

# DATENSCHUTZ- BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

**Chefredakteur: Dr. Carlo Piltz**

**Schriftleitung: Prof. Dr. Alexander Golland, Tilman Herbrich, Philipp Quiel, Laurenz Strassemeyer**

## Editorial

---

Dr. Carlo Piltz

**Gibt es etwas Neues zur Aufbewahrungsdauer von Bewerberdaten?**

Seite 101

## Stichwort des Monats

---

Sascha Kremer

**GmbH und Geschäftsführer: Allein, gemeinsam, nebeneinander Verantwortliche?**

Seite 102

## Datenschutz im Fokus

---

Dr. Moritz Holm-Hadulla, Dr. Hannah Bug und Nora Johanna Pollmeier

**Der Kommissionsentwurf des Data Acts – Ein Überblick**

Seite 108

Bernadette Bucheli und Dr. David Vasella

**Das revidierte schweizerische Datenschutzrecht: Hinweise für ausländische Unternehmen**

Seite 112

## Aktuelles aus den Aufsichtsbehörden

---

Tilman Herbrich und Domenic Trybull

**Ergänzung zur DSK Orientierungshilfe Telemedien: FAQs zu Cookies und Tracking**

Seite 115

## Rechtsprechung

---

Peter Hense und Dr. Franziska Wahedi

**Unterlassungsanspruch des Eigentümers gegen die Installation einer Überwachungs-App durch Dritte**

Seite 119

Dr. Dominik Sorber

**BAG bestätigt einschränkende Rechtsprechung zum Auskunftsanspruch nach Art. 15 Abs. 1 DSGVO**

Seite 123

Dr. Paweł Litwiński

**US-Gerichte nehmen DSGVO zur Kenntnis – Rechtsprechung zur Datenübermittlung in die USA**

Seite 125

▪ **Nachrichten Seite 104**

Tilman Herbrich und Domenic Trybull

# Ergänzung zur DSK Orientierungshilfe Telemedien: FAQs zu Cookies und Tracking

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI BaWü) bietet mit dem im März 2022 veröffentlichten „FAQ zu Cookies und Tracking“ eine praxisorientierte Ergänzung zur DSK „Orientierungshilfe für Anbieter:innen von Telemedien ab dem 1. Dezember 2021“ an. Betreibern von Websites und Anbietern von Apps soll ein Leitfaden an die Hand gegeben werden, um Inhalte möglichst datenschutzfreundlich und rechtskonform einzubinden. Hierzu werden häufige Fragen in Bezug auf Cookies und Tracking beantwortet. Der Beitrag gibt einen kurzen Überblick über die wichtigsten Erkenntnisse und Erläuterung dieser Antworten.

## Einwilligung für Einsatz von Cookies

Zu Beginn der FAQs wird durch den Landesbeauftragten für Datenschutz und Informationsfreiheit des Landes Baden-Württemberg (LfDI BaWü) die allgemeingültige Empfehlung ausgesprochen, so weit wie möglich auf den Einsatz von einwilligungsbedürftigen Verarbeitungen zu verzichten. Bezogen auf die Anwendung der Neuregelung in § 25 Abs. 1 Satz 1 TTDSG für „die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder den Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind“ fasst der LfDI BaWü jede dem Einsatz von Cookies ähnliche Technologie (z. B. Fingerprinting, Auslesen von Web-Storage oder Werbe- und Geräte IDs) unter dem Begriff „Cookies“ zusammen.

## Ausnahmen von der Einwilligungspflicht

Cookies sind grundsätzlich einwilligungspflichtig, § 25 Abs. 1 TTDSG. Hiervon macht § 25 Abs. 2 TTDSG zwei Ausnahmen: zum einen für die reine Durchführung elektronischer Kommunikation und zum anderen für die unbedingte Erforderlichkeit des Endgerätezugriffs für die Zurverfügungstellung eines vom Nutzer gewünschten Telemediendienstes.

