

Themenheft:

AV-Vertrag? Prüfen Sie zuerst die Rollen

NICHT VORSCHNELL ZUM AV-VERTRAG: DIE RICHTIGE EINORDNUNG ZÄHLT

SELBSTTEST

AV-Vertrag oder doch etwas anderes? Testen Sie Ihr Wissen anhand typischer Praxisfälle

3

PRÜFSHEMA

Die richtige Einordnung: Prüfschema und Prüfkriterien

4–5



Onlinebereich:
<https://www.privacyxperts.de>



Live-Talk:
<https://t1p.de/live-talk>



E-Mail-Beratung:
<https://t1p.de/anna-mauch>



PRIVACYXPERTS



Die richtige Einordnung zählt

Liebe Leserin, lieber Leser,

ein Vertrag zur Auftragsverarbeitung (AV-Vertrag) schafft nicht automatisch Rechtssicherheit. Entscheidend ist die tatsächliche Rollenverteilung. Gerade bei Anwendungen der Künstlichen Intelligenz (KI), Cloud-Diensten und anderen Softwareplattformen ist die Abgrenzung zwischen Auftragsverarbeitung, gemeinsamer Verantwortlichkeit und eigenständiger Verantwortlichkeit häufig anspruchsvoll.

Dieses Themenheft zeigt Ihnen, worauf es bei der richtigen Einordnung ankommt und welche Pflichten sich daraus ergeben.

Viele Grüße

Dr. Anna-Kathrin Mauch,
Rechtsanwältin und Redakteurin

Ihre Expertin für Datenschutz

Dr. Anna-Kathrin Mauch ist Rechtsanwältin und Europajuristin mit Erfahrung im Vertrags- und Datenschutzrecht. Sie bringt Datenschutz verständlich und praxisnah auf den Punkt.

Inhalt

Einordnung

Datenschutzrechtliche Rollen und ihre Abgrenzung

Seiten 1–2

Selbsttest

AV-Vertrag oder doch etwas anderes?
Testen Sie Ihr Wissen anhand typischer Praxisfälle

Seite 3

Prüfschema

Die richtige Einordnung: Prüfschema und Prüfkriterien

Seiten 4–5

KI

Und wie sieht es bei KI aus?
Wer trägt die datenschutzrechtliche Verantwortung?

Seiten 6–7

Auswertung

Selbsttest aufgelöst:
Warum welche Lösung richtig ist.

Seite 8



Zu Ihrem Onlinebereich:
<https://www.privacyxperts.de>



Live-Talk:
<https://t1p.de/live-talk>



E-Mail-Beratung:
<https://t1p.de/anna-mauch>

Impressum



ein Unternehmensbereich des
VNR Verlags für die Deutsche Wirtschaft AG
Theodor-Heuss-Str. 2–4, 53095 Bonn
Telefon: 02 28 / 9 55 01 60
Fax: 02 28 / 3 69 64 80
ISSN: 1614 – 5674

Vorstand: Richard Rentrop, Michael Schrader, Bonn
V.i.S.d.P.: Michael Jodda (Adresse s. oben)
Produktmanagement: Franziska Rohrbach, Bonn

Autorin:

Dr. Anna-Kathrin Mauch, Rottweil

Design: Kreativ Konzept Agentur für Werbung, Bonn
Satz: Schmelzer Medien GmbH, Siegen

Druck: Warlich Druck Meckenheim GmbH,
Am Hambuch 5, 53340 Meckenheim

Bildnachweise: Titel: Adobe Stock | Bernhard; Seite 1: Adobe Stock
| MQ-Illustrations

Erscheinungsweise: 36-mal pro Jahr

E-Mail: kundendienst@privacyxperts.de

Internet: www.privacyxperts.de

(bei Rückfragen bitte Kundennummer angeben)

Alle Angaben wurden mit äußerster Sorgfalt ermittelt und überprüft. Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen. Eine Gewähr kann deshalb nicht übernommen werden.

Im Interesse der Lesbarkeit verzichten wir in unseren Beiträgen auf geschlechtsbezogene Formulierungen. Selbstverständlich sind immer alle Geschlechterformen gemeint, auch wenn explizit nur eines der Geschlechter angesprochen wird.

Dieses Produkt besteht aus FSC®-zertifiziertem Papier.

© 2026 by VNR Verlag für die Deutsche Wirtschaft AG, Bonn, Berlin, Bukarest, Jacksonville, Manchester, Passau, Warschau



Auf die tatsächliche Rollenverteilung kommt es an – nicht auf den Vertrag.

Datenschutzrechtliche Rollen und ihre Abgrenzung

Die Abgrenzung zwischen Auftragsverarbeitung, gemeinsamer Verantwortlichkeit und eigenständiger Verantwortlichkeit bereitet in der Praxis häufig Schwierigkeiten. Nicht selten wird vorsorglich ein Auftragsverarbeitungsvertrag geschlossen, obwohl die tatsächliche Rollenverteilung eine andere ist. Maßgeblich ist nicht der Vertrag, sondern die tatsächliche Rollenverteilung im konkreten Verarbeitungsvorgang. Eine fehlerhafte Einordnung kann zu erheblichen rechtlichen und finanziellen Konsequenzen führen.

Die richtige Einordnung wird immer wichtiger

Ob Auftragsverarbeitung, gemeinsame Verantwortlichkeit oder eigenständige Verantwortlichkeit – die richtige Einordnung ist die Grundlage jeder datenschutzrechtlichen Zusammenarbeit. Denn davon hängt ab, welche Pflichten Ihr Unternehmen erfüllen muss und welche Vereinbarungen erforderlich sind.

Die Abgrenzung wird allerdings immer schwieriger. Viele Cloud-Dienste, KI-Anwendungen oder Plattformen beschränken sich nicht mehr darauf, Daten ausschließlich im Auftrag zu verarbeiten.

Gleichzeitig hat die Rechtsprechung des Europäischen Gerichtshofs (EuGH) den Begriff der gemeinsamen Verantwortlichkeit in den vergangenen Jahren weit ausgelegt. Dadurch kommt diese Form der Zusammenarbeit heute deutlich häufiger in Betracht als noch vor einigen Jahren. So kann beispielsweise bereits der Betrieb einer Unternehmens-Fanpage in sozialen Netzwerken oder die Einbindung von Social-Media-Plug-ins (etwa eines „Gefällt mir“-Buttons) auf der Unternehmenswebsite eine gemeinsame Verantwortlichkeit begründen.

Entscheidend ist die tatsächliche Zusammenarbeit

Ob eine Auftragsverarbeitung oder eine gemeinsame Verantwortlichkeit vorliegt, entscheidet sich nicht nach der Bezeichnung im Vertrag, sondern nach der tatsächlichen Ausgestaltung der Zusammenarbeit. Prüfen Sie daher zunächst, welche Rolle die Beteiligten im konkreten Verarbeitungsvorgang tatsächlich einnehmen.

