusammenhang mit dem COVID-19-Ausbruch (21.4.2020).

Leitlinien 04/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19 (21.4 2020).

Guidelines 05/2020 on consent under Regulation 2016/679 (4.5.2020).

Leitlinien 06/2020 zum Zusammenspiel zwischen der zweiten Zahlungsdiensterichtlinie und der DSGVO (15.10.2020).

Guidelines 07/2020 on the concepts of controller and processor in the GDPR (6.9.2020).

Guidelines 08/2020 on the targeting of social media users (7.9.2020).

Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679 (13.10.2020).

2 Abgerufen unter https://edpb.europa.eu/ (Stand 27.9.2021).

Guidelines 10/2020 on restrictions under Article 23 GDPR (18.12.2020).
Guidelines 01/2021 on Examples regarding Data Breach Notification (19.1.2021).
Guidelines 02/2021 on Virtual Voice Assistants (9.3.2021).
Guidelines 03/2021 on the application of Article 65(1)(a) GDPR (13.4.2021).
Guidelines 04/2021 on codes of conduct as tools for transfers (7.7.2021).

Autorenverzeichnis

Univ.-Lektor RA Dr. ***Michael M. Pachinger,*** CIPP/E

Dr. Michael M. Pachinger ist Rechtsanwalt und Partner bei Saxinger Chalupsky & Partner Rechtsanwälte GmbH (SCWP Schindhelm, Österreich) und neben dem allgemeinen Wirtschafts- und Unternehmensrecht seit mehr als 15 Jahren spezialisiert auf **Datenschutzrecht** (Data Protection Lawyer of the Year in Austria 2021, Corporate INTL, Global Law Experts) sowie **IP- & IT-Recht**. Er ist auch zugelassener European Trademark & Design Attorney. Als akkreditierter **EuroPriSe Certified European Privacy Expert** („CEPE L PS") unterstützt er bei der Begutachtung von IT-Produkten und webbasierten Dienstleistungen im Rahmen von Zertifizierungsverfahren zum Europäischen Datenschutz-Gütesiegel „EuroPriSe".

Zu seiner Expertise zählt ua die Beratung von Unternehmen, Universitäten und Organisationen in IT- und datenschutzrechtlichen Belangen, insbesondere die Formulierung von **Datenschutzverträgen**, der Aufbau sowie die regelmäßige Betreuung von **Datenschutz-Managementsystemen**, die Durchführung von **Daten-Due-Diligences** und **Datenschutz-Audits** sowie die Unterstützung bei der Ausübung der Rechte betroffener Personen. Bei der Vertragsgestaltung liegt sein Fokus vor allem auch auf der Beratung internationaler Mandanten in englischer, französischer und spanischer Sprache. Diese Expertise erlangte er mitunter durch seine Studien an den Universitäten Linz, Straßburg und Barcelona sowie seine mehrmonatigen Internships in renommierten Wirtschaftskanzleien in Frankreich und Spanien. So ist er seit 2012 auch bei der Pariser Anwaltskammer (Barreau de Paris) eingetragen und Mitglied des Ilustre Colegio de Abogados de Valencia.

Neben seiner anwaltlichen Tätigkeit ist Michael M. Pachinger **Lektor** an **Universitäten** und **Fachhochschulen**, lehrt an der **Anwaltsakademie** und ist Vortragender auf nationalen und internationalen Konferenzen. Pachinger ist Bearbeiter des KODEX Datenschutz sowie IP-/IT-Recht, Herausgeber und Autor des Handbuches „Datenschutz, Recht und Praxis" und publiziert laufend Beiträge zu aktuellen IT- und datenschutzrechtlichen Themen in nationalen und internationalen Zeitschriften. Als Mitglied der International Association of Privacy Professionals (IAPP) ist er nach dem einzigen weltweit anerkannten Datenschutz-Diplom, **Certified Information Privacy Professional** (CIPP/E), zertifiziert.

Georg Beham, MSc

Georg Beham arbeitet seit 1989 in der IT-Branche. Er ist **Gerichtssachverständiger**, IT-Sicherheit und Forensik. Georg Beham ist **Lektor** an mehreren Hochschulen und arbeitet seit über 15 Jahren in der Unternehmensberatung.