Als Beispiel, welche unbedingt erforderlichen Cookies ohne Einwilligung eingesetzt werden dürfen, führt der LfDI BaWü etwa Cookies für die notwendige Sitzungsverwaltung (Login- und Warenkorb-Cookies), Erfassung der ausgewählten Sprache im Fall der Abweichung von der Standardsprache, Erfassung des Einwilligungsstatus (ja/nein) ohne Verwendung einer eindeutigen ID sowie für Sicherheitszwecke an. Der LfDI BaWü bestätigt insofern die strikte Linie der DSK Orientierungshilfe Telemedien (DSK OH Telemedien 2021, vgl. Piltz/Schweers DSB 2022, 22 f.), dass die Ausnahmeregelung in § 25 Abs. 2 TTDSG nicht für die endgerätebezogene Erfassung von Nutzerpräferenzen und Spracheinstellungen gelte.

## Gestaltung von Einwilligungen

Einwilligungsbanner sollten nach Ansicht des LfDI BaWü nur dann eingeblendet werden, wenn ein einwilligungsbe-

zogener Vorgang auf der Startseite oder Unterseite stattfindet. Wichtig sei, dass Datenschutzhinweise und Impressum trotz Anzeige eines Einwilligungsbanner zugänglich bleiben. Unerlässlich sei eine Ablehnungsmöglichkeit bereits auf der ersten Schicht des Einwilligungs-Banners, denn die Ablehnung einer Einwilligungserklärung müsse so einfach wie deren Erteilung sein.

Eine wirksame Einwilligungserklärung setzt aufgrund des Verweises gemäß § 25 Abs. 1 Satz 2 TTDSG voraus, dass sie vor Verarbeitung aktiv, freiwillig sowie unabhängig von anderen Erklärungen erfolgt, die betroffene Person transparent über die Vorgänge informiert wird und die Einwilligung jederzeit widerrufen werden kann. In der Einwilligungserklärung müssen laut LfDI BaWü die Speicherung und der Zugriff auf Informationen sowie die weitere Verarbeitung klar beschrieben werden. Generische Hinweise seien hierfür nicht ausreichend. Insbesondere bedürfe es einer klaren und einfachen Sprache sowie einer genauen namentlichen Auflistung der Empfänger sowie die von den Empfängern verfolgte Zwecke. Insbesondere sei nicht ausreichend, nur das Ergebnis der Verarbeitung (z. B. Anzeige von Werbung) zu benennen, vielmehr müsse auch die Verarbeitung selbst (z. B. Erstellung eines Profils über die Interessen und Vorlieben durch Aufzeichnung des Nutzerverhaltens) in verständlicher Form beschrieben werden.

Hieran scheitern in der Praxis viele Einwilligungsgestaltungen, die lediglich stichpunktartig abstrakte Zweckbeschreibungen und Datenparameter aufführen, ohne die einzelnen Funktionsweisen der Verarbeitungsvorgänge nachvollziehbar darzulegen. Bereits der EuGH forderte in der „Planet49“-Entscheidung für eine informierte Einwilligung, dass ein Nutzer die „Konsequenzen einer Einwilligung“ in „voller Kenntnis der Sachlage“ erblicken können müsse, um „die Funktionsweise der verwendeten Cookies zu verstehen“ (EuGH, Urt. v. 1.10.2019 – C-673/17, Rn. 74).

Anders als die DSK OH Telemedien 2021 äußert sich der LfDI BaWü zur Einbindung von ausdrücklichen Einwilligungen für besondere Kategorien personenbezogener Da-

ten. Nutzer müssten explizit auf die Verarbeitung von z. B. Gesundheitsdaten hingewiesen und ihr ausdrücklicher Wille hierzu abgefragt werden. Dies lässt sich in einem Einwilligungs-Banner nur durch eine separate Schaltfläche oder Checkbox realisieren, was zulasten der Einwilligungs-raten des gesamten Banners gehen dürfte. Ebenfalls stellt der LfDI BaWü im Gegensatz zur DSK klar, dass ein Einwilligungs-Banner in der Sprache abgefasst sein müssen, in der das entsprechende Zielpublikum angesprochen wird. Überdies warnen die FAQs vor dem Einsatz unsicherer Selbstregulierungsstandards zur Abfrage einer Einwilligungserklärung. Wie die belgische Datenschutzaufsichts-behörde in ihrem Bußgeldbescheid vom 2.2.22 (Fall-Nummer DOS-2019-01377) feststellte, verstoße etwa der weitläufig eingesetzte Standard IAB Europe „Transparency and Consent Framework v2.0“ unter anderem gegen die Transparenzvorgaben der DSGVO.