Eine **Auftragsverarbeitung** liegt vor, wenn ein Dienstleister personenbezogene Daten ausschließlich im Auftrag und nach Weisung des Verantwortlichen verarbeitet. Eigene Entscheidungen über Zwecke oder wesentliche Mittel der Verarbeitung trifft er dabei nicht. Er handelt datenschutzrechtlich als „verlängerter Arm“ des Verantwortlichen.

Von einer **gemeinsamen Verantwortlichkeit** ist dagegen auszugehen, wenn zwei oder mehr Stellen gemeinsam über Zwecke und wesentliche Mittel einer Verarbeitung entscheiden. Nach Auffassung des Europäischen Datenschutzausschusses (EDSA) genügt hierfür bereits ein maßgeblicher Einfluss auf das „Ob“ und „Wie“ der Verarbeitung. Der EuGH verlangt dabei keine gleichmäßig verteilte Entscheidungsbefugnis. Bereits ein begrenzter Einfluss kann – abhängig von den Umständen des Einzelfalls – eine gemeinsame Verantwortlichkeit begründen.

Eine **eigenständige Verantwortlichkeit** liegt dagegen vor, wenn eine Stelle selbst über Zwecke und wesentliche Mittel der Verarbeitung entscheidet oder personenbezogene Daten zur Erfüllung eigener gesetzlicher oder wirtschaftlicher Aufgaben verarbeitet. Typische Beispiele sind Steuerberater, Rechtsanwälte oder Banken.

Praxisbeispiel: Ein Cloud-Anbieter verarbeitet Kundendaten zur Bereitstellung seiner Software ausschließlich nach Weisung des Kunden und ist insoweit Auftragsverarbeiter. Nutzt er Protokoll- oder Nutzungsdaten zusätzlich zur Produktverbesserung oder zum Training eigener KI-Modelle, handelt er hierfür als eigenständig Verantwortlicher. Je nach Verarbeitung kann derselbe Anbieter unterschiedliche datenschutzrechtliche Rollen einnehmen.

Auf den Punkt gebracht

Nicht jede Zusammenarbeit führt zu einer gemeinsamen Verantwortlichkeit. Ebenso wenig wird ein Dienstleister allein durch den Abschluss eines Auftragsvertrags zum Auftragsverarbeiter. Entscheidend ist die tatsächliche Rollenverteilung: Eine Auftragsverarbeitung setzt Weisungsgebundenheit voraus, eine gemeinsame Verantwortlichkeit gemeinsame Entscheidungen über Zwecke und wesentliche Mittel der Verarbeitung.

Aktuelle Rechtsprechung: das Urteil des VG Berlin

Wie praxisrelevant die Abgrenzung zwischen Auftragsverarbeitung und gemeinsamer Verantwortlichkeit ist, zeigt ein aktuelles Urteil des Verwaltungsgerichts (VG) Berlin (Urteil vom 14.10.2025, Az. 1 K 74/24). Eine Theaterbetreiberin beauftragte einen Adresshändler mit dem Versand von Werbeschreiben. Zwar legte sie die Zielgruppe fest, hatte jedoch weder Zugriff auf die Adressdaten noch Einfluss auf deren Auswahl oder den Versand. Das VG Berlin entschied, dass dies für eine gemeinsame Verantwortlichkeit nicht

ausreicht. Maßgeblich sei vielmehr, wer tatsächlich über die Zwecke und wesentlichen Mittel der Datenverarbeitung entscheidet. Da Auswahl, Verwaltung und Verarbeitung der Adressdaten ausschließlich durch den Adresshändler erfolgten, lag keine gemeinsame Verantwortlichkeit vor.

Für Datenschutzbeauftragte bedeutet das: Nicht jede Zusammenarbeit zwischen zwei Unternehmen begründet automatisch eine gemeinsame Verantwortlichkeit. Entscheidend ist die tatsächliche Rollenverteilung. Prüfen und dokumentieren Sie diese daher bereits vor Beginn der Zusammenarbeit. So schaffen Sie Rechtssicherheit und können Ihre Einordnung gegenüber der Datenschutzaufsicht nachvollziehbar begründen.

Welche praktischen Unterschiede sich aus der jeweiligen Rollenverteilung ergeben, zeigt die folgende Übersicht.

Welche Folgen hat die richtige Einordnung?

Die datenschutzrechtliche Rolle entscheidet nicht nur darüber, welcher Vertrag abgeschlossen werden muss. Sie bestimmt auch, welche Rechte, Pflichten und Verantwortlichkeiten die Beteiligten während der gesamten Zusammenarbeit treffen.

