Verzeichnis von Verarbeitungstätigkeiten

Praxishandbuch für Verantwortliche zur praktischen Umsetzung aus rechtlicher, organisatorischer und technischer Sicht

von

Heiko Roth, LL.M.

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Alle im Buch verwendeten Begriffe verstehen sich geschlechterneutral. Aus Gründen der besseren Lesbarkeit wird teilweise auf eine geschlechtsspezifische Differenzierung verzichtet – entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat lediglich redaktionelle Gründe und beinhaltet keine Wertung.

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 ISBN 978-3-8005-1875-3

dfv Mediengruppe

www.ruw.de

Satzkonvertierung: Lichtsatz Michael Glaese GmbH, 69502 Hemsbach

Druck und Verarbeitung: Beltz Grafische Betriebe GmbH, 99947 Bad Langensalza

Der Autor sagt „Moin“ – wichtige Leitsätze zum Umgang mit und zu den Zielen des Praxishandbuchs

Moin.

Für uns Datenschutzbeauftragte und DatenschutzberaterInnen ist es das „täglich Brot“, Verantwortliche bei der Erfüllung ihrer vielseitigen Organisationspflichten bestmöglich zu unterstützen. Anders als noch zu Zeiten der EG-Datenschutz-Richtlinie begegnen uns seit Inkrafttreten der DSGVO täglich neue Informationen aus der gesamten EU, die wir für unsere Beratungs- und Überwachungsaufgaben nutzen können und müssen. Die laufende Fortschreibung des EU-Datenwirtschaftsrechts bewirkt ihr übriges.

An dieser Stelle darf jede Leserin und jeder Leser dieses Vorworts mit Recht fragen: Warum dann noch ein Buch mit mehreren Hundert Textseiten zum Datenschutz? Kurzum: Weil es nötig ist. Obwohl die DSGVO dutzende Pflichten für Verantwortliche und Rechte für betroffene Personen mit sich bringen, erfreuten sich zuletzt nur wenige dieser Pflichten einer überragenden publizistischen Popularität. Man denke etwa an die Interpretation der Umsetzung des Auskunftsrechts.

Konträr dazu fristen andere Organisationspflichten in der Literatur eher ein Schattendasein. Artikel 30 DSGVO gehört zu dieser eher verschmähten Gattung im Pflichtenheft des Verantwortlichen. Er verpflichtet den Verantwortlichen zur „Führung“ eines „Verzeichnisses von Verarbeitungstätigkeiten“.

Praktisch ist dieses Verzeichnis im operativen Datenschutzmanagement oft ein wichtiger Träger, auf den sich andere Pflichten aus der DSGVO stützen oder mit dem sie verbunden sind. Bei der der täglichen Beschäftigung und Übung mit diesem Verzeichnis begegnen dem Anwender eine Vielzahl praktischer, aber eben auch ganz grundlegende dogmatische Fragen des Datenschutzes. Beispiele: Was genau ist eine „Verarbeitung“? Wie lege ich einen tauglichen „Zweck“ fest? Wo bestehen Unterschiede zwischen einer „Verarbeitungstätigkeit“ und einem „Geschäftsprozess“? Welchen „Reifegrad“ sollen die einzelnen Prozesse hinter dem VVT aufweisen?

Diese Arbeit hat zum Ziel, die verschiedenen Inhalte, die Strukturen, das Potenzial, aber auch die Herausforderungen dieser eher im Verborgenen blühende Pflicht aufzuzeigen. Auch soll durch die Arbeit die wiederkehrende Frage beantwortet werden: „Wie machen es denn andere?“ Und weiter, von besonderem Interesse für Beauftragte und BeraterInnen in Konzer-

nen: „Welche Anforderungen ergeben sich aus der Rechtslage und der Rechtspraxis anderer Staaten innerhalb und außerhalb der EU/EWR?“

Um diese Ziele zu erreichen, wurden mehrere Hundert Quellen ausgewertet. Der Großteil der Quellen datiert ab 2016. Ich habe darauf geachtet, dass die Mehrzahl der Quellen öffentlich frei verfügbar ist und damit zum Nachlesen abgerufen werden kann. Diese Quellenauswahl soll auch zeigen, wie einfach es sein kann, an öffentliche Informationen zum Datenschutzrecht und zum Datenschutzmanagement zu gelangen. Zurückgegriffen wurde auf Quellen aus der EU, dem EWR und darüber hinaus.