Er ist geschäftsführender Partner bei der internationalen Wirtschaftsprüfungs- und Beratungsgesellschaft PwC und leitet den Bereich Cybersecurity & Privacy in Österreich. Georg Beham unterstützt gemeinsam mit seinem Team Unternehmen dabei, ihre Daten zu schützen und für Cyberattacken gerüstet zu sein. Georg Beham implementiert seit 15 Jahren Managementsysteme nach ISO 27001. Die dort verwendete kontrollbasierende Methode wurde im Zuge vieler Kundenprojekte, unter anderem auch auf Datenschutzmanagement, übertragen.

Georg Beham ist Autor mehrerer Werke im Bereich Compliance, Informationssicherheit und Cloud Computing bzw Herausgeber des Fachbuches „EU-Datenschutzgrundverordnung – Praxiseinführung in 7 Schritten“. Des Weiteren ist er ISO 27001 Lead Auditor der Österreichischen Computer Gesellschaft (OCG) und verantwortlich für das gesamte Auditoren-Team und leitet den Lehrgang „Zertifizierter Informationssicherheitsauditor nach ISO/IEC 27001:2013“ an der Donau-Universität Krems.

Georg Beham hat einen Abschluss im Master-Lehrgang „Sichere Informationssysteme“ der Fachhochschule Hagenberg.

Dr. ***Christian Jaksch***, LL.M.

Dr. Christian Jaksch, LL.M. arbeitet für den Konzerndatenschutzbeauftragten eines Automobilkonzerns und berät aktuell die neu geschaffene Organisationseinheit für die markenübergreifende Bündelung aller Aktivitäten zur Softwareentwicklung im Konzern. Er beschäftigt sich insbesondere mit Fragen zur Fahrzeugdatenverarbeitung sowie der Implementierung von Datenschutz im Rahmen der Softwareentwicklung.

Dr. Christian Jaksch studierte Rechtswissenschaften mit Schwerpunkt Internationales Recht, anschließend Promotionsstudium (Universität Wien, Leibniz Universität Hannover) mit Promotion an der Universität Wien. Ergänzend absolvierte er einen Postgraduate-Master (LL.M.) im Informations- und Medienrecht. Er publiziert regelmäßig zu datenschutzrechtlichen Themen in deutschen und österreichischen Fachzeitschriften.

Thorsten Jost, CISM, ISO 27001 Lead Auditor

Thorsten Jost ist seit 1998 im IT- und Organisationsmanagement tätig und hat nach mehrjähriger Funktion als Konzernbeauftragter für Informationssicherheit (Group CISO) in einem internationalen Konzern 2012 das Beratungsunternehmen secriso Consulting (www.secriso.com) gegründet. Als Geschäftsführer der secriso Consulting GmbH berät er seit mehreren Jahren renommierte Unternehmen in Österreich und dem angrenzenden Ausland zu den Themen **Informations- und Cybersicherheit, Datenschutz** sowie **Risikomanagement**. Der Fokus liegt beim Aufbau von integrierten Managementsystemen für Informationssicherheit und Datenschutz sowie bei der Abwehr von Wirtschafts- und Industriespionage. Von seinem praxisbezogenen Wissen und seiner Erfahrung im Zusammenhang mit dem Aufbau von Datenschutzmanagementsystemen auf Basis der DSGVO profitieren bereits viele Unternehmen und Behörden.

Er führt des Weiteren IT-, Informationssicherheits- und Datenschutz-Audits und als Zertifizierungsauditor im Auftrag der Österreichischen Computergesellschaft (OCG) Zertifizierungen nach ISO/IEC 27001 durch. Seit 2020 ist er auch NISG-Prüfer im Rahmen der QuaSteV und auditiert Betreiber wesentlicher Dienste von kritischen Infrastrukturen. Thorsten Jost ist unter anderem **Lektor** an der **Donau-Universität Krems** für die Lehrgänge „Zertifizierter Informationssicherheitsmanager nach ISO/IEC 27001:2013“ und „Geprüfter Datenschutzmanager mit Universitätszertifikat“ sowie für den Universitätslehrgang „Datenschutz und Privacy“. Er ist Vortragender beim österreichischen Konferenz- und Seminaranbieter imh und bei diversen Fachkongressen. Als Landessprecher der IT-Security ExpertsGroup der Wirtschaftskammer Kärnten engagiert er sich für Informationssicherheit im Unternehmensumfeld.