	Auftragsverarbeitung	Gemeinsame Verantwortlichkeit	Eigenständige Verantwortlichkeit
Erforderliche Vereinbarung	Vertrag zur Auftragsverarbeitung nach Art. 28 Datenschutz-Grundverordnung (DSGVO)	Vereinbarung über die gemeinsame Verantwortlichkeit nach Art. 26 DSGVO	Keine besondere Vereinbarung nach Art. 26 oder Art. 28 DSGVO erforderlich
Wer entscheidet über die Verarbeitung?	Der Verantwortliche entscheidet über Zwecke und wesentliche Mittel der Verarbeitung. Der Auftragsverarbeiter handelt ausschließlich auf Weisung.	Zwei oder mehr Stellen entscheiden gemeinsam über Zwecke und wesentliche Mittel der gemeinsamen Verarbeitung.	Jeder Verantwortliche entscheidet eigenständig über Zwecke und Mittel seiner Verarbeitung.
Technische und organisatorische Maßnahmen (TOM)	Der Auftragsverarbeiter muss geeignete TOM umsetzen. Der Verantwortliche muss sich hiervon überzeugen und die Einhaltung angemessen kontrollieren.	Beide Beteiligten müssen für die gemeinsame Verarbeitung ein angemessenes Schutzniveau gewährleisten und ihre Verantwortlichkeiten abstimmen.	Jeder Verantwortliche ist selbst für geeignete TOM verantwortlich.
Rechtsgrundlage der Verarbeitung	Der Verantwortliche stellt sicher, dass für die Verarbeitung eine Rechtsgrundlage nach Art. 6 DSGVO besteht.	Jeder gemeinsam Verantwortliche benötigt eine tragfähige Rechtsgrundlage für die gemeinsame Verarbeitung. Art. 26 DSGVO ersetzt keine Rechtsgrundlage.	Jeder Verantwortliche benötigt eine eigene Rechtsgrundlage für seine Verarbeitung.
Verantwortung gegenüber Betroffenen	Der Verantwortliche bleibt erster Ansprechpartner für Betroffenenrechte. Der Auftragsverarbeiter unterstützt ihn bei deren Erfüllung.	Die Zuständigkeiten müssen transparent geregelt werden. Betroffene können ihre Rechte grundsätzlich gegenüber jedem gemeinsam Verantwortlichen geltend machen.	Jeder Verantwortliche erfüllt Informationspflichten und Betroffenenrechte für seine eigene Verarbeitung selbst.
Datenschutzrechtliche Verantwortung	Der Verantwortliche trägt die Verantwortung für die Rechtmäßigkeit der Verarbeitung und muss den Auftragsverarbeiter sorgfältig auswählen und überwachen.	Beide Beteiligten tragen Verantwortung für die gemeinsame Verarbeitung. Die Aufgaben und Zuständigkeiten sind vertraglich eindeutig festzulegen.	Jeder Verantwortliche trägt die volle Verantwortung für seinen eigenen Verantwortungsbereich.
Haftung und Bußgelder	Der Verantwortliche bleibt für Auswahl und Überwachung des Auftragsverarbeiters verantwortlich. Verstöße können zu aufsichtsbehördlichen Maßnahmen, Bußgeldern oder Schadensersatzansprüchen führen.	Jeder gemeinsam Verantwortliche kann gegenüber Betroffenen und Aufsichtsbehörden verantwortlich sein. Intern sollten Verantwortlichkeiten eindeutig geregelt werden, um Haftungsrisiken zu minimieren.	Jeder Verantwortliche haftet für Verstöße in seinem eigenen Verantwortungsbereich.
Dokumentationspflichten	Dokumentationspflichten des Verantwortlichen (u. a. Verzeichnis von Verarbeitungstätigkeiten und ggf. Datenschutz-Folgenabschätzung), AV-Vertrag (einschließlich regelmäßiger Überprüfung), Dokumentation von Unterauftragsverarbeitern und ggf. Drittlandtransfers sowie Verzeichnis von Verarbeitungstätigkeiten des Auftragsverarbeiters (Art. 30 Abs. 2 DSGVO).	Allgemeine Dokumentationspflichten der gemeinsam Verantwortlichen sowie Abschluss einer Vereinbarung nach Art. 26 DSGVO und nachvollziehbare Dokumentation der tatsächlichen Aufgaben- und Verantwortungsverteilung	Eigenständige Erfüllung der allgemeinen Dokumentationspflichten (z. B. Verzeichnis von Verarbeitungstätigkeiten, ggf. Datenschutz-Folgenabschätzung)

Testen Sie Ihr Wissen: AV-Vertrag oder doch etwas anderes?

Ein AV-Vertrag ist schnell abgeschlossen – doch liegt tatsächlich auch eine Auftragsverarbeitung vor? Gerade bei Cloud-Diensten, KI-Anwendungen oder der Zusammenarbeit mehrerer Unternehmen ist die richtige Einordnung oft anspruchsvoll. Machen Sie als Datenschutzbeauftragter den Praxistest: Wie würden Sie die folgenden Fallkonstellationen datenschutzrechtlich einordnen?

A = Auftragsverarbeitung

B = gemeinsame Verantwortlichkeit

C = eigenständige Verantwortlichkeit



Nr.	Fallkonstellation	A	B	C
1	Marketingkampagne mit externer Agentur Ihr Unternehmen plant eine Werbekampagne für Bestandskunden. Die Marketingagentur entwickelt nicht nur das Kampagnenkonzept, sondern legt gemeinsam mit Ihrem Unternehmen fest, welche Kundengruppen angesprochen und welche Kundendaten hierfür ausgewertet werden. Die endgültige Entscheidung trifft Ihr Unternehmen, allerdings werden sämtliche Maßnahmen gemeinsam abgestimmt und während der Kampagne regelmäßig angepasst.	☐	☐	☐
2	Cloudbasiertes CRM-System Sie nutzen ein cloudbasiertes CRM-System. Der Anbieter verarbeitet personenbezogene Kundendaten zur Bereitstellung der Software. Laut AV-Vertrag erfolgt die Verarbeitung ausschließlich nach Ihren Weisungen. In den allgemeinen Nutzungsbedingungen ist jedoch vorgesehen, dass Diagnosedaten, Nutzungsinformationen und Protokolldaten zur Verbesserung des Dienstes ausgewertet werden dürfen. Welche Daten hierfür konkret verwendet werden, bleibt offen.	☐	☐	☐
3	KI-Assistenz im Unternehmen Beschäftigte nutzen einen KI-Assistenten zur Erstellung interner Dokumente. Der Anbieter stellt einen AV-Vertrag zur Verfügung. Gleichzeitig enthalten die Nutzungsbedingungen eine Klausel, wonach Eingaben zur Verbesserung der KI verwendet werden können, sofern der Kunde diese Funktion nicht deaktiviert.	☐	☐	☐
4	Gemeinsames Kundenportal Ein Hersteller und sein Vertriebspartner betreiben gemeinsam ein Kundenportal. Beide Unternehmen legen fest, welche personenbezogenen Daten erhoben werden, welche Funktionen das Portal bietet und welche Auswertungen für Marketing- und Vertriebszwecke erfolgen sollen. Die technische Entwicklung übernimmt zwar der Hersteller, über Änderungen entscheiden jedoch beide Unternehmen gemeinsam.	☐	☐	☐
5	Recruiting-Plattform mit KI-Unterstützung Ihr Unternehmen nutzt eine cloudbasierte Recruiting-Plattform. Bewerbungen werden ausschließlich Ihrer Personalabteilung zur Verfügung gestellt. Zusätzlich setzt der Anbieter KI ein, um Bewerbungen zu kategorisieren und seinen Kunden neue Auswertungsmöglichkeiten bereitzustellen. Nach eigenen Angaben erfolgt dies auf Grundlage anonymisierter Datensätze.	☐	☐	☐
6	Externe IT-Administration Ein externer IT-Dienstleister administriert Ihre Server per Fernzugriff. Dabei kann er jederzeit auf personenbezogene Daten zugreifen. Er entscheidet jedoch weder darüber, welche Daten verarbeitet werden, noch zu welchem Zweck. Art und Umfang seiner Tätigkeiten werden ausschließlich von Ihrem Unternehmen vorgegeben.	☐	☐	☐
7	Bonusprogramm mit Kooperationspartner Ein Handelsunternehmen und ein Kreditinstitut führen gemeinsam ein Kundenbindungsprogramm ein. Beide Unternehmen legen gemeinsam fest, welche Daten erhoben werden, welche Vorteile Teilnehmer erhalten und welche Auswertungen für Marketingmaßnahmen durchgeführt werden. Beide Partner möchten die gewonnenen Erkenntnisse anschließend auch für eigene Geschäftsentscheidungen nutzen.	☐	☐	☐
8	Videokonferenzsystem Ihr Unternehmen nutzt einen Videokonferenzdienst für interne und externe Besprechungen. Der Anbieter verarbeitet Bild-, Ton- und Chatdaten zur Durchführung der Meetings. Darüber hinaus erkennt und analysiert er automatisch ungewöhnliche Anmeldeversuche und andere sicherheitsrelevante Ereignisse, um seine Plattform vor Missbrauch und Angriffen zu schützen. Über Art und Umfang dieser Sicherheitsmaßnahmen entscheidet der Anbieter selbst.	☐	☐	☐
9	Steuerberater Sie übermitteln Ihrem Steuerberater Lohn- und Finanzdaten Ihrer Beschäftigten. Der Steuerberater entscheidet eigenständig, welche Unterlagen zur Bearbeitung erforderlich sind, wie lange diese aufzubewahren sind und welche gesetzlichen Dokumentationspflichten einzuhalten sind. Weisungen zur konkreten Verarbeitung erteilen Sie ihm nicht.	☐	☐	☐
10	Weitergabe von Kundendaten an einen Vertragspartner Ihr Unternehmen verkauft Waren oder Dienstleistungen gemeinsam mit einem externen Vertragspartner. Zur Vertragsabwicklung übermitteln Sie diesem die Kontaktdaten des Kunden (z. B. Name, Anschrift, Telefonnummer und E-Mail-Adresse), damit er seine vertraglichen Leistungen gegenüber dem Kunden erbringen kann. Der Vertragspartner entscheidet eigenständig, welche personenbezogenen Daten hierfür erforderlich sind, wie lange diese aufzubewahren sind und welche gesetzlichen Pflichten er erfüllen muss. Weisungen zur konkreten Verarbeitung erhält er von Ihrem Unternehmen nicht.	☐	☐	☐