Das Werk ist primär als „Praxishandbuch“ konzipiert. Es wird mit vielen praktischen Einzelbeispielen gearbeitet. Im Umgang mit den Beispielen werden „rote Linien“ gezeichnet, Fragen aufgeworfen sowie kommentiert, um neue Impulse zu liefern. Manchmal stehen die Beispiele auch nur für sich und überlassen dem Anwender die weitere Bewertung. Wo es zur Schwerpunktsetzung geboten war, wurde analytisch „tiefer gebohrt“, um allen sich zeigenden Facetten auf den Grund zu gehen.

Als Autor erhebe ich nicht den Anspruch, sämtliche Informationsquellen innerhalb der EU/EWR seit 2016 mit Bedeutung für die Führung des VVT gefunden, gelesen, analysiert und in dieses Buch eingearbeitet zu haben. Dennoch habe ich versucht, das Praxishandbuch so „europäisch“ wie möglich zu halten, d.h. nicht nur eine marginale Zahl an Fundstellen abseits von Deutschland einzuarbeiten. Zur Erinnerung: Art. 30 DSGVO zählt zum Sekundärrecht der EU.

Wo es im Einzelfall unbedingt geboten war, habe ich die Erörterung spezifischer Rechtsfragen im deutschen Recht zugelassen (z. B. zum kollektiven Arbeitsrecht). Im Übrigen thematisieren die aus Deutschland stammenden Quellen Fragen, die auch abseits von Deutschland für die Handhabe des Art. 30 DSGVO von Relevanz sind. Auch Tendenzen und Umsetzungen in Staaten außerhalb der EU/EWR habe ich berücksichtigt, da die Pflicht zur Führung des VVT heute in vielen Rechtsordnungen und der damit verbundenen Rechtspraxis Einzug gefunden hat.

Metriken und Statistiken zum Quellenapparat finden sich am Ende dieses Buches (Quellenverzeichnis).

Wichtig für die Handhabe des Buches:

– Jede Leserin und jeder Leser sollte sich vor der Lektüre des Praxishandbuchs von dem Gedanken lösen, dass es „das“ Verzeichnis von Verarbeitungstätigkeiten gibt oder dass mit diesem Praxishandbuch „die“ Muster-Prozesse zur Umsetzung wiedergegeben werden. Die Umsetzung des

Art. 30 DSGVO erfolgt in jeder Organisation individuell und ist von den dortigen Gegebenheiten abhängig, die sich auch mit der Zeit ändern können.

- Beispiele: Nicht jede Organisation hat einen Betriebsrat, dessen Funktion in einem VVT-Prozess und dessen Workflow berücksichtigt werden müsste. Nicht jede Organisation kann ein Datenschutzmanagementsystem (DSMS) mit verschiedenen Rollen vorweisen. Nicht jede Organisation setzt auf Binding Corporate Rules, unterliegt einem Code of Conduct, verknüpft ihr DSMS mit einem ISMS oder arbeitet mit (Leistungs-) Kennzahlen.
- Deswegen sollte sich auch keine Leserin und kein Leser von den vielen Details und Hinweisen „erschlagen“ fühlen, die dieses Praxishandbuch bereithält. Picken Sie sich die Punkte heraus, die Sie in der Umsetzung besonders interessieren! – z. B. als langjährige Berater und DSB, die ihr Wissen gezielt auf den aktuellen Stand bringen wollen; als Dogmatiker, die sich fragen, was der Unterschied zwischen „Verarbeitung“ und „Verarbeitungstätigkeit“ ist; als Risikomanager, die Prüfungsschwerpunkte der Behörden erkennen möchten; als Auditoren, die sich für Prozess-Reifegrade im DSMS interessieren; … – oder lesen Sie das Buch als interessierter Berufsanfänger oder Quereinsteiger von Beginn bis zum Ende, um einen Überblick zu all den denkbaren Verästelungen in der Umsetzung des Art. 30 DSGVO zu erhalten.

Ich wünsche allen Leserinnen und Lesern viel Freude beim Studium dieses Buches – und vor allem den ein oder anderen hilfreichen Gedankenanstoß für die tägliche Arbeit. Über konstruktives Feedback freut sich der Autor jederzeit via Mail: feedback-vvt@proton.me

Nordische Grüße

Heiko Roth

Disclaimer: Das vorliegende Werk spiegelt ausschließlich die private Meinung des Autors wider und nicht die seines Arbeitgebers. Mit dem Werk erbringt der Autor keine Rechtsdienstleistung im Sinne des Rechtsdienstleistungsgesetzes (RDG).

Inhaltsverzeichnis