Peter Kleebauer, MSc

Peter Kleebauer ist als Senior Manager bei der internationalen Wirtschaftsprüfungs- und Beratungsgesellschaft PwC tätig und leitet den Bereich Informationssicherheits- und Datenschutzmanagement. Nach seiner akademischen Ausbildung an der Fachhochschule Hagenberg in den Studien „Sichere Informationssysteme" und „Computer- und Mediensicherheit" ist er seit 13 Jahren in den Themenbereichen **Informationssicherheit, Datenschutz** und **Penetration Testing** beratend tätig. Er führt IT-Prüfungen und Benchmarking von IT-Abteilungen im Rahmen des COBIT und ISO 27001 Frameworks durch und unterstützt beim Aufbau von Managementsystemen für Informationssicherheit und Datenschutz, Business Continuity, Notfallmanagement und IT-Risikomanagement.

Als Nachweis für die Einhaltung von Informationssicherheits- und Datenschutzvorgaben erstellt Peter Kleebauer gemeinsam mit seinen Kunden nachweisbare, ISAE 3402- und **ISAE 3000-**konforme Datenschutzkontrollen und führt die Attestierung anhand dieser Vorgaben durch.

Peter Kleebauer ist des Weiteren wesentlich für die Erstellung der bei Grant Thornton International angewendeten Methode zur Umsetzung eines Datenschutzmanagementsystems und der damit verbundenen Ausbildung für die Anwendung dieser Methodik verantwortlich.

Darüber hinaus ist Peter Kleebauer für die Österreichische Computer Gesellschaft (OCG) als **ISO 27001 Lead Auditor** tätig und führt im Auftrag der OCG Zertifizierungen nach ISO 27001 durch.

Peter Kleebauer ist Mitglied der Österreichischen Arbeitsgruppe für Datenschutz (ASI-AG 001 18), der Österreichischen Arbeitsgruppe für die Erstellung eines österreichischen Standards zur Umsetzung eines Datenschutzmanagements beim Austrian Standards Institute, ist Lektor an der **Donau-Universität Krems** für den Lehrgang „Zertifizierter Informationssicherheitsauditor nach ISO/IEC 27001:2013" sowie Vortragender für „Betriebliche Datenschutzbeauftragte" am Berufsförderungsinstitut.

Arvid Rosinski

Nach einer Ausbildung zum Dipl.-Ing. (FH) im Maschinenbau arbeitete Arvid Rosinski in verschiedenen IT-Positionen. Das Thema Datenschutz begleitet seinen Werdegang seit langem, und aus seiner technischen Erfahrung heraus sind vor allem die technisch-organisatorischen Maßnahmen zum Schutz personenbezogener Daten ein stetiger Fokus seiner Arbeit. Er arbeitet derzeit als Chief Informationen Security Officer in der Automobilindustrie und hat in seiner beruflichen Laufbahn unter anderem Positionen im Consulting und der IT-Revision innegehabt. Er hält verschiedene Zertifizierungen, darunter zum ISO 27001 Lead Auditor und ist als Mitglied der ISACA zertifiziert als CISA, CISM und CRISC.

Erik Rusek, MSc

Erik Rusek ist als Senior Manager bei der internationalen Wirtschaftsprüfungs- und Beratungsgesellschaft PwC im Bereich Cybersecurity und Privacy tätig und fokussiert auf die Bereiche **Informationssicherheitsmanagement, Datenschutz** sowie **Awareness**. Darüber hinaus verantwortet er den Bereich **Security Culture & Change**.

Nach seiner Ausbildung an der Fachhochschule Oberösterreich am Campus Hagenberg war er in verschiedenen Unternehmen mit der Beratung und Attestierung von Klienten sowie dem **Betrieb** und der **Verbesserung** von **Informationssicherheits-** und **Datenschutzmanagementsystemen** betraut. Seit mehr als fünf Jahren ist Erik Rusek auf den **Faktor Mensch** in der Cybersecurity spezialisiert und unterstützt Klienten bei der umfassenden und nachhaltigen Sensibilisierung der Mitarbeiter. Zudem ist er noch Mitgründer und -entwickler einer Awareness-Trainingsplattform.

Darüber hinaus ist Erik Rusek zertifizierter Datenschutzbeauftragter und ISO/IEC 27001 Auditor. Er hält zudem Zertifikate für den Certified Ethical Hacker (CEHv8) sowie den Certified Information Security Manager (CISM).