Die Auflösung mit ausführlichen Erläuterungen und Praxishinweisen finden Sie auf Seite 8.



Die richtige Einordnung: Prüfschema und Prüfkriterien

Viele der Fälle auf Seite 3 finden Sie vermutlich schwieriger als erwartet. Das überrascht nicht. Ob Auftragsverarbeitung, gemeinsame Verantwortlichkeit oder eigenständige Verantwortlichkeit vorliegt, lässt sich häufig nur anhand einer systematischen Prüfung beurteilen. Die folgende Prüfreihefolge hat sich in der Praxis bewährt:

Schritt 1: Handelt der Dienstleister ausschließlich in Ihrem Auftrag?

Ein Auftragsverarbeiter handelt wie der „verlängerte Arm“ des Verantwortlichen. Er verarbeitet personenbezogene Daten ausschließlich im Auftrag und nach dessen Weisung und verfolgt keine eigenen Verarbeitungszwecke. Über Zweck und wesentliche Mittel der Verarbeitung entscheidet der Verantwortliche.

Schritt 2: Verfolgt der Dienstleister eigene Zwecke?

Ergibt die erste Prüfung kein eindeutiges Bild, sollten Sie die Gegenprobe machen. Bereits einzelne Kriterien können darauf hindeuten, dass der Dienstleister nicht lediglich in Ihrem Auftrag handelt, sondern eigenständig datenschutzrechtlich verantwortlich ist.



Prüfkriterium	Trifft zu?
Die Verarbeitung personenbezogener Daten erfolgt ausschließlich nach Ihren datenschutzrechtlichen Weisungen.	☐
Der Dienstleister übernimmt lediglich eine Unterstützungs- oder Hilfsfunktion.	☐
Sie bestimmen den Zweck der Verarbeitung.	☐
Sie legen fest, welche personenbezogenen Daten verarbeitet werden.	☐
Sie entscheiden, welche Personen betroffen sind.	☐
Sie bestimmen, ob und an wen personenbezogene Daten weitergegeben werden.	☐
Sie legen die Aufbewahrungsfristen fest.	☐
Der Dienstleister nutzt die Daten nicht für eigene Zwecke.	☐
Der Dienstleister erzielt keinen wirtschaftlichen Nutzen aus den Daten – außer seiner Vergütung.	☐
Betroffenenfragen werden von Ihrem Unternehmen verantwortet; der Dienstleister unterstützt lediglich bei deren Bearbeitung.	☐
Die Rechtsgrundlage der Verarbeitung wird ausschließlich von Ihrem Unternehmen festgelegt.	☐
Der Dienstleister darf personenbezogene Daten nach Vertragsende nicht weiterverwenden.	☐
Ohne Ihren Auftrag würde die konkrete Verarbeitung nicht stattfinden.	☐
Der Dienstleister entscheidet lediglich über technische Einzelheiten der Verarbeitung.	☐
Der Dienstleister tritt gegenüber Betroffenen nicht als eigenständiger Ansprechpartner auf.	☐
Er darf personenbezogene Daten weder verkaufen noch für Produktentwicklung oder Marketing verwenden.	☐
Die Verarbeitung dient ausschließlich der Erfüllung Ihres Auftrags.	☐

Orientierungshilfe: Je mehr Kriterien erfüllt sind, desto eher spricht dies für eine Auftragsverarbeitung. Keines der Kriterien ist allein entscheidend. Erst die Gesamtbetrachtung führt zur richtigen Einordnung.



Prüfkriterium	Trifft zu?
Der Dienstleister entscheidet selbst über den Zweck der Verarbeitung.	☐
Er bestimmt eigenständig, welche personenbezogenen Daten verarbeitet werden.	☐
Er legt wesentliche Mittel der Verarbeitung selbst fest.	☐
Er entscheidet selbst über die Rechtsgrundlage der Verarbeitung.	☐
Er verarbeitet Daten aufgrund eigener gesetzlicher Verpflichtungen.	☐
Zwischen ihm und den betroffenen Personen besteht eine eigene Vertrags- oder Rechtsbeziehung.	☐
Er entscheidet eigenständig über Speicherdauer und Löschung der Daten.	☐
Er bestimmt selbst, an wen personenbezogene Daten weitergegeben werden.	☐
Er nutzt personenbezogene Daten auch für eigene wirtschaftliche oder organisatorische Zwecke.	☐
Er informiert Betroffene eigenständig über die Datenverarbeitung.	☐
Er entscheidet selbst über die Bearbeitung von Betroffenenrechten.	☐
Die Verarbeitung würde grundsätzlich auch ohne Ihren Auftrag stattfinden.	☐
Er trägt das datenschutzrechtliche Risiko und die Verantwortung für die Verarbeitung.	☐
Er setzt weitere Dienstleister zur Erfüllung eigener Zwecke ein.	☐
Er trifft eigenständige Entscheidungen über das Ergebnis der Verarbeitung.	☐
Er profitiert selbst unmittelbar von den Verarbeitungsergebnissen.	☐
Er kann wesentliche Änderungen der Verarbeitung eigenständig vornehmen.	☐

Achtung: Nicht jeder externe Dienstleister ist automatisch Auftragsverarbeiter. Erhält ein Dienstleister personenbezogene Daten, bedeutet das nicht zwangsläufig, dass eine Auftragsverarbeitung

vorliegt. Steuerberater, Rechtsanwälte, Banken oder Paketdienstleister handeln regelmäßig eigenverantwortlich, obwohl sie personenbezogene Daten erhalten.