Oft begangene Fehler bei der Gestaltung von Einwilligungslösungen seien etwa die Nutzung einer Opt-Out-Lösung, bei der die Zustimmung bereits vorausgewählt ist oder die nur generelle und nicht nach Kategorien aufgeschlüsselte Möglichkeit der Einwilligung. Auch dürften Nutzer:innen nicht durch „Nudging“ bei ihrer Entscheidung beeinflusst werden. Zudem wird die Erschwerung einer Ablehnung als häufige Fehlerquelle genannt. Lehrreich sind die zahlreichen Negativbeispiele für konkrete Banner-Gestaltungen sowie die Fehlerliste; sie stellen eine praxisnahe Beurteilung verbreiteter Gestaltungen dar.

Der LfDi BaWü rät von der Einholung einer Einwilligung im Fall des Eingreifens von Ausnahmen nach § 25 Abs. 2 TTDSG ab. In der Praxis trifft man regelmäßig auf Einwilligungs-Banner mit einer nicht abwählbaren und voreingestellten Kategorie „technisch notwendig“. Dabei werde Betroffenen suggeriert, ihnen stünde ein Widerruf einer etwaigen Einwilligung zu. Dies stellt nach Ansicht des LfDI BaWü einen Verstoß gegen die Grundsätze von Treu und Glauben sowie den Grundsatz der Transparenz (Art. 5 Abs. 1 DSGVO, Art. 12 Abs. 1 i. V. m. Art. 13 Abs. 2 lit. c DSGVO) dar. Von derartigen Gestaltungen ist zur Vermeidung einer Irreführung über die Rechte der Verbraucher nach § 5 Abs. 1 Satz 2 Nr. 6 UWG abzuraten (vgl. LG Frankfurt [Oder], Urt. v. 18.6.2020 – 31 O 59/19). Sofern ein endgerätebezogener Vorgang einer Ausnahme in § 25 Abs. 2 TTDSG unterfällt, sind lediglich die Angaben nach Art. 13 DSGVO in den Datenschutzinformationen erforderlich.

Was den Einsatz von Google Analytics angeht, schließt sich der LfDI BaWü u. a. der Ansicht der österreichischen Behörde an, dass für den Drittlandtransfer die von Google in den Standardvertragsklauseln aufgeführten technischen und organisatorischen Maßnahmen wie die Kürzung der IP-Adresse nach Übermittlung in die USA nicht ausreichen, um die Anforderungen des EuGH-Urteils „Schrems II“ an

zusätzliche Maßnahmen (Urt. v. 16.07.2020 – C-311/18) zu erfüllen (vgl. Schweiger DSB 2022, 52 f.). Im Übrigen hält der LfDI BaWü in Anschluss an die DSK OH Telemedien 2021 fest, dass der Einsatz von Tracking-Tools zur Nachverfolgung des Nutzerverhaltens aufgrund der wiederkehrenden Endgerätezugriffe nicht auf eine Einwilligung nach Art. 49 Abs. 1 lit. a) DSGVO gestützt werden könne.

### Externe Inhalte und Elemente

Für die Einbindung von Inhalten und Elementen (Textteile, Schriften, Bilder, Videos Kartendienste etc.) von Drittanbietern fordert der LfDI BaWü die Umsetzung einer datenschutzfreundlichen Einbindung als Ansatz für „Data Protection by Design“ oder „Privacy-Enhancing Technologies (PETs)“. Hierfür kämen verschiedene Lösungswege in Betracht.

#### Zwei-Klick-Lösung

Nach der „Zwei-Klick-Lösung“ (z. B. Embetty von c't) wird zu den eingebundenen Social-Media-Inhalten eine Vorschau gegeben. Entscheidet sich die betroffene Person zum Aufruf des Inhalts, so muss sie durch erneutes Anklicken dies aktiv bestätigen. Vorteil der Lösung sei, dass es zu keiner direkten Übermittlung an Dritte wie YouTube oder Twitter kommt. Jedoch müssten auch bei dieser Lösung Nutzer:innen darüber informiert werden, dass bei Abruf des Inhalts eine Übermittlung der Daten an den Drittanbieter und ggf. eine Verkettung von Daten erfolgt. Noch datenschutzfreundlicher stuft der LfDI BaWü die bloße Einbindung von Screenshots und textliche Zitate von Social-Media-Inhalten z. B. Twitter oder Verlinkungen auf externe Medien wie YouTube-Videos ein. In diesem Fall erfolgt keinerlei Datenaustausch mit Drittanbietern.