FOTONACHWEISE:

Pachinger: SCWP Schindhelm • Beham: PwC • Jaksch: privat • Jost: privat • Kleebauer: PwC • Rosinski: privat • Rusek: PwC

1. Einführung

Datenschutz 2018 = Recht, Organisation, Prozess und IT[1]

Datenschutz ist heutzutage umfassend zu sehen und durchdringt Unternehmen[2] in den Bereichen Recht, Organisation, Prozess und IT. Dies hat Auswirkungen auf die gesamte Unternehmenskultur.[3]

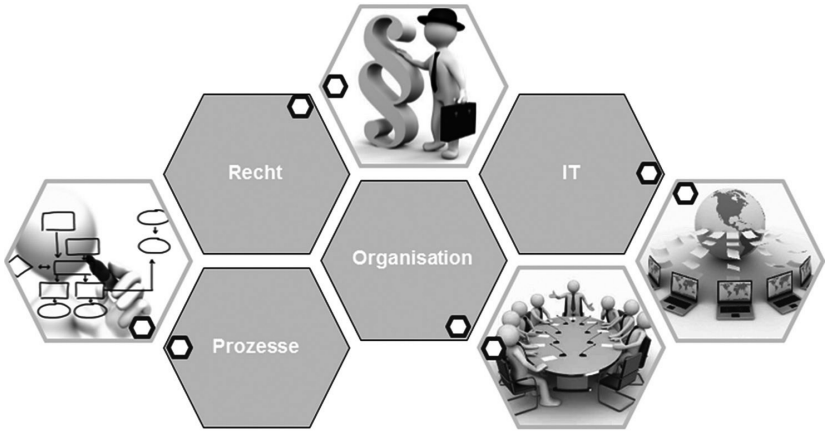

Abbildung 1: Tangierte Unternehmensbereiche

Es ist notwendig, die Verarbeitung personenbezogener Daten im Unternehmen strukturiert und transparent zu gestalten sowie koordiniert und zweckmäßig aufzubereiten, um für die Wahrung der Rechte von Betroffenen vorbereitet zu sein und Datensicherheit zu gewährleisten. Darüber hinaus ist Datenschutz in unserer Zeit vor allem auch unter dem Blickwinkel der Compliance zu betrachten.

Der Aufbau von Datenschutzmanagementsystemen (DSMS) und die Durchführung von regelmäßigen Datenschutz-Audits zur Überwachung der Erfüllung der gesetzlichen Vorgaben anhand klar definierter „Kontrollen" und „Maßnahmen" sind in Anbetracht der Datenschutz-Grundverordnung (DSGVO) unumgänglich. Die zahlreichen und oft komplexen neuen Pflichten bieten aber gerade jetzt auch die Möglichkeit, Prozesse, Organisations-

1 Auf diese Schlussfolgerung ließen sich die Vorbereitungen auf die seit 25.5.2018 geltende Datenschutz-Grundverordnung zusammenfassend und schlagwortartig bringen.
2 Wie auch Organisationen, Behörden und öffentliche Stellen.
3 Bildnachweis: secriso Consulting GmbH – *Thorsten Jost*, Nutzungsrecht für Teilgrafiken.

abläufe und IT-Anwendungen im Unternehmen proaktiv zu gestalten und damit Transparenz und (auch) Mehrwert zu schaffen. **Nutzen wir diese Chance und gestalten wir!**[4]

Compliance mit der DSGVO ist im ureigenen Unternehmensinteresse. Eine „Daten-Strategie" bzw ein sorgsamer Umgang mit personenbezogenen Daten verlangt einen permanenten Prozess, der in Zukunft notwendig und Kernelement jeder Unternehmensführung sein soll. Ziel eines DSMS ist, die Vorgaben der DSGVO fristgerecht und effizient umzusetzen. In weiterer Folge sollen datenschutzgerechte Services das Vertrauen in Dienstleistungen stärken, vorhandene Risiken absichern, Transparenz für betroffene Personen bieten und die Marktposition stärken.

Der Aufbau eines DSMS verlangt zunächst eine Evaluierung des IST-Standes („Daten-Due-Diligence"). Zweck dieser Bestandsaufnahme ist es, den notwendigen Gesamtüberblick und das essentielle Detailwissen über die einzelnen Datenverarbeitungen zu erlangen, welches für ein entsprechendes Datenschutz-Compliance-Projekt bzw ein Datenschutz-Audit erforderlich ist.