Schritt 3: Liegt eine gemeinsame Verantwortlichkeit vor?

Eine gemeinsame Verantwortlichkeit setzt nicht voraus, dass beide Beteiligten sämtliche Entscheidungen gemeinsam treffen oder gleichermaßen Einfluss ausüben. Es genügt bereits, dass mehrere Stellen gemeinsam über Zwecke oder wesentliche Mittel der Verarbeitung entscheiden. Nach der Rechtsprechung des EuGH kann hierfür bereits ein begrenzter Einfluss ausreichen.



Prüfkriterium	Trifft zu?
Die beteiligten Unternehmen verfolgen einen gemeinsamen Zweck.	☐
Sie entscheiden gemeinsam, welche personenbezogenen Daten verarbeitet werden.	☐
Sie bestimmen gemeinsam wesentliche Mittel der Verarbeitung.	☐
Das Verarbeitungskonzept wurde gemeinsam entwickelt.	☐
Beide Unternehmen profitieren von den Ergebnissen der Verarbeitung.	☐
Die Verarbeitung erfolgt auf einer gemeinsamen Datenbasis oder Plattform.	☐
Entscheidungen über die Verarbeitung werden gemeinsam vorbereitet oder abgestimmt.	☐
Die Datenverarbeitung des einen Unternehmens beeinflusst unmittelbar die Verarbeitung des anderen.	☐
Ohne das Zusammenwirken beider Unternehmen könnte die Verarbeitung in dieser Form nicht stattfinden.	☐
Ein Unternehmen veranlasst die Verarbeitung des anderen und profitiert von deren Ergebnissen.	☐
Beide Unternehmen legen gemeinsam fest, welche Personen-gruppen betroffen sind.	☐
Beide entscheiden gemeinsam über wesentliche Änderungen der Verarbeitung.	☐
Die Verarbeitung dient einem gemeinsamen Geschäftsmodell oder einer gemeinsamen wirtschaftlichen Zielsetzung.	☐
Beide bestimmen gemeinsam, welche Daten erhoben oder ausgewertet werden.	☐
Beide legen gemeinsam fest, wer Zugriff auf personenbezogene Daten erhält.	☐
Beide stimmen Informationspflichten oder Datenschutzinformationen gemeinsam ab.	☐
Beide Unternehmen tragen Verantwortung für den Erfolg der Verarbeitung – auch wenn ihre Aufgaben unterschiedlich verteilt sind.	☐

Lesetipp – EDSA-Leitlinien 07/2020

Die EDSA-Leitlinien 07/2020 konkretisieren die Begriffe des Verantwortlichen, Auftragsverarbeiters und der gemeinsamen Verantwortlichkeit. Sie enthalten zahlreiche Auslegungshinweise und typische Fallkonstellationen und bieten damit eine wertvolle Orientierung für die

datenschutzrechtliche Einordnung komplexer Verarbeitungssituationen.

Besonders hilfreich sind die Ausführungen zu

- der Abgrenzung zwischen Verantwortlichem, Auftragsverarbeiter und gemeinsam Verantwortlichem,
- der Bedeutung der tatsächlichen Rollenverteilung gegenüber der bloßen Vertragsbezeichnung sowie
- typischen Praxisbeispielen zur datenschutzrechtlichen Einordnung.

Nicht mit dem Vertrag beginnen – sondern mit der Rollenverteilung

Das Prüfschema unterstützt dabei, die datenschutzrechtliche Rolle systematisch zu bestimmen. Es ersetzt jedoch nicht die Prüfung der konkreten Umstände des jeweiligen Einzelfalls. Entscheidend ist nicht die Bezeichnung oder Überschrift eines Vertrags, sondern die tatsächliche Ausgestaltung der Zusammenarbeit. Maßgeblich ist insbesondere, wer über die Zwecke der Verarbeitung entscheidet, wer die wesentlichen Mittel festlegt und ob der Dienstleister eigene Interessen an den personenbezogenen Daten verfolgt.

Von einer zutreffenden Rollenbestimmung hängen sowohl die anzuwendenden datenschutzrechtlichen Anforderungen als auch die Auswahl der richtigen vertraglichen Gestaltung ab.

Die Rollenverteilung sollte daher bereits im Rahmen datenschutzrechtlicher Freigabeprozesse vor Beginn der Zusammenarbeit geprüft werden. Dabei ist zu beachten, dass sie für jeden Verarbeitungsvorgang gesondert zu bestimmen ist.

Jetzt wird es praktisch: Was folgt aus der Einordnung?

Liegt eine Auftragsverarbeitung vor, müssen Sie vor allem

- › einen Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO abschließen oder einen bestehenden Vertrag überprüfen,
- › die TOM des Auftragsverarbeiters bewerten,
- › Unterauftragsverarbeiter und mögliche Drittlandübermittlungen kontrollieren sowie
- › die weisungsgebundene Verarbeitung regelmäßig überwachen.

Liegt eine gemeinsame Verantwortlichkeit vor, müssen Sie

- › eine Vereinbarung nach Art. 26 DSGVO abschließen,
- › die Aufgaben- und Verantwortungsverteilung eindeutig festlegen und dokumentieren,
- › Zuständigkeiten für Informationspflichten, Betroffenenrechte und den Umgang mit Datenschutzverletzungen regeln sowie
- › sicherstellen, dass für die gemeinsame Verarbeitung eine geeignete Rechtsgrundlage besteht.

Handelt der Dritte eigenständig verantwortlich, ist kein AV-Vertrag erforderlich. Stattdessen müssen/sollten Sie

- › prüfen, auf welcher Rechtsgrundlage personenbezogene Daten zwischen den Verantwortlichen übermittelt werden,
- › sicherstellen, dass jeder Verantwortliche seine datenschutzrechtlichen Pflichten eigenständig erfüllt, und
- › die Einordnung als getrennte Verantwortlichkeiten sowie die maßgeblichen Erwägungen nachvollziehbar dokumentieren.



Datenschutzrechtliche Verantwortung bei KI

Spätestens seit dem Durchbruch generativer KI-Systeme wie Chatbots oder Bildgeneratoren stellt sich in vielen Unternehmen dieselbe Frage: Wer trägt eigentlich die datenschutzrechtliche Verantwortung? Reicht ein AV-Vertrag mit dem KI-Anbieter aus oder liegt – zumindest für einzelne Verarbeitungsschritte – eine eigene oder sogar gemeinsame Verantwortlichkeit vor?

Auch bei KI gilt: erst die Rolle bestimmen

Eine pauschale Antwort gibt es nicht. Die DSGVO unterscheidet nicht zwischen klassischer Software und KI-Systemen. Auch beim Einsatz von KI gelten dieselben Grundsätze wie bei jeder anderen Verarbeitung personenbezogener Daten: Verantwortlich ist die Stelle, die über Zwecke und wesentliche Mittel der Verarbeitung entscheidet. Verantwortlicher kann dabei nur eine natürliche oder juristische Person, Behörde oder sonstige Stelle sein – nicht jedoch eine Software oder ein KI-System. Auch wenn moderne KI-Systeme eigenständig Inhalte generieren oder Entscheidungen vorbereiten, verbleiben die datenschutzrechtlichen Pflichten bei den beteiligten Unternehmen. Da bei KI häufig mehrere Akteure zusammenwirken, kann sich ihre datenschutzrechtliche Rolle je nach Verarbeitungsvorgang unterscheiden.

Nicht die KI, sondern jeder Verarbeitungsschritt ist zu bewerten

Ein wesentlicher Unterschied zu klassischen Softwarelösungen besteht darin, dass sich die Verarbeitung personenbezogener Daten bei KI regelmäßig in mehrere Schritte unterteilen lässt. Für jeden dieser Schritte kann die datenschutzrechtliche Verantwortlichkeit unterschiedlich ausfallen.

Verarbeitungsschritt	Wer trifft die wesentlichen Entscheidungen?	Typische datenschutzrechtliche Rolle
1. Auswahl des Daten-Inputs	Das Unternehmen entscheidet, welche personenbezogenen Daten oder Dokumente in die KI eingegeben werden.	Verantwortlicher ist regelmäßig der Nutzer der KI.
2. Verarbeitung durch das KI-System	Abhängig von der technischen Ausgestaltung und den vertraglichen Regelungen	Auftragsverarbeitung oder – für einzelne Verarbeitungsvorgänge – eigene Verantwortlichkeit des KI-Anbieters
3. Nutzung des Daten-Outputs	Das Unternehmen entscheidet, ob und wie die KI-Ergebnisse weiterverwendet werden.	Verantwortlicher bleibt grundsätzlich der Nutzer.

Gerade diese differenzierte Betrachtung übersehen viele Unternehmen in der Praxis. Stattdessen wird der Einsatz einer KI-Anwendung häufig pauschal einer einzigen datenschutzrechtlichen Rolle zugeordnet. Tatsächlich ist die Rollenverteilung für jeden Verarbeitungsvorgang gesondert zu bestimmen. Dieselbe KI-An-

wendung kann daher unterschiedliche Verarbeitungstätigkeiten unterstützen, für die jeweils eine andere datenschutzrechtliche Einordnung erforderlich ist.

Der Nutzer trägt Verantwortung für den Daten-Input

Für den Daten-Input ist regelmäßig das Unternehmen verantwortlich. Es entscheidet über die Eingabe personenbezogener Daten, den Verarbeitungszweck und den Einsatz des KI-Systems. Ein AV-Vertrag ändert an dieser Verantwortlichkeit nichts. Vor der Einführung einer KI-Anwendung sollte daher geprüft werden, ob personenbezogene Daten überhaupt erforderlich sind oder anonymisierte oder pseudonymisierte Informationen ausreichen.

Mit der Antwort der KI endet die Prüfung nicht

Auch nach der eigentlichen Verarbeitung endet die datenschutzrechtliche Verantwortung nicht. Das von der KI erzeugte Ergebnis – etwa ein Text, eine Zusammenfassung oder eine Analyse – kann wiederum personenbezogene Daten enthalten. Entscheidet Ihr Unternehmen, diesen Output weiterzuverwenden, zu speichern oder an Dritte weiterzugeben, handelt es sich um einen eigenständigen Verarbeitungsvorgang.

Die Verantwortung hierfür liegt grundsätzlich ebenfalls beim Nutzer der KI. Datenschutzbeauftragte sollten daher nicht nur den Input, sondern auch den späteren Umgang mit den generierten Ergebnissen in ihre Prüfung einbeziehen.

Praxisbeispiel KI zur Bearbeitung von Kundenbeschwerden

1. Input

Mitarbeiter übermittelt Kunden-E-Mails an den KI-Assistenten.



2. Verarbeitung

Die KI erstellt automatisch eine Zusammenfassung.



3. Output

Die Zusammenfassung wird im CRM gespeichert.

→ Datenschutzrechtlich handelt es sich um drei getrennte Verarbeitungsvorgänge, die jeweils gesondert bewertet werden müssen.

Hinweis: Datenschutzrechtlich handelt es sich um drei getrennt zu bewertende Verarbeitungsvorgänge, für die die jeweilige Rollenverteilung gesondert zu bestimmen ist. Dienen sie einem gemeinsamen Zweck, können sie dennoch als eine zusammenhängende Verarbeitungstätigkeit dokumentiert werden.

Die Rolle des KI-Anbieters: Auftragsverarbeiter oder eigener Verantwortlicher?

Während die Verantwortlichkeit des Nutzers für die Auswahl der Eingabedaten und die spätere Verwendung des Ergebnisses meist eindeutig ist, wirft die Rolle des KI-Anbieters deutlich schwierigere Fragen auf. Gerade hier zeigt sich, dass eine pauschale Einordnung als Auftragsverarbeiter häufig zu kurz greift.

Betreibt ein Unternehmen ein KI-System ausschließlich in seiner eigenen IT-Umgebung („Self-Hosted-Lösung“), ohne dass personenbezogene Daten an den Anbieter übermittelt werden, bleibt der Anbieter regelmäßig außerhalb der konkreten Datenverarbeitung. Anders verhält es sich allerdings bei cloudbasierten KI-Diensten („Software as a Service“). Hier verarbeitet der Anbieter die Eingaben des Nutzers, um die gewünschte Antwort zu erzeugen. Dies allein macht ihn jedoch noch nicht automatisch zum Verantwortlichen.

Entscheidend ist vielmehr, ob der Anbieter die Daten ausschließlich verarbeitet, um den vereinbarten Dienst bereitzustellen, oder ob er darüber hinaus eigene Zwecke verfolgt. Handelt er ausschließlich auf Weisung des Kunden und beschränkt sich die Verarbeitung auf die Erbringung der vereinbarten Leistung, spricht dies regelmäßig für eine Auftragsverarbeitung. Verwendet der Anbieter personenbezogene Daten hingegen zusätzlich zur Verbesserung seiner Modelle, zur Produktentwicklung oder für andere eigene Zwecke, verlässt er für diese Verarbeitung seine Rolle als bloßer Auftragsverarbeiter.

Für Sie als Datenschutzbeauftragten bedeutet dies: Nicht der Name des Vertrags entscheidet, sondern die tatsächliche Datenverarbeitung. Ein AV-Vertrag kann daher zwar ein wichtiges Indiz sein, ersetzt aber nicht die Prüfung der Nutzungsbedingungen und der tatsächlichen Funktionsweise des KI-Systems.

Ein Anbieter – mehrere datenschutzrechtliche Rollen

Eine Besonderheit moderner KI-Anwendungen besteht darin, dass ein Anbieter nicht zwangsläufig nur eine einzige Rolle innehat. Unterschiedliche Verarbeitungsvorgänge können datenschutzrechtlich unterschiedlich zu bewerten sein.

Gerade diese Differenzierung wird in der Praxis häufig übersehen. Nicht jede zusätzliche Verarbeitung führt automatisch dazu, dass der Anbieter insgesamt kein Auftragsverarbeiter mehr ist. Vielmehr sind die einzelnen Verarbeitungsvorgänge getrennt zu betrachten und datenschutzrechtlich gesondert zu bewerten. Maßgeblich ist dabei die tatsächliche Funktion des Anbieters im jeweiligen Verarbeitungsvorgang.

Verarbeitungsvorgang	Mögliche Rolle des KI-Anbieters
Verarbeitung des Prompts zur Erstellung einer Antwort	Häufig Auftragsverarbeiter
Speicherung von Protokoll- oder Diagnose-daten zur Fehleranalyse	Je nach Ausgestaltung Auftragsverarbeiter oder eigener Verantwortlicher
Nutzung von Eingaben oder Ausgaben zur Weiterentwicklung des KI-Modells	Regelmäßig eigene Verantwortlichkeit
Erfüllung gesetzlicher Aufbewahrungs- oder Sicherheitsanforderungen	Eigene Verantwortlichkeit für diese Verarbeitung möglich

Merke

Auch derselbe KI-Anbieter kann gleichzeitig Auftragsverarbeiter und eigener Verantwortlicher sein. Entscheidend ist, welcher Verarbeitungsvorgang betrachtet wird. Für unterschiedliche Verarbeitungen kann dieselbe Stelle unterschiedliche datenschutzrechtliche Rollen einnehmen.

Gemeinsame Verantwortlichkeit – bei KI eher die Ausnahme

Dass sowohl der Nutzer als auch der KI-Anbieter Verantwortliche sein können, führt nicht automatisch zu einer gemeinsamen Verantwortlichkeit nach Art. 26 DSGVO. Diese setzt voraus, dass beide Beteiligten gemeinsam über Zwecke oder wesentliche Mittel der Verarbeitung entscheiden. Genau daran fehlt es bei den meisten Standard-KI-Anwendungen.

Während das Unternehmen die KI etwa zur Erstellung von Texten, zur Dokumentenanalyse oder zur Unterstützung interner Prozesse einsetzt, verfolgt der Anbieter regelmäßig andere Zwecke, etwa die Bereitstellung des Dienstes oder die Weiterentwicklung seiner Modelle. Diese unterschiedlichen Zielsetzungen sprechen in der Regel gegen eine gemeinsame Verantwortlichkeit.

Anders kann die Bewertung ausfallen, wenn Anbieter und Unternehmen eine KI-Lösung gemeinsam entwickeln oder an die Bedürfnisse des Unternehmens anpassen und dabei gemeinsam festlegen, welche Daten verarbeitet und wie sie ausgewertet werden. Solche Konstellationen sind in der Praxis jedoch eher die Ausnahme.

Checkliste: Das sollten Verantwortliche – unterstützt durch Datenschutzbeauftragte – vor der Einführung einer KI-Anwendung prüfen

Prüffrage	Erledigt
Ist der Zweck der KI-Nutzung durch die zuständige Fachabteilung eindeutig festgelegt und dokumentiert?	☐
Wurde geprüft, ob personenbezogene Daten überhaupt erforderlich sind?	☐
Ist dokumentiert, welche personenbezogenen Daten in die KI eingegeben werden?	☐
Wurde jeder Verarbeitungsschritt (Input, Verarbeitung, Output) gesondert bewertet?	☐
Ist die datenschutzrechtliche Rollenverteilung nachvollziehbar dokumentiert?	☐
Liegt ein AV-Vertrag vor, sofern eine Auftragsverarbeitung angenommen wird?	☐
Stimmen AV-Vertrag, Leistungsbeschreibung und Nutzungsbedingungen überein?	☐
Verwendet der Anbieter Eingaben oder Ausgaben zusätzlich für Training oder Produktverbesserungen?	☐
Werden Protokoll-, Diagnose- oder Nutzungsdaten verarbeitet?	☐
Sind Unterauftragsverarbeiter und Drittlandübermittlungen geprüft?	☐
Sind interne Vorgaben oder Richtlinien für die KI-Nutzung vorhanden?	☐



Auflösung und Erläuterungen

Wie viele Fälle haben Sie richtig eingeordnet? Die Abgrenzung zwischen Auftragsverarbeitung, gemeinsamer Verantwortlichkeit und eigenständiger Verantwortlichkeit ist häufig anspruchsvoll. Die folgenden Erläuterungen zeigen die entscheidenden Abgrenzungskriterien.

1. Marketingkampagne mit externer Agentur

Lösung: B – gemeinsame Verantwortlichkeit

Agentur und Unternehmen gestalten die Kampagne gemeinsam und entscheiden fortlaufend über Zielgruppen, Datennutzung und Erfolgsmessung. Die Agentur setzt daher nicht nur Weisungen um, sondern wirkt an den wesentlichen Entscheidungen mit. Entwickelt ein Dienstleister das Verarbeitungskonzept gemeinsam mit Ihrem Unternehmen, genügt ein AV-Vertrag regelmäßig nicht.

2. Cloubasiertes CRM-System

Lösung: A – Auftragsverarbeitung

Für die Bereitstellung des CRM-Systems verarbeitet der Anbieter die Kundendaten ausschließlich im Auftrag Ihres Unternehmens. Die Nutzung von Diagnosedaten führt nicht automatisch zu einer eigenen Verantwortlichkeit; entscheidend ist vielmehr, ob hierfür ausschließlich anonymisierte oder aggregierte Daten oder auch personenbezogene Daten für eigene Zwecke verarbeitet werden.

3. KI-Assistenz im Unternehmen

Lösung: C – eigene Verantwortlichkeit

Ein AV-Vertrag allein entscheidet nicht über die datenschutzrechtliche Einordnung. Nutzt der Anbieter Eingaben zusätzlich zur Verbesserung seiner KI-Modelle oder für andere eigene Zwecke, handelt er insoweit eigenverantwortlich. Prüfen Sie deshalb AV-Vertrag und Nutzungsbedingungen stets gemeinsam und bewerten Sie die einzelnen Verarbeitungsvorgänge getrennt.

4. Gemeinsames Kundenportal

Lösung: B – gemeinsame Verantwortlichkeit

Beide Unternehmen bestimmen gemeinsam, welche Daten erhoben werden, welche Funktionen das Portal bietet und wie die Daten verwendet werden. Damit entscheiden sie gemeinsam über Zwecke und wesentliche Mittel der Verarbeitung. Maßgeblich ist dabei nicht die technische Umsetzung, sondern wer die datenschutzrechtlich relevanten Entscheidungen trifft.

5. Recruiting-Plattform mit KI-Unterstützung

Lösung: A – Auftragsverarbeitung

Die Bewerberdaten werden ausschließlich im Auftrag Ihres Unternehmens verarbeitet. Dass der Anbieter anonymisierte Daten zur Weiterentwicklung seiner Systeme verwendet, ändert daran grundsätzlich nichts. Prüfen Sie jedoch sorgfältig, ob tatsächlich anonymisierte oder lediglich pseudonymisierte Daten verwendet werden.

6. Externe IT-Administration

Lösung: A – Auftragsverarbeitung

Der IT-Dienstleister kann zwar auf personenbezogene Daten zugreifen, entscheidet jedoch weder über Zweck noch Art der Verarbeitung und handelt ausschließlich im Auftrag Ihres Unternehmens. Entscheidend ist dabei nicht die Häufigkeit des Zugriffs, sondern die Weisungsgebundenheit.

7. Bonusprogramm mit Kooperationspartner

Lösung: B – gemeinsame Verantwortlichkeit

Beide Unternehmen bestimmen gemeinsam über die Datenerhebung und verfolgen damit eigene wirtschaftliche Ziele. Die Datenverarbeitung bildet die Grundlage eines gemeinsamen Geschäftsmodells. Prüfen Sie daher frühzeitig, ob eine Vereinbarung nach Art. 26 DSGVO erforderlich ist.

8. Videokonferenzsystem

Lösung: C – eigene Verantwortlichkeit (für die Sicherheitsverarbeitung)

Bei der Bereitstellung des Videokonferenzdienstes spricht vieles für eine Auftragsverarbeitung. Analysiert der Anbieter darüber hinaus sicherheitsrelevante Ereignisse zum Schutz seiner Plattform und entscheidet hierüber selbst, verfolgt er eigene Zwecke und handelt eigenverantwortlich. Prüfen Sie bei Cloud-Diensten die einzelnen Verarbeitungsvorgänge getrennt, da derselbe Anbieter unterschiedliche datenschutzrechtliche Rollen einnehmen kann.

9. Steuerberater

Lösung: C – eigene Verantwortlichkeit

Steuerberater erfüllen eigene gesetzliche und berufsrechtliche Pflichten. Sie entscheiden eigenständig darüber, welche Daten sie zur Bearbeitung benötigen und wie lange diese aufzubewahren sind. Berufsgeheimnisträger handeln daher regelmäßig nicht als Auftragsverarbeiter.

10. Weitergabe von Kundendaten an einen Vertragspartner

Lösung: C – eigenständige Verantwortlichkeit

Der Vertragspartner verarbeitet die Kundendaten nicht im Auftrag Ihres Unternehmens, sondern zur Erfüllung eigener vertraglicher und gesetzlicher Pflichten. Er entscheidet eigenständig über die hierfür erforderliche Verarbeitung und handelt daher als Verantwortlicher. Die bloße Übermittlung personenbezogener Daten begründet für sich genommen keine Auftragsverarbeitung.

PROFITIEREN SIE VON DEN DIGITALEN ARBEITSHILFEN



PRIVACYXPERTS – neuer Onlinebereich



Den gesamten Inhalt von „Datenschutz aktuell“
stellen wir Ihnen auch online zur Verfügung.
Schauen Sie einfach unter www.privacyxperts.de

QR-Code scannen
und loslegen!



Ihre Vorteile im Überblick:

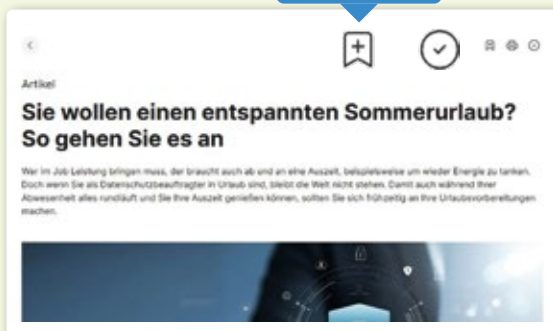
Ihr Onlinebereich bietet Ihnen alle Ausgaben und Beiträge auf einen Klick sowie zahlreiche Muster und Vorlagen zum praktischen Sofort-Download.

Alle Inhalte auf einen Blick!

Lassen Sie sich alle bisher erschienenen Ausgaben online anzeigen. Wählen Sie die gewünschten Inhalte – Ausgaben, Beiträge und Muster-Vorlagen. Laden Sie sich diese herunter oder lesen und nutzen Sie sie gleich online.



Merken



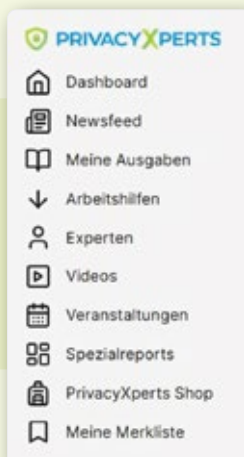
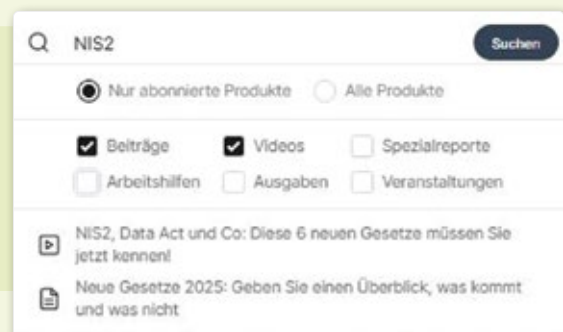
Tipp:

Setzen Sie die für Sie wichtigsten Ausgaben, Beiträge und Arbeitshilfen auf Ihre Merkliste. So haben Sie Ihre TOP-Themen immer schnell im Blick.

Praktische Suchfunktion!

Sie suchen nach etwas Bestimmtem – beispielsweise Informationen über das Thema NIS2?

Geben Sie Ihren Suchbegriff in das Suchfeld ein und wählen Sie das gewünschte Format.



Erkunden Sie Ihren Onlinebereich ...

... und entdecken Sie viele weitere, nützliche, hilfreiche und interessante Inhalte und Inklusivleistungen, die Ihren Fachratgeber optimal ergänzen. Viel Erfolg!



Telefon: 02 28 95 50 150

Fax: 02 28 36 96 480

E-Mail: kundendienst@privacyxperts.de

Internet: www.privacyxperts.de

**Ein Unternehmensbereich des VNR Verlags
für die Deutsche Wirtschaft AG
Theodor-Heuss-Straße 2–4
53177 Bonn**