#### „Proxy“-Lösung

Für die Einbindung von externen Kartendiensten empfiehlt der LfDI BaWü neben einer „Zwei-Klick-Lösung“ die Nutzung von Proxy-Lösungen, wie sie von OpenStreetmap angeboten wird. Mithilfe einer Proxy-Lösung könne vermieden werden, dass Drittanbieter clientseitig auf das Endgerät zugreifen. Da nicht der Client, sondern der Proxy-Server die HTTPS-Anfrage zum Abruf des Kartendienstes sende, finde keine Übermittlung personenbezogener Daten statt.

#### Lokale Verarbeitung

Schließlich sei eine lokale Einbindung eine Alternative zur Einbindung externer Schriftarten und Fonts über Schnittstellen wie APIs zu Drittanbietern wie Google oder Adobe, die einen Datenaustausch mit dem Endgerät des Nutzers bedingen. Hier helfe ein lokaler Einsatz von Fonts auf eigenen Servern in der EU z. B. mithilfe des Google Web Fonts Helper. Auch auf diesem Wege könne eine Datenübermittlung an Drittanbieter vermieden werden. Soweit es die Unternehmensstruktur zulasse, könne auch ein eigener

OpenStreetmap-Server verwendet oder Kartendienste lokal implementiert werden.

### Reichweitenanalyse vs. Tracking

Grundsätzlich besteht bei Websitebetreibern ein Bedürfnis danach, Inhalte und entsprechende Interaktionen von Nutzer:innen zu analysieren. Der LfDI BaWü grenzt eine einfache Reichweitenanalyse zur Erstellung von nicht personenbeziehbaren aggregierten Statistiken von hartem Tracking ab. Beim Tracking erfolge über einen längeren Zeitraum eine Wiedererkennung und Datenerfassung einzelner Nutzer:innen. Dagegen werden bei einer Reichweitenmessung zum frühestmöglichen Zeitpunkt Nutzerdaten vom Personenbezug befreit. Dies bedeutet z. B. die Entfernung einer dem Nutzer zugewiesenen ID, sodass kein „singling out“ aus einer aggregierten Statistik mehr möglich ist. Anders als die DSK OH Telemedien 2021 verlangt der LfDI BaWü keine bloße sitzungsbezogene Erfassung von Nutzerdaten für die Belastbarkeit der Ausnahmen in § 25 Abs. 2 TTDSG, sondern lehnt lediglich eine Messung über einen „längeren Zeitraum“ als Reichweitenanalyse ab. Dies würde eine sitzungsübergreifende Erfassung des Nutzungsverhaltens nicht ausschließen, sofern man hierin den frühestmöglichen Zeitpunkt für die Anonymisierung etwa bei domänenübergreifenden Reichweitenanalysen erblickt.

### Reichweitenanalyse ohne Einwilligung

Nach Einschätzung des LfDI BaWü ist auch eine zustimmungsfreie Reichweitenanalyse z. B. mittels reiner Logfile-Analyse ohne Einschaltung von Drittanbietern möglich. Ein Endgerätezugriff finde nicht statt, da die Informationen ohne Zutun oder Verwendung von Skripten und HTML-Elementen vom Nutzer an den Website-Betreiber gesendet werden.

Man darf diese Ansicht zum Vorliegen eines Endgerätezugriffs unter Berücksichtigung der englischen Sprachfassung von Art. 5 Abs. 3, S. 1 ePrivacy-RL „the gaining of access“ und der Ansicht der Artikel-29-Datenschutzgruppe, WP 224, S. 9) kritisieren. Denn der Zugriff auf Endgeräteinformationen muss laut dem EDSA-Vorgängergremium nicht im Rahmen derselben Kommunikation erfolgen. Ein Zugriff auf Informationen wie die IP-Adresse, aufgerufene Website, vorherige Website (Referrer), Timestamp und User Agent (verwendeter Browser und Betriebssystem), die bereits im Endgerät gespeichert sind, erfolgt auch dann, wenn entsprechende Informationen aus einer Serveranfrage des Nutzers in angelegten Logfiles erfasst werden. Das Verwenden von Logfiles verlangt ein Zutun des Website-Betreibers; der Betrieb einer Website ist auch ohne Logfiles möglich. Es hätte sich angeboten, Logfile-Analysen als unbedingt erforderlichen Zugriff auf Endgeräteinformationen einzustufen und entsprechende Auslegungskriterien an die Hand zu geben. Erst die sich anschließende Auswertung lässt sich im Einklang mit der Rechtsprechung des EuGH im Verfahren

„One-Stop-Shop“ als nachgelagerten Verarbeitungsvorgang einstufen, der nicht mehr durch Art. 5 Abs. 3 ePrivacy-RL gedeckt ist und dem Anwendungsbereich der DSGVO unterfällt (Urt. v. 15.6.2021 – C-645/19, Rn. 74).

Nach Ansicht des LfDI BaWü kann im Einklang mit der OH Telemedien 2019 die Rechtsgrundlage aus Art. 6 Abs. 1, Satz 1 lit. f DSGVO herangezogen werden (vgl. Herbrich/Ettig, DSB 2019, 108 f.). Dies setzt eine dokumentierte Interessenabwägung voraus, die sich mittels eines Legitimate Interests Assessment durchführen lässt (vgl. hierzu Herbrich, DSB 2020, 181).

### Nutzungsanalyse mit Einwilligung

Etwas anderes gilt, wenn in den Übertragungsvorgang – z. B. aktiv über JavaScript-Befehle – eingegriffen und anhand von Browser- und Geräteeinstellungen ein Fingerprint zur Wiedererkennung des Endgeräts erstellt wird (aktives Fingerprinting). In diesem Fall bejaht der LfDI BaWü wie bei Cookies einen „Zugriff“ auf das Endgerät und es ist eine Einwilligung nach § 25 Abs. 1 TTDSG erforderlich.

### Serverseitiges Tracking

Erstmals positioniert sich eine Datenschutzbehörde zum Server-Side-Tracking. Hinter diesem Begriff verbirgt sich ein Konzept, das Tracking vom Endgerät des Nutzers auf den Server des Verantwortlichen auszulagern, der ohnehin den gesamten Datenverkehr einer Website mitschneiden kann. Deshalb sind Lösungen wie der Server Side Google Tag Manager, der innerhalb der Google Cloud Umgebung läuft, nicht von den Äußerungen der Behörde betroffen. Werden für das Server-Side-Tracking Cookies verwendet oder findet Fingerprinting statt, so gelten laut LfDI BaWü jedoch das TTDSG und die DSGVO uneingeschränkt.

Bemerkenswert ist dagegen die Einschätzung, dass ein vom Verantwortlichen durchgeführtes Server-Side-Tracking ohne Cookies und Durchführung einer Anonymisierung der Nutzerdaten vor Weitergabe an einen Tracking-Anbieter nicht in den Anwendungsbereich des TTDSG falle und auf Art. 6 Abs. 1, Satz 1 lit. f DSGVO gestützt werden könne. Da für die Nutzung von Server-Side-Tracking in der Regel für die Wiedererkennung von Nutzer die Einbindung von JavaScript-Code in der Website erforderlich ist, widersprechen sich die FAQs mit den eigenen Ausführungen zur Reichweitenanalyse.

Zutreffender wäre insofern die Annahme eines Endgerätezugriffs gewesen, der jedoch aufgrund des Einsatzzweckes – vollständige Kontrolle über einzelne Datenpunkte, Reduzierung oder Synthetisierung (Pseudonymisierung) von Datenpunkten zur Gewährung der Rechtskonformität der späteren Verarbeitung, Kontrolle über Weitergabe von Datenpunkten an Drittanbieter durch Festlegungen von Bedingungen – im Rahmen einer dokumentierten Erfor-

derlichkeitsprüfung als unbedingt erforderlich einzustufen ist. Aufgrund der Gewährleistung von „Data Protection by Design“ spricht vieles dafür, diese Erwägungen auch auf Lösungen von Drittanbietern zu erstrecken, die ein serverseitiges Tracking als Middleware oder Tracking-Proxy-Lösung bereitstellen und strikt weisungsgebunden als Auftragsverarbeiter eingebunden werden.

### Fazit

Die FAQs des LfDI BaWü stehen im Einklang mit den ED-SA Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 und ergänzen die DSK OH Telemedien 2021 in sinnvoller Weise. Erkenntnisreich und positiv hervorzuheben sind insbesondere die Vielzahl an Negativbeispielen und die Mängelliste zur Gestaltung von Einwilligungslösungen.

Spätestens nach dem zu erwartenden Urteil des EuGH in dem Vorlageverfahren „Facebook App-Zentrum“ am 28.4.2022 zur Klagebefugnis von Verbänden und Wettbewerbern ist mit der flächendeckenden Fortsetzung der Rechtsdurchsetzung zu rechnen. Bis dahin können die Auslegungshinweise der Aufsichtsbehörden eine gute Orientierung bei der (Neu)Gestaltung von Einwilligungslösungen dienen.

Tracking-Prevention-Systemen wie ITP von Safari oder ETP von Firefox oder AdBlocking-Systemen, die endgerätebezogene Nutzungsanalysen wesentlich erschweren, werden den Einsatz von serverseitigen Tracking-Mechanismen fördern. Insoweit sind ausdifferenzierte Stellungnahmen der Aufsichtsbehörden wünschenswert, um in der Praxis die notwendige Rechtssicherheit zu gewährleisten.

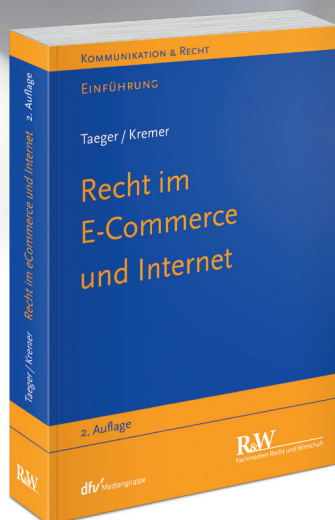
**Autoren:** Tilman Herbrich (CIPP/E) ist Teil der Schriftleitung und Rechtsanwalt bei Spirit Legal in Leipzig. Er berät Unternehmen bei der Nutzung neuer Werbetechnologien im Einklang mit dem Europäischen Datenschutz- und Wettbewerbsrecht.



Domenic Trybull ist Wissenschaftlicher Mitarbeiter bei Spirit Legal in Leipzig.



## Kompakte Einführung



### Themenschwerpunkte

- Zivilrechtliche Regulierung von Plattformen (P2B-VO)
- Fernabsatzrecht inkl. elektronischem Streitschlichtungsverfahren
- Widerrufsrecht und Informationspflichten im eCommerce und mCommerce
- Eigenes Kapitel zu den neuen Regelungen für digitale Inhalte
- Haftung der Portalbetreiber sowie wettbewerbs- und datenschutzrechtliche Fragen
- **Topaktuell:** Enthält bereits die Neuregelungen aufgrund der Umsetzung der Richtlinie über digitale Inhalte und das sog. ‚**Faire Verbraucherverträge**‘ -Gesetz

### Von erfahrenen Spezialisten

Prof. Dr. Prof. h. c. **Jürgen Taeger** ist Of Counsel bei DLA Piper. Bis März 2020 war er Inhaber des Lehrstuhls für Bürgerliches Recht, Handels- und Wirtschaftsrecht sowie Informationsrecht an der Universität Oldenburg und Direktor des Zentrums für Recht der Informationsgesellschaft (ZRI). Er ist Vorstandsvorsitzender der Deutschen Stiftung für Recht und Informatik (DSRI).

**Sascha Kremer** ist FA für IT-Recht, Datenschutzexperte und Lehrbeauftragter an den Hochschulen Düsseldorf und Bonn-Rhein-Sieg für IT- und Datenschutzrecht.

Taeger/Kremer | **Recht im E-Commerce und Internet**

2. Auflage 2021 | Kommunikation & Recht | Einführung | 538 Seiten | Broschur | € 98,- | ISBN: 978-3-8005-1727-5

Weitere Informationen [shop.ruw.de/17275](https://shop.ruw.de/17275)