Der erste Schritt der Kontaktaufnahme und Involvierung der einzelnen Unternehmensbereiche wurde im Rahmen des IAPP Europe Data Protection Congress im November 2016 plakativ anhand des Beispiels Booking.com dargestellt:[5]

Involve the business:

1. Start with an easy department
2. Contact the manager of the department
3. Set up a meeting
4. Bring coffee
5. Walk your colleague through the questionnaire
6. Make your colleague the point of contact for the department
7. Set up a follow-up meeting
8. Be thankful, you will need them again

Das vorliegende Werk basiert auf dem aus unseren Erfahrungen in der täglichen Praxis erarbeiteten und bereits in zahlreichen Workshops erfolgreich umgesetzten Konzept der ganzheitlichen Beleuchtung des Themas Datenschutz und soll ein Praxisleitfaden für die Gestaltung im Unternehmen sein.

---

4 In Anlehnung an *Jyn Schultze-Melling*, LLM, Director for Privacy Policy Europe, Facebook Ireland, im Rahmen der Tagung der IAPP zur GDPR im Februar 2016.

5 *Caroline Hooper*, Legal & Privacy Counsel, Booking.com am 9.11.2016 im Rahmen des IAPP Europe Data Protection Congress 2016 in Brüssel.

Die einzelnen Kapitel wurden unter den Autoren nach ihren jeweils ausgewiesenen Spezialbereichen aufgeteilt. Die beiden Herausgeber fungieren auch als Autoren für die Einführung, den Kontrollbereich Recht und Kontrollbereich des nationalen Datenschutzrechts (*Michael M. Pachinger*) sowie Grundlagen eines Audits (*Georg Beham*). Die Kontrollbereiche Organisation und Prozess stammen von *Thorsten Jost*, der Kontrollbereich IT von *Peter Kleebauer* bzw *Erik Rusek*. Die Ausführungen zu den Kontrollbereichen als Basis für das Datenschutz-Audit wurden von Herausgebern und Autoren gemeinsam formuliert. Die Kontrollgruppen zum nationalen Datenschutzrecht mit jenen spezifischen Kontrollen, die auf die deutsche Rechtslage abstellen, wurden von *Christian Jaksch* und *Arvid Rosinski* verfasst.

1.1 Die Datenschutz-Grundverordnung (DSGVO)

Seitdem der Vorschlag für die Datenschutz-Grundverordnung (DSGVO) auf dem Tisch lag, wurde über das Thema Privatsphäre und Schutz der persönlichen Daten heftig diskutiert. In den letzten Jahren reichte die Bandbreite von kritischen Äußerungen zum Vorschlag über „demonstrative Schwarzmalerei" bis zum Datenschutz als „mögliches Opfer im Lobbykrieg". Aktuelle Ereignisse trugen außerdem dazu bei, dass Datenschutz seit geraumer Zeit beinahe in aller Munde ist.[6]

Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) wurde schließlich am 4.5.2016 im Amtsblatt der Europäischen Union veröffentlicht (L 119/1). Gemäß Art 99 ist diese Verordnung am 20. Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft getreten und gilt seit dem 25.5.2018.

Hingewiesen sei darauf, dass die DSGVO in zahlreichen Artikeln darauf verweist, dass Rechtsvorschriften der Mitgliedstaaten unberührt bleiben bzw die Mitgliedstaaten zusätzliche Bedingungen vorsehen könnten bzw müssen (sog Öffnungsklauseln).

6 Vgl dazu *Pachinger*, Auf dem schwierigen Weg zum „EU-Datenschutz", jusIT 2013/87, 181.

1.2 Accountability als Grundlage verpflichtender Datenschutz-Audits

Mit der DSGVO steigt die Selbstverantwortung der Unternehmen im Datenschutz erheblich. Wir sprechen von „Accountability" oder „Rechenschaftspflicht". Die Erfüllung der Pflichten ist durch den Verantwortlichen nachzuweisen, insbesondere durch genehmigte Verhaltensregeln oder Zertifizierungsverfahren (siehe Art 24 Abs 3 DSGVO). Ein eigener Artikel über Zertifizierung erwähnt datenschutzspezifische **Zertifizierungsverfahren** und **Datenschutzsiegel** bzw -prüfzeichen (Art 42 DSGVO).

