DATENSCHUTZAKTUELL HERBST 2026

IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH

Themenheft:
**KI-VO, NIS2 und Co.: Ihr Wegweiser durch den Gesetzesdschungel**




# MACHEN SIE DEN PRAXISCHECK FÜR 7 TYPISCHE SITUATIONEN

**ORIENTIERUNG GEWINNEN**
Neue Digitalgesetze – was bedeutet das für Sie? 1–2

**BESTANDSAUFNAHME**
Unternehmens-Check 2026: Wie gut ist Ihr Unternehmen aufgestellt? 6–7



## *Alles im Blick bei KI-VO, NIS2 und Co.?*

*Liebe Leserin, lieber Leser,*

*der europäische Gesetzesdschungel wird dichter: KI-Verordnung (KI-VO), NIS2, Data Act, Cyber Resilience Act, Data Governance Act – wer soll da eigentlich noch den Überblick behalten?*

*2026 ist Zeit für eine Bestandsaufnahme: Viele neue Digitalgesetze stellen Unternehmen vor konkrete Herausforderungen. Prüfen Sie, wie gut Sie als Datenschutzbeauftragter und Ihr Unternehmen darauf vorbereitet sind. Testen Sie Ihr Wissen anhand konkreter Praxisfälle und machen Sie den Unternehmens-Check: Sind Zuständigkeiten und Prozesse klar geregelt? Funktioniert die Zusammenarbeit der beteiligten Bereiche?*

*Viele Grüße*



**Ihr Experte für Datenschutz**
Andreas Würtz verfügt über mehr als 20 Jahre Berufserfahrung als Vollzeit-Datenschützer im Unternehmen. Er zeigt Ihnen, wie sich Datenschutz im Unternehmen pragmatisch umsetzen lässt.

# Inhalt

**Orientierung**
Neue Digitalgesetze – was bedeutet das für Sie?
Seiten 1–2

**Überblick**
Welches Regelwerk regelt was? – Ein Überblick
Seite 3

**Wissenscheck**
Machen Sie den Praxischeck für 7 typische Situationen
Seiten 4–5

**Bestandsaufnahme**
Unternehmens-Check: Wie gut ist Ihr Unternehmen aufgestellt?
Seiten 6–7

**Auswertung**
Auflösung: Wie haben Sie abgeschnitten?
Seite 8

**Zu Ihrem Onlinebereich:**
**https://www.privacyxperts.de**

**Live-Talk:**
**https://t1p.de/live-talk**

**E-Mail-Beratung:**
**https://t1p.de/andreas-wuertz**

## Impressum

PRIVACYXPERTS

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

Verantwortlicher Chefredakteur:
RA Andreas Würtz, Freiberg am Neckar

Design: Kreativ Konzept Agentur für Werbung, Bonn
Satz: Schmelzer Medien GmbH, Siegen
Druck: Warlich Druck Meckenheim GmbH,
Am Hambuch 5, 53340 Meckenheim
Bildnachweise: Titel: KI_generiert; Seite 1: Adobe Stock | andranik123

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




Höchste Zeit, zu prüfen, ob alle Zuständigkeiten geklärt sind.

# Neue Digitalgesetze – was bedeutet das für Sie?

**Neben die Datenschutz-Grundverordnung (DSGVO) treten immer mehr europäische Digitalgesetze. KI-VO, NIS2, Data Act und Co. bringen neue Anforderungen für Unternehmen – und schaffen zugleich zahlreiche Schnittstellen zum Datenschutz. Was bedeutet das für Ihre Arbeit als Datenschutzbeauftragter? Welche Regelwerke sollten Sie kennen, wo liegen die Berührungspunkte – und wo endet Ihre Zuständigkeit?**

## Warum 2026 ein Schlüsseljahr ist

Viele neue europäische Digitalgesetze wurden bereits vor einiger Zeit verabschiedet. 2026 werden jedoch weitere wichtige Vorgaben praktisch relevant. So gelten seit dem 2. August 2026 neue Transparenzpflichten der KI-VO. Auch die Ende 2025 in Deutschland gültigen NIS2-Vorgaben müssen betroffene Unternehmen nun in der Praxis umsetzen. Für Unternehmen bedeutet das: Ein Projekt kann heute mehrere Prüfungen, Dokumentationen oder Meldepflichten auslösen.

Höchste Zeit also für einen Check: Sind die Zuständigkeiten in Ihrem Unternehmen geklärt? Arbeiten Datenschutz, IT, Informationssicherheit, Compliance und die Fachbereiche frühzeitig zusammen? Nutzen Sie diese aktuelle Ausgabe für eine Bestandsaufnahme – Ihres eigenen Wissens und der Strukturen in Ihrem Unternehmen.

## Müssen Sie jetzt alle neuen Digitalgesetze kennen?

Nein. Ihre Aufgaben als Datenschutzbeauftragter bleiben grundsätzlich die gleichen. Die DSGVO bestimmt weiterhin Ihre gesetzlichen Aufgaben. Sie beraten zu datenschutzrechtlichen Fragen, überwachen die Einhaltung der DSGVO und unterstützen unter anderem bei Datenschutz-Folgenabschätzungen. Die neuen Digitalgesetze machen Sie daher nicht automatisch zum KI-, NIS2- oder Compliance-Beauftragten.

Trotzdem sollten Sie die wichtigsten Regelwerke kennen. Denn immer häufiger treffen bei einem Projekt mehrere Anforderungen aufeinander. Für Sie kommt es deshalb vor allem darauf an, die Schnittstellen zu kennen.

Auch Vorgaben aus anderen Regelwerken können für Ihre Datenschutzprüfung wichtig sein. Sie können beispielsweise beeinflussen, wie ein System abgesichert wird, welche Informationen dokumentiert werden oder wie Daten bereitgestellt werden müssen. Das kann sich wiederum auf die Verarbeitung personenbezogener Daten auswirken. Beziehen Sie deshalb bei Ihrer Prüfung auch relevante Informationen aus anderen Fachbereichen ein.

Sie müssen nicht jede Frage selbst beantworten. Sie sollten aber erkennen, wann neben der DSGVO weitere Anforderungen eine Rolle spielen, wie diese ineinandergreifen und wer im Unternehmen zusätzlich einzubeziehen ist. Ebenso sollten Sie wissen, welche Informationen Sie aus den Fachbereichen benötigen, um die Einhaltung der Anforderungen sicherzustellen.

## KI-VO, NIS2 und Co.: So gehen Sie als Datenschutzbeauftragter vor

Ihr Unternehmen möchte ein neues KI-Tool einführen, einen Cloud-Dienst beschaffen oder Daten mit einem Geschäftspartner austauschen. Schnell stellt sich die Frage: Welche der zahlreichen neuen Vorschriften müssen dabei berücksichtigt werden?

Versuchen Sie nicht, jedes Projekt sofort anhand sämtlicher neuer Digitalgesetze zu prüfen. Gehen Sie stattdessen Schritt für Schritt vor: Klären Sie zunächst die datenschutzrechtlichen Fragen, achten Sie auf Schnittstellen zu anderen Regelwerken und holen Sie die zuständigen Stellen dazu.

**Schritt 1:** Prüfen Sie zuerst den Datenschutz

Ihre erste Frage lautet: Werden personenbezogene Daten verarbeitet?

Wenn ja, bleiben die bekannten datenschutzrechtlichen Fragen entscheidend:

- Welche personenbezogenen Daten werden verarbeitet?
- Zu welchem Zweck?
- Auf welcher Rechtsgrundlage?
- Wer erhält Zugriff?
- Werden Dienstleister eingesetzt?
- Fließen Daten in Drittländer?
- Welche Risiken bestehen für die betroffenen Personen?

**Wichtig:** Lassen Sie sich nicht von der Bezeichnung des Projekts leiten. Auch ein „KI-Projekt", ein „NIS2-Thema" oder ein Vorhaben zum Data Act kann personenbezogene Daten betreffen. Die neuen Regelwerke verdrängen die DSGVO nicht.

## Schritt 2: Erkennen Sie weitere Regelwerke

Richten Sie anschließend den Blick auf weitere mögliche Anforderungen. Auch wenn keine personenbezogenen Daten betroffen sind, können andere Digitalgesetze für das Vorhaben relevant sein. Sie müssen dafür nicht jedes Regelwerk bis ins Detail kennen. Achten Sie zunächst auf typische Auslöser:

### Übersicht: Typische Auslöser und relevante Regelwerke

| Wenn es um … geht | Denken Sie auch an … |
|---|---|
| KI-Systeme oder automatisierte Entscheidungen | KI-VO |
| Cyberangriffe oder Sicherheitsmaßnahmen | NIS2/Informationssicherheit |
| Daten aus vernetzten Produkten | Data Act |
| Produkte mit digitalen Elementen | Cyber Resilience Act |
| neue Formen des Datenaustauschs | Data Act/Data Governance Act |

Die entscheidende Frage lautet also nicht: „DSGVO oder neues Digitalgesetz?", sondern häufig: „Welche Anforderungen gelten nebeneinander?"

Welche Regelwerke welche Bereiche erfassen und wo die wichtigsten Berührungspunkte zum Datenschutz liegen, zeigt Ihnen die Übersicht auf der folgenden Seite.

## Schritt 3: Klären Sie Ihre Rolle als Datenschutzbeauftragter

Sie haben eine Schnittstelle erkannt? Dann müssen Sie die zusätzliche Rechtsfrage nicht automatisch selbst lösen. Fragen Sie stattdessen: Was gehört zu meiner Aufgabe als Datenschutzbeauftragter – und wer ist für die weiteren Anforderungen zuständig?

Sie bringen die datenschutzrechtliche Perspektive ein. Für andere Fragen können je nach Projekt beispielsweise IT, Informationssicherheit, Compliance, Rechtsabteilung oder der zuständige Fachbereich verantwortlich sein. **Merke:** Schnittstelle erkannt heißt nicht automatisch selbst zuständig. Entscheidend ist, dass Sie als Datenschutzbeauftragter die Frage erkennen und an die richtige Stelle weitergeben.

## Schritt 4: Sorgen Sie dafür, dass die richtigen Stellen früh zusammenkommen

Gerade bei Digitalprojekten reicht die Perspektive eines einzelnen Bereichs häufig nicht aus. Datenschutz, IT, Informationssicherheit, Compliance und Fachbereiche sollten deshalb nicht nacheinander, sondern möglichst früh miteinander arbeiten.

Klären Sie gemeinsam: Was ist geplant? Welche Daten und Systeme sind betroffen? Welche Anforderungen kommen in Betracht? Wer prüft was? Und welche Maßnahmen sind vor der Einführung erforderlich?

Dabei müssen Sie nicht für jedes neue Digitalgesetz einen eigenen Prozess schaffen. Prüfen Sie vielmehr, ob sich bestehende Beschaffungs-, Freigabe-, Projekt- und Meldeprozesse nutzen oder ergänzen lassen.

### Praxistipp:

**Erfahren Sie von neuen KI-Anwendungen, Cloud-Diensten oder Datenaustauschprojekten erst kurz vor dem Produktivstart? Dann lohnt sich ein Blick auf die internen Abläufe. Sie als Datenschutzbeauftragter sollten so früh eingebunden sein, dass Sie wesentliche Entscheidungen noch beeinflussen können.**

Ob Ihr Unternehmen dafür bereits gut aufgestellt ist, können Sie mit dem Unternehmens-Check auf Seite 6–7 prüfen.

## Ihr Prüfweg auf einen Blick

Bei Ihrem nächsten Digitalprojekt helfen Ihnen vier Fragen:

1. Ist der Datenschutz betroffen?
   Werden personenbezogene Daten verarbeitet?

2. Welche weiteren Regelwerke könnten relevant sein?
   Geht es beispielsweise um KI, Cybersicherheit, Datennutzung oder vernetzte Produkte?

3. Was ist meine Aufgabe – und wer ist zusätzlich zuständig?
   Trennen Sie Ihre datenschutzrechtliche Aufgabe von den Verantwortlichkeiten anderer Bereiche.

4. Sind die richtigen Stellen frühzeitig eingebunden?
   Sorgen Sie dafür, dass die zuständigen Stellen Schnittstellen gemeinsam bewerten und Aufgaben klar verteilen.

## Jetzt sind Sie gefragt

Wenden Sie diesen Prüfweg direkt in der Praxis an: Auf Seite 4–5 erwarten Sie zehn typische Situationen aus dem Unternehmensalltag. Entscheiden Sie, welche Regelwerke eine Rolle spielen, worauf Sie als Datenschutzbeauftragter achten müssen und welche Stellen Sie einbeziehen sollten.

# Welches Regelwerk regelt was? – Ein Überblick

**Wann sollten Sie an KI-VO, NIS2, Data Act und Co. denken? Nicht jedes Regelwerk ist für jedes Projekt relevant – und nicht jede Vorgabe fällt in Ihren Aufgabenbereich. Sie müssen die neuen Digitalgesetze nicht im Detail kennen. Einen Überblick sollten Sie trotzdem haben: Nur wenn Sie wissen, worum es in den einzelnen Regelwerken geht, können Sie mögliche Schnittstellen zum Datenschutz erkennen und bei Bedarf die richtigen Ansprechpartner im Unternehmen einbeziehen.**

## Diese Regelwerke sollten Sie im Blick haben

Die folgende Übersicht zeigt Ihnen auf einen Blick, wen die wichtigsten Regelwerke betreffen, was sie regeln und warum sie für Ihre Arbeit relevant sein können.

### Übersicht: Regelwerke auf einen Blick

| Regelwerk | An wen richtet es sich? | Worum geht es? | Warum ist das für Datenschutzbeauftragte relevant? |
|---|---|---|---|
| **DSGVO** | Verantwortliche, Auftragsverarbeiter, öffentliche Stellen sowie – hinsichtlich ihrer Aufgaben – Datenschutzbeauftragte | Die DSGVO bildet den europaweit einheitlichen Rechtsrahmen für den Schutz personenbezogener Daten. Sie regelt unter anderem die Grundsätze der Datenverarbeitung, die Rechte betroffener Personen sowie die Pflichten von Verantwortlichen und Auftragsverarbeitern. | Die DSGVO bleibt die zentrale Grundlage der Tätigkeit von Datenschutzbeauftragten. Beratung, Überwachung der Einhaltung datenschutzrechtlicher Vorgaben, Unterstützung bei Datenschutz-Folgenabschätzungen sowie die Sensibilisierung der Beschäftigten gehören weiterhin zu ihren gesetzlichen Kernaufgaben. Die übrigen europäischen Regelwerke ergänzen die DSGVO, ersetzen sie jedoch nicht. |
| **KI-VO** | Anbieter, Betreiber (Deployer), Einführer und Händler von KI-Systemen sowie weitere Akteure der KI-Wertschöpfungskette | Die KI-VO schafft einen einheitlichen Rechtsrahmen für die Entwicklung, Bereitstellung und Nutzung von KI-Systemen. Welche Anforderungen gelten, hängt unter anderem von der Art des KI-Systems und der Rolle des jeweiligen Akteurs ab. | Viele KI-Anwendungen verarbeiten personenbezogene Daten. Als Datenschutzbeauftragter sollten Sie KI-Projekte frühzeitig begleiten, um datenschutzrechtliche Risiken zu bewerten und die Schnittstellen zwischen DSGVO und KI-VO zu erkennen. |
| **NIS2-Richtlinie** | Unternehmen und Einrichtungen in bestimmten besonders relevanten Sektoren; die Betroffenheit hängt unter anderem von Tätigkeit und Unternehmensgröße ab | Die NIS2-Richtlinie stärkt die Cybersicherheit in der Europäischen Union. Sie verpflichtet zahlreiche Unternehmen zu einem angemessenen Risikomanagement sowie zur Umsetzung technischer und organisatorischer Sicherheitsmaßnahmen. | Datenschutz und Informationssicherheit sind eng miteinander verknüpft. Sicherheitsvorfälle können zugleich Datenschutzverletzungen darstellen. Eine enge Zusammenarbeit zwischen Datenschutz, Informationssicherheit und IT gewinnt daher weiter an Bedeutung. |
| **Data Act** | Hersteller vernetzter Produkte, Anbieter verbundener Dienste, Dateninhaber, Nutzer und Datenempfänger sowie Anbieter von Datenverarbeitungsdiensten | Der Data Act soll den Zugang zu und die Nutzung von Daten innerhalb der Europäischen Union erleichtern und einen fairen Datenaustausch fördern. | Verarbeitet oder übermittelt das Unternehmen personenbezogene Daten, gelten weiterhin die Anforderungen der DSGVO. Datenschutzbeauftragte sollten daher insbesondere prüfen, ob die datenschutzrechtlichen Voraussetzungen für die Datenverarbeitung erfüllt sind. |
| **Cyber Resilience Act** | Hersteller, Importeure und Händler von Produkten mit digitalen Elementen | Der Cyber Resilience Act verpflichtet Hersteller digitaler Produkte, Sicherheitsanforderungen bereits bei der Entwicklung zu berücksichtigen und Sicherheitsupdates über den Produktlebenszyklus bereitzustellen. | Technische Schwachstellen können personenbezogene Daten gefährden. Für Datenschutzbeauftragte bestehen daher Schnittstellen zur Sicherheit der Verarbeitung und zur Informationssicherheit. |
| **Data Governance Act** | Öffentliche Stellen und zuständige Stellen für die Weiterverwendung bestimmter geschützter Daten, Anbieter von Datenvermittlungsdiensten sowie anerkannte datenaltruistische Organisationen | Der Data Governance Act regelt insbesondere die Weiterverwendung bestimmter geschützter Daten des öffentlichen Sektors, Datenvermittlungsdienste und Datenaltruismus. | Enthält ein Datenaustausch personenbezogene Daten, gelten weiterhin die Vorgaben der DSGVO. Als Datenschutzbeauftragter sollten Sie daher die datenschutzrechtlichen Voraussetzungen prüfen und auf klare Verantwortlichkeiten achten. |

# Machen Sie den Praxischeck für 7 typische Situationen

**Theorie verstanden – aber wie sicher sind Sie bei der Anwendung? Testen Sie Ihr Wissen anhand von sieben typischen Situationen aus dem Unternehmensalltag. Wie würden Sie vorgehen?**

## Was würden Sie entscheiden?

Nutzen Sie für die folgenden Fälle Ihren Prüfweg: Ist der Datenschutz betroffen? Welche weiteren Vorgaben könnten eine Rolle spielen? Und welche Stellen sollten Sie einbeziehen? Wählen Sie jeweils die eine richtige Antwort aus.

### 1. KI-gestützte Bewerberauswahl

Die Personalabteilung möchte eine neue Software einsetzen, die eingehende Bewerbungen automatisch analysiert. Das System soll Lebensläufe auswerten, Qualifikationen gewichten und eine Rangfolge geeigneter Bewerber erstellen. Die abschließende Entscheidung trifft weiterhin ein Mitarbeiter der Personalabteilung.

Der Anbieter stellt einen Vertrag zur Auftragsverarbeitung zur Verfügung. Ob der Anbieter die eingegebenen Daten zusätzlich zur Verbesserung des KI-Systems nutzt, geht aus den Unterlagen jedoch nicht eindeutig hervor. Wie sollte das Unternehmen vorgehen?

- ☐ Da die abschließende Auswahlentscheidung bei einem Mitarbeiter liegt, sollte zunächst geprüft werden, ob die Voraussetzungen der DSGVO einschließlich der Auftragsverarbeitung erfüllt sind. Anforderungen der KI-VO werden erst relevant, wenn das System selbst über die Auswahl von Bewerbern entscheidet.
- ☐ Neben der DSGVO können Anforderungen der KI-VO relevant sein. Zudem sollte das Unternehmen vor dem Einsatz prüfen, wie der Anbieter die Bewerberdaten verarbeitet und ob er sie für eigene Zwecke nutzt.
- ☐ Da der Anbieter einen Vertrag zur Auftragsverarbeitung anbietet, kann das Unternehmen grundsätzlich von einer Verarbeitung in seinem Auftrag ausgehen. Ob Daten zur Verbesserung des KI-Systems verwendet werden, ist vor allem im Rahmen der vertraglichen Kontrolle des Auftragsverarbeiters zu berücksichtigen.
- ☐ Datenschutz und KI-Regulierung sollten vor dem Einsatz gemeinsam geprüft werden. Da die Bewerberdaten im Verantwortungsbereich der Personalabteilung verarbeitet werden, kann diese nach Beteiligung des Datenschutzbeauftragten abschließend über den Einsatz entscheiden.

### 2. Cyberangriff auf das Unternehmensnetzwerk

Am Montagmorgen können Beschäftigte plötzlich nicht mehr auf verschiedene Server zugreifen. Kurz darauf erscheint eine Lösegeldforderung. Die IT-Abteilung geht von einem Ransomware-Angriff aus. Ob personenbezogene Daten lediglich verschlüsselt oder zuvor auch kopiert wurden, ist zunächst unklar.

Die Geschäftsleitung möchte mit der Einbindung des Datenschutzbeauftragten warten, bis ein Datenabfluss nachgewiesen ist. Was ist jetzt richtig?

- ☐ Zunächst sollte die IT klären, ob personenbezogene Daten tatsächlich abgeflossen sind. Der Datenschutzbeauftragte sollte eingebunden werden, sobald sich konkrete Hinweise auf einen solchen Abfluss ergeben.
- ☐ Datenschutz, IT und Informationssicherheit sollten den Vorfall frühzeitig gemeinsam bewerten, weil neben Sicherheitsanforderungen auch datenschutzrechtliche Meldepflichten betroffen sein können.
- ☐ Solange unklar ist, ob personenbezogene Daten kopiert wurden, sollte die technische Eindämmung des Angriffs Vorrang haben. Die Prüfung möglicher datenschutzrechtlicher Meldepflichten kann unmittelbar anschließend erfolgen.
- ☐ Zunächst sollten die möglichen Meldepflichten aufgrund der Sicherheitsregulierung geprüft werden. Ergibt die Untersuchung Hinweise auf einen Abfluss personenbezogener Daten, ist ergänzend die datenschutzrechtliche Bewertung vorzunehmen.

### 3. Schnelle Einführung eines Cloud-Dienstes

Ein Fachbereich möchte kurzfristig einen cloudbasierten Dienst zur gemeinsamen Bearbeitung von Dokumenten einführen. Beschäftigte haben bereits Testkonten angelegt und erste Dateien mit Kunden- und Beschäftigtendaten hochgeladen.

Der Anbieter sitzt in den USA. Ein Vertrag zur Auftragsverarbeitung ist verfügbar. Angaben zu Unterauftragnehmern, Speicherorten und Sicherheitsmaßnahmen wurden bislang nicht geprüft. Was sollte vor dem weiteren Einsatz geschehen?

- ☐ Das Unternehmen sollte den Einsatz umfassender prüfen: Neben Auftragsverarbeitung und Drittlandtransfer sollte es insbesondere Datenverarbeitung, Unterauftragnehmer und Sicherheitsmaßnahmen prüfen und die zuständigen Stellen einbeziehen.
- ☐ Da ein Vertrag zur Auftragsverarbeitung angeboten wird, sollte zunächst geklärt werden, ob die Voraussetzungen für einen zulässigen Drittlandtransfer erfüllt sind. Die Sicherheitsmaßnahmen können anschließend risikobasiert geprüft werden.
- ☐ Das Unternehmen sollte zunächst die Grundlage der Übermittlung in die USA prüfen. Sind die Anforderungen an den Drittlandtransfer erfüllt, können Unterauftragnehmer und Sicherheitsmaßnahmen im Rahmen der regulären Anbieterprüfung bewertet werden.
- ☐ Da bislang nur Testkonten genutzt werden, kann die Prüfung bis zum regulären Einsatz verschoben werden, sofern keine besonderen Kategorien personenbezogener Daten verarbeitet werden.

### 4. Maschinendaten weitergeben

Ein Maschinenhersteller stattet seine Produkte mit Sensoren aus. Diese erfassen Laufzeiten, Fehlermeldungen, Wartungsdaten und

Angaben zur Nutzung. Der Hersteller erhält die Daten und möchte sie künftig auch einem Geschäftspartner zur Verfügung stellen, der zusätzliche Wartungsleistungen anbietet.

Ein Teil der Daten lässt sich einzelnen Kunden oder Bedienern zuordnen. Die Fachabteilung verweist für die geplante Weitergabe auf den Data Act. Welche Einschätzung ist richtig?

- ☐ Sieht der Data Act für die betreffenden Maschinendaten eine Bereitstellung vor, bildet diese Verpflichtung zugleich die maßgebliche Grundlage für die Weitergabe. Eine zusätzliche datenschutzrechtliche Prüfung ist nur bei besonders sensiblen personenbezogenen Daten erforderlich.
- ☐ Entscheidend ist zunächst die Einordnung als Daten eines vernetzten Produkts. Fallen die betreffenden Informationen unter den Data Act, richten sich Umfang und Voraussetzungen ihrer Bereitstellung vorrangig nach diesem Regelwerk.
- ☐ Soweit sich die Daten auf Personen beziehen lassen, müssen neben den Vorgaben des Data Act weiterhin die Anforderungen der DSGVO berücksichtigt werden.
- ☐ Soweit Maschinendaten personenbezogen sind, sollte ihre Weitergabe ausschließlich nach der DSGVO beurteilt werden. Die Vorgaben des Data Act sind insoweit nur für die nicht personenbezogenen Bestandteile des Datensatzes relevant.

**5. Fehlende Sicherheitsupdates**

Das Unternehmen setzt seit mehreren Jahren ein digitales Zutrittskontrollsystem ein. Der Hersteller kündigt an, für die eingesetzte Produktversion künftig keine Sicherheitsupdates mehr bereitzustellen. Ein Austausch des Systems wäre mit erheblichen Kosten verbunden.

Die IT weist darauf hin, dass bekannte Schwachstellen möglicherweise nicht mehr geschlossen werden können. Das System verarbeitet unter anderem Namen, Berechtigungen und Zutrittszeiten von Beschäftigten. Wie sollte das Unternehmen reagieren?

- ☐ Solange für die eingesetzte Produktversion keine konkrete ausnutzbare Schwachstelle bekannt ist, kann das Unternehmen das System zunächst weiterbetreiben und die Sicherheitslage beobachten. Eine erneute Datenschutzprüfung wird erst bei einer wesentlichen Änderung der Risikolage erforderlich.
- ☐ Das Ende der Sicherheitsupdates betrifft zunächst die technische Produktsicherheit. Datenschutzrechtlicher Handlungsbedarf entsteht insbesondere dann, wenn sich daraus eine konkrete Gefährdung der Vertraulichkeit oder Integrität personenbezogener Daten nachweisen lässt.
- ☐ Da das System bereits vor Inkrafttreten neuer europäischer Produktvorgaben eingesetzt wurde, sollte zunächst geprüft werden, ob diese auf das Bestandsprodukt überhaupt Anwendung finden. Bis dahin kann die bisherige datenschutzrechtliche Bewertung fortgelten.
- ☐ Das Unternehmen sollte die daraus entstehenden Sicherheitsrisiken bewerten. Fehlende Updates können auch die Sicherheit personenbezogener Daten beeinträchtigen und damit datenschutzrechtlich relevant sein.

**6. Wer ist eigentlich für die neuen EU-Vorgaben zuständig?**

Der Geschäftsführer bittet den Datenschutzbeauftragten, künftig sämtliche Anforderungen aus KI-VO, NIS2, Data Act und Cyber Resilience Act zu überwachen. Schließlich habe der Datenschutzbeauftragte bereits Erfahrung mit europäischen Regulierungsvorgaben.

Im Unternehmen bestehen außerdem eine Informationssicherheitsabteilung und eine Compliance-Funktion. Klare Zuständigkeiten für die neuen Regelwerke wurden bislang nicht festgelegt. Wie sollten Sie als Datenschutzbeauftragter reagieren?

- ☐ Aufgrund der zahlreichen Schnittstellen zum Datenschutz kann der Datenschutzbeauftragte die Koordination der neuen Digitalgesetze übernehmen, sofern die fachliche Prüfung einzelner Anforderungen weiterhin durch die jeweils zuständigen Bereiche erfolgt.
- ☐ Der Datenschutzbeauftragte sollte seine Tätigkeit auf die DSGVO beschränken. Anforderungen anderer Digitalgesetze sollten nur berücksichtigt werden, wenn sie unmittelbar die Verarbeitung personenbezogener Daten verändern.
- ☐ Die gesetzlichen Aufgaben des Datenschutzbeauftragten richten sich weiterhin nach der DSGVO. Er sollte relevante Schnittstellen kennen und auf die Einbindung der zuständigen Stellen hinwirken; die Verantwortung für andere Regelwerke fällt ihm aber nicht automatisch zu.
- ☐ Bei bereichsübergreifenden Digitalgesetzen sollten Datenschutzbeauftragter und Compliance die Gesamtverantwortung gemeinsam übernehmen und einzelne technische Fragestellungen an die Informationssicherheit delegieren.

**7. Datenaustausch über einen Datenvermittlungsdienst**

Ein Unternehmen möchte künftig einen externen Datenvermittlungsdienst nutzen, um Daten mit Geschäftspartnern auszutauschen. Über die Plattform sollen vor allem technische und betriebliche Daten bereitgestellt werden. Ein Teil der Informationen lässt sich jedoch einzelnen Kunden oder Beschäftigten zuordnen.

Die Fachabteilung geht davon aus, dass für den Datenaustausch allein die Vorgaben des Data Governance Act maßgeblich sind. Wie ist die Situation einzuordnen?

- ☐ Erfüllt der Datenvermittlungsdienst die Anforderungen des Data Governance Act, kann das Unternehmen grundsätzlich davon ausgehen, dass die regulatorischen Voraussetzungen des Datenaustauschs erfüllt sind. Eine zusätzliche DSGVO-Prüfung ist vor allem bei besonderen Kategorien personenbezogener Daten erforderlich.
- ☐ Das Unternehmen sollte zunächst prüfen, ob der Anbieter die Anforderungen des Data Governance Act an Datenvermittlungsdienste erfüllt. Soweit dies der Fall ist, liegt die weitere datenschutzrechtliche Verantwortung für die über die Plattform erfolgende Verarbeitung grundsätzlich beim Anbieter.
- ☐ Soweit personenbezogene Daten über die Plattform ausgetauscht werden, hat die DSGVO als spezielles Datenschutzrecht Vorrang. Eine gesonderte Prüfung nach dem Data Governance Act ist für diese Daten daher grundsätzlich nicht erforderlich.
- ☐ Neben möglichen Anforderungen des Data Governance Act muss das Unternehmen weiterhin die DSGVO beachten, soweit es personenbezogene Daten verarbeitet. Zudem sollte es klären, welche Stellen den Datenaustausch weiter prüfen.

**Die Auflösung mit den richtigen Antworten und kurzen Erläuterungen finden Sie auf Seite 8.**

# Unternehmens-Check: Wie gut ist Ihr Unternehmen aufgestellt?

**Den eigenen Wissensstand haben Sie geprüft – jetzt ist Ihr Unternehmen an der Reihe. Denn neue Anforderungen zu kennen ist das eine. Entscheidend ist, ob sie im Arbeitsalltag auch ankommen: Sind Zuständigkeiten geklärt? Werden die richtigen Stellen rechtzeitig eingebunden? Und funktionieren die Abläufe, wenn mehrere Bereiche zusammenarbeiten müssen?**

## So gut ist Ihr Unternehmen aufgestellt

Mit der folgenden Checkliste nehmen Sie Organisation, Prozesse und Zusammenarbeit unter die Lupe. Prüfen Sie, was bereits gut funktioniert – und wo noch Handlungsbedarf besteht.

Dabei geht es nicht darum, einzelne gesetzliche Anforderungen erneut abzufragen. Im Mittelpunkt steht die praktische Umsetzung: Wer übernimmt Verantwortung? Wie gelangen neue Projekte zu den zuständigen Stellen? Und wie arbeiten Datenschutz, IT, Informationssicherheit, Compliance und Fachbereiche zusammen?

Nutzen Sie das Ergebnis anschließend als Ausgangspunkt für konkrete Verbesserungen. Schon kleine Anpassungen an bestehenden Beschaffungs-, Freigabe- oder Abstimmungsprozessen können helfen, neue Anforderungen frühzeitig zu erkennen und verlässlich in den Unternehmensalltag zu integrieren.

Hinweis: Die Checkliste dient der ersten Orientierung und ersetzt keine rechtliche Prüfung oder ein Audit.

Bewerten Sie jede Aussage mit:

○ Ja ○ Teilweise ○ Nein

**Checkliste: Digital-Check**

| Themenbereich/Aussage | Ja | Teilweise | Nein |
|---|---|---|---|
| **1. Organisation und Verantwortlichkeiten** | | | |
| Für die wichtigsten neuen EU-Digitalgesetze ist festgelegt, wer ihre Relevanz für das Unternehmen prüft und ihre Umsetzung verantwortet. | ○ | ○ | ○ |
| Datenschutz, IT, Informationssicherheit, Compliance und Fachbereiche wissen, für welche Aufgaben sie jeweils zuständig sind. | ○ | ○ | ○ |
| Das Unternehmen erfasst und bewertet neue regulatorische Anforderungen systematisch und ordnet sie den zuständigen Stellen zu. | ○ | ○ | ○ |
| Die Projektverantwortlichen binden den Datenschutz bei relevanten Digitalisierungsprojekten bereits in der Planungsphase ein. | ○ | ○ | ○ |
| Für bereichsübergreifende Digitalprojekte sind feste Ansprechpartner und Abstimmungswege festgelegt. | ○ | ○ | ○ |
| Die Geschäftsleitung kennt wesentliche neue Digitalvorgaben und unterstützt deren Umsetzung. | ○ | ○ | ○ |
| **2. Künstliche Intelligenz** | | | |
| Das Unternehmen kennt und dokumentiert die KI-Anwendungen, die Beschäftigte und Fachbereiche einsetzen. | ○ | ○ | ○ |
| Beschäftigte wissen, welche KI-Anwendungen sie nutzen dürfen und welche nicht. | ○ | ○ | ○ |
| Das Unternehmen prüft und genehmigt neue KI-Anwendungen nach einem festgelegten Verfahren, bevor sie zum Einsatz kommen. | ○ | ○ | ○ |
| Bei neuen KI-Anwendungen prüft der Datenschutz frühzeitig, ob und wie personenbezogene Daten verarbeitet werden. | ○ | ○ | ○ |
| Für eingesetzte KI-Systeme ist festgelegt, wer die einschlägigen Anforderungen der KI-VO prüft. | ○ | ○ | ○ |
| Beschäftigte erhalten klare Vorgaben und Schulungen für den sicheren und datenschutzgerechten Einsatz von KI. | ○ | ○ | ○ |
| **3. Informationssicherheit und NIS2** | | | |
| Das Unternehmen hat geprüft und dokumentiert, ob und in welchem Umfang NIS2 für es gilt. | ○ | ○ | ○ |
| Datenschutz und Informationssicherheit stimmen sich bei gemeinsamen Themen regelmäßig ab. | ○ | ○ | ○ |
| Für Sicherheitsvorfälle sind klare interne Melde- und Eskalationswege festgelegt. | ○ | ○ | ○ |
| Bei Sicherheitsvorfällen prüfen die zuständigen Stellen, welche gesetzlichen Meldepflichten und Fristen gelten. | ○ | ○ | ○ |
| Die zuständigen Stellen überprüfen und dokumentieren Sicherheitsrisiken und Schutzmaßnahmen regelmäßig. | ○ | ○ | ○ |
| Das Unternehmen berücksichtigt externe IT-Dienstleister bei der Bewertung von Sicherheitsrisiken und -anforderungen. | ○ | ○ | ○ |

| Themenbereich/Aussage | Ja | Teilweise | Nein |
|---|---|---|---|
| **4. Daten, Cloud und digitale Produkte** | | | |
| Das Unternehmen prüft neue Software- und Cloud-Dienste nach einem verbindlichen Verfahren, bevor es sie einführt. | ○ | ○ | ○ |
| Bei Datenaustauschprojekten klären die zuständigen Stellen, welche Daten betroffen sind und welche rechtlichen Anforderungen für deren Nutzung oder Weitergabe gelten. | ○ | ○ | ○ |
| Bei Daten aus vernetzten Produkten prüfen die zuständigen Stellen, ob Anforderungen des Data Act zu berücksichtigen sind. | ○ | ○ | ○ |
| Für Produkte mit digitalen Elementen ist festgelegt, wer die Anforderungen des Cyber Resilience Act prüft. | ○ | ○ | ○ |
| Der Datenschutz prüft internationale Übermittlungen personenbezogener Daten vorab datenschutzrechtlich. | ○ | ○ | ○ |
| Die zuständigen Stellen überprüfen Verträge, Zugriffsrechte und technische Schutzmaßnahmen für eingesetzte Dienste regelmäßig. | ○ | ○ | ○ |
| **5. Prozesse, Dokumentation und Kontrolle** | | | |
| Bei neuen gesetzlichen Anforderungen prüfen die zuständigen Stellen, welche bestehenden Prozesse und Dokumentationen sie anpassen müssen. | ○ | ○ | ○ |
| Beschaffungs- und Freigabeprozesse sehen feste Prüfpunkte für Datenschutz und weitere relevante Digitalvorgaben vor. | ○ | ○ | ○ |
| Die zuständigen Stellen stoßen Datenschutz-Folgenabschätzungen und andere erforderliche Risikoprüfungen frühzeitig an. | ○ | ○ | ○ |
| Das Unternehmen informiert und schult Beschäftigte zu den Datenschutz-, Sicherheits- und Digitalthemen, die für ihre Tätigkeit relevant sind. | ○ | ○ | ○ |
| Die zuständigen Stellen dokumentieren beschlossene Maßnahmen, weisen sie Verantwortlichen zu und verfolgen ihre Umsetzung nach. | ○ | ○ | ○ |
| Das Unternehmen nutzt Erkenntnisse aus Projekten, Prüfungen und Vorfällen, um bestehende Prozesse zu verbessern. | ○ | ○ | ○ |

## Auswertung

**Ja = 2 Punkte, Teilweise = 1 Punkt, Nein = 0 Punkte**

**51–60 Punkte: Bleiben Sie am Ball**

Ihr Unternehmen verfügt bereits über klare Verantwortlichkeiten und etablierte Abläufe für neue Digitalthemen. Die relevanten Bereiche stimmen sich frühzeitig und strukturiert miteinander ab.

Ruhen Sie sich darauf aber nicht aus: Prüfen Sie regelmäßig, ob neue regulatorische Entwicklungen Anpassungen erfordern und ob die festgelegten Prozesse auch in der Praxis funktionieren. Achten Sie besonders auf einzelne Aussagen, die Sie noch mit „Teilweise" oder „Nein" beantwortet haben.

**39–50 Punkte: Schließen Sie einzelne Lücken**

Viele wichtige Strukturen und Prozesse sind bereits vorhanden. An einzelnen Stellen gibt es aber noch Lücken.

Schauen Sie sich insbesondere Ihre „Teilweise"- und „Nein"-Antworten an: Sind Verantwortlichkeiten noch nicht eindeutig geregelt? Fehlen feste Abstimmungswege? Oder greifen bestehende Prüf- und Freigabeprozesse noch nicht bei allen Digitalprojekten? Setzen Sie dort an, wo sich mit überschaubarem Aufwand klare Verbesserungen erreichen lassen.

**24–38 Punkte: Gehen Sie die wichtigsten Lücken an**

Ihr Unternehmen hat erste Strukturen geschaffen, bei der praktischen Umsetzung bestehen jedoch noch deutliche Lücken. Dadurch besteht das Risiko, dass Ihr Unternehmen neue Anforderungen zu spät erkennt, Zuständigkeiten nicht klärt oder relevante Stellen nicht rechtzeitig einbezieht.

Setzen Sie Prioritäten: Schauen Sie zunächst auf die Themenbereiche mit den meisten „Nein"-Antworten. Legen Sie konkrete Verbesserungsmaßnahmen fest und bestimmen Sie, wer für deren Umsetzung verantwortlich ist und bis wann sie erfolgen soll.

**0–23 Punkte: Werden Sie jetzt aktiv**

Die grundlegenden Strukturen für den Umgang mit neuen Digitalanforderungen fehlen noch oder sind bislang nur punktuell vorhanden.

Beginnen Sie mit einer Bestandsaufnahme: Welche neuen Regelwerke betreffen Ihr Unternehmen? Wer kümmert sich jeweils darum? Wann wird der Datenschutz eingebunden? Und wie arbeiten Datenschutz, IT, Informationssicherheit, Compliance und Fachbereiche zusammen?

Versuchen Sie nicht, alle offenen Punkte gleichzeitig zu lösen. Klären Sie zunächst die wichtigsten Verantwortlichkeiten und schaffen Sie feste Abläufe für neue Digitalprojekte. Anschließend können Sie weitere Lücken Schritt für Schritt schließen.

## So gehen Sie jetzt weiter vor

Die Gesamtpunktzahl gibt Ihnen eine erste Orientierung – wichtiger sind jedoch Ihre einzelnen Antworten.

Schauen Sie deshalb, in welchem der fünf Themenbereiche Sie besonders häufig „Teilweise" oder „Nein" angekreuzt haben.

### Praxistipp

**Wählen Sie aus Ihrem schwächsten Themenbereich zwei oder drei konkrete Punkte, die Sie zuerst angehen möchten. Legen Sie Verantwortliche, Maßnahmen und einen Zeitrahmen fest. So wird aus Ihrem Ergebnis direkt eine To-do-Liste für die Praxis.**

# Auflösung: Wie haben Sie abgeschnitten?

**Jetzt können Sie Ihre Antworten mit den Lösungen vergleichen. Lagen Sie mit Ihrer Einschätzung richtig – oder steckt in dem einen oder anderen Fall mehr, als es den Anschein hatte? Achten Sie beim Vergleich nicht nur auf die richtige Antwort. Entscheidend ist, warum neben der DSGVO weitere Vorgaben eine Rolle spielen und welche Stellen im Unternehmen einzubeziehen sind.**

### 1. KI-gestützte Bewerberauswahl

Richtig ist Antwort 2: Neben der DSGVO können Anforderungen der KI-VO relevant sein. Zudem sollte das Unternehmen prüfen, wie der Anbieter mit den Bewerberdaten umgeht.

Prüfblick: DSGVO – Bewerberdaten und Verarbeitung durch den Anbieter, Schnittstelle: KI-VO, Beteiligte: Personal, Datenschutz, ggf. Recht/Compliance

Ein AV-Vertrag allein reicht nicht. Das Unternehmen muss insbesondere prüfen, ob der Anbieter die Daten ausschließlich im Auftrag oder auch für eigene Zwecke verarbeitet.

### 2. Cyberangriff auf das Unternehmensnetzwerk

Richtig ist Antwort 2: Datenschutz, IT und Informationssicherheit sollten den Vorfall frühzeitig gemeinsam bewerten.

Prüfblick: DSGVO – mögliche Datenschutzverletzung, Schnittstelle: Informationssicherheit/NIS2, Beteiligte: Datenschutz, IT, Informationssicherheit

Ob personenbezogene Daten abgeflossen sind, steht unmittelbar nach einem Angriff häufig noch nicht fest. Trotzdem sollten Datenschutz, IT und Informationssicherheit mögliche Datenschutz- und Sicherheitsfolgen frühzeitig bewerten, die Meldefristen im Blick behalten und – je nach Schwere und Erkenntnisstand – ggf. eine vorsorgliche Meldung abgeben.

### 3. Schnelle Einführung eines Cloud-Dienstes

Richtig ist Antwort 1: Das Unternehmen sollte den Cloud-Dienst vor dem weiteren Einsatz umfassender prüfen.

Prüfblick: DSGVO – Auftragsverarbeitung und Drittlandtransfer, Schnittstelle: Informationssicherheit, Beteiligte: Datenschutz, IT, Informationssicherheit, ggf. Einkauf/Recht

Ein AV-Vertrag allein genügt nicht. Die Prüfung muss auch Datenflüsse, Unterauftragnehmer, Speicherorte und Sicherheitsmaßnahmen erfassen.

### 4. Nutzungsdaten einer vernetzten Maschine

Richtig ist Antwort 3: Soweit sich die Daten auf Personen beziehen lassen, muss das Unternehmen neben dem Data Act weiterhin die DSGVO berücksichtigen.

Prüfblick: DSGVO – Personenbezug der Nutzungsdaten, Schnittstelle: Data Act, Beteiligte: Datenschutz und die für Datennutzung/Data Act zuständigen Stellen

Entscheidend ist nicht die Bezeichnung als „Maschinendaten". Lassen sich die Daten Personen zuordnen, bleiben die Anforderungen der DSGVO neben dem Data Act bestehen.

### 5. Fehlende Sicherheitsupdates

Richtig ist Antwort 4: Das Unternehmen sollte die entstehenden Sicherheitsrisiken bewerten.

Prüfblick: DSGVO – Sicherheit personenbezogener Daten, Schnittstelle: Informationssicherheit, ggf. Produktsicherheit/Cyber Resilience Act, Beteiligte: Datenschutz, IT, Informationssicherheit

Fehlende Updates können Schwachstellen offenlassen und damit auch die Sicherheit personenbezogener Daten beeinträchtigen. Das Thema betrifft deshalb nicht allein IT oder Produktsicherheit.

### 6. Zuständigkeit für neue EU-Vorgaben

Richtig ist Antwort 3: Die neuen Digitalgesetze gehören nicht automatisch zu den Aufgaben des Datenschutzbeauftragten.

Prüfblick: DSGVO – Aufgaben des Datenschutzbeauftragten, Schnittstelle: KI-VO, NIS2, Data Act & Co., Beteiligte: je nach Thema Recht, Compliance, IT, Informationssicherheit

Der Datenschutzbeauftragte sollte relevante Schnittstellen erkennen und die zuständigen Stellen hinzuziehen. Eine Schnittstelle zu erkennen bedeutet nicht, automatisch selbst zuständig zu sein.

### 7. Datenaustausch über einen Datenvermittlungsdienst

Richtig ist Antwort 4: Neben möglichen Anforderungen des Data Governance Act ist weiterhin die DSGVO zu beachten, soweit personenbezogene Daten verarbeitet werden.

Prüfblick: DSGVO – Personenbezug und Datenweitergabe, Schnittstelle: Data Governance Act, Beteiligte: Datenschutz sowie die für Datenaustausch und Data Governance Act zuständigen Stellen

Dass ein Datenvermittlungsdienst genutzt wird, verdrängt die DSGVO nicht. Enthält der Datensatz personenbezogene Daten, müssen die datenschutzrechtlichen Anforderungen weiterhin berücksichtigt werden. Gleichzeitig ist zu klären, welche zusätzlichen Vorgaben für den Datenaustausch gelten und wer diese im Unternehmen prüft.

### Praxistipp: Nutzen Sie Ihre Fehler als Hinweis

**Schauen Sie sich die Fälle noch einmal an, bei denen Sie nicht richtig lagen. Oft liegt die Schwierigkeit nicht bei der DSGVO selbst, sondern an der Schnittstelle zu einem weiteren Regelwerk. Prüfen Sie hier künftig genauer: Welche zusätzlichen Vorgaben könnten betroffen sein und wer ist dafür zuständig? So wird aus dem Praxischeck zugleich eine persönliche Prüfliste für künftige Fälle.**

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.







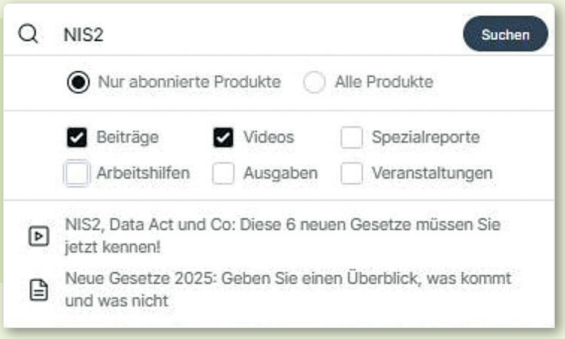
### Tipp:

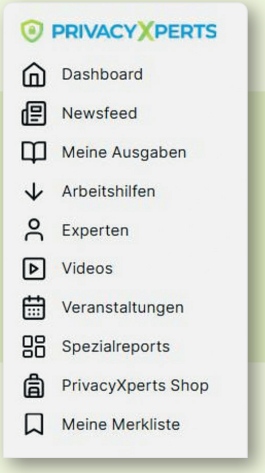
Setzen Sie die für Sie wichtigsten Ausgaben, Beiträge und Arbeitshilfen auf Ihre Merkliste. So haben Sie Ihre TOP-Themen immer schnell im Blick.

### 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!



PRIVACYXPERTS

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

## Vorschau:

Minimieren