Nachweispflichten finden sich in der DSGVO häufig und an verschiedensten Stellen:[7]

- Einhaltung der Datenschutzgrundsätze (Art 5 DSGVO)
- Wirksamkeit von Einwilligungen (Art 7 und 8 DSGVO)
- Datensicherheitsmaßnahmen (Art 24 und 32 DSGVO)
- Datenschutz durch Technik (Art 25 DSGVO)
- Auftragsverarbeitung (Art 28 DSGVO)

Können diese Nachweise nicht erbracht werden, droht das hohe Haftungs- und Sanktionsregime der DSGVO; demgegenüber kann die Einhaltung genehmigter Verhaltensregeln oder von Zertifizierungsverfahren bei der Verhängung von Geldbußen und deren Höhe gebührend berücksichtigt werden (Art 83 Abs 2 lit j DSGVO), sodass **Datenschutz-Audits** gem Art 40 und 42 DSGVO durchaus **Haftungsrisiken minimieren** können.[8]

Der (interne oder externe) **Datenschutzbeauftragte** wird vor diesem Hintergrund in Zukunft eine ganz zentrale Rolle einnehmen. Ihm kommt Schnittstellenfunktion im Unternehmen zu und er sorgt für eine regelmäßige Überwachung, ob das Unternehmen und insb die genannten Bereiche (Recht, Organisation, Prozess und IT) die geforderten Standards erfüllen („Auditierung"). Die Geschäftsleitung wird auf seine profunde Unterstützung angewiesen sein, denn erfolgreiche Unternehmensführung verlangt einen sorgsamen und transparenten Umgang mit Daten.

Haben Datenschutz und Datensicherheit schon in den letzten Jahren laufend an Bedeutung gewonnen, kommen jetzt neue Verpflichtungen hinzu. Datenschutz sollte dabei – wie erwähnt – nicht als „lästige Pflicht" gesehen, sondern auch als Möglichkeit zur Gestaltung und als Mehrwert für

7 Vgl *Karper*, Datenschutzsiegel und Zertifizierungen nach der DSGVO, PinG Privacy in Germany 05.16, 201.

8 Vgl *Karper*, Datenschutzsiegel und Zertifizierungen nach der DSGVO, PinG Privacy in Germany 05.16, 201.

Unternehmen selbst wahrgenommen und genutzt werden. Mit der korrekten Erfüllung der Pflicht zur Führung eines Verzeichnisses über Verarbeitungstätigkeiten kann etwa auch ein tiefer Einblick in das eigene Unternehmen gewonnen werden. Dies wiederum sollte auch zum eigenen Vorteil genutzt werden. Datenschutzgerechte Services und deren Nachweis durch entsprechende Audits können wiederum das Vertrauen in die Dienstleistungen des Unternehmens stärken, vorhandene Risiken absichern, Transparenz bieten und die Marktposition verbessern.

Das vorliegende Werk verfolgt das Ziel, die Arbeit im Rahmen von Datenschutz-Audits und Zertifizierungsverfahren entscheidend zu unterstützen.

1.3 Das deutsche Datenschutzrecht

Die in diesem Buch dargestellten Verpflichtungen und Kontrollen wurden von der Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO) abgeleitet. Daher werden auch die Begriffe und Formulierungen der DSGVO (zB Verantwortlicher, Auftragsverarbeiter etc) hier umfassend verwendet.

Die Darstellung des nationalen Datenschutzrechts beschränkt sich auf die Anforderungen für nicht-öffentliche Stellen. Diese werden in § 2 Abs 4 BDSG definiert:

> *„Nichtöffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts* (…)*. Nimmt eine nichtöffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes."* (§ 2 Abs 4 BDSG). Gemäß der Erläuterung der Deutschen Datenschutzkonferenz sind unter *„dem Begriff der „nicht-öffentliche Stellen"* (…) *natürliche Personen, juristische Personen des Privatrechts unabhängig von ihrer Rechtsform und der Art ihrer Betätigung, z. B. eingetragene Vereine, Genossenschaften, Kapital-und Personengesellschaften des Privatrechts (z. B. GmbH, AG, OHG, KG, GmbH und Co. KG, GbR), und andere privatrechtlich organisierte Personenvereinigungen (z. B. Genossenschaften, nichteingetragene Vereine, Gewerkschaften, Parteien, Berufsverbände, Gruppierungen ohne Rechtspersönlichkeit) zu verstehen."*[9]

Seit 25.5.2018 gilt nun die DSGVO. Die erste Anpassung des deutschen Datenschutzrechts (Bundesdatenschutzgesetz – BDSG) an die DSGVO erfolgte mit dem DSAnpUG-EU (BGBl I 2017, S. 2097)[10]. Die zweite Anpassung

9 *Datenschutzkonferenz*, Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen (2020), S. 1, https://www.datenschutzkonferenz-online.de/media/oh/20200903_oh_v%C3%BC_dsk.pdf (zuletzt abgerufen am 4.6.2021).

10 Gesetz vom 30.6.2017 – BGBl I 2017, Nr 44 v. 5.7.2017, S. 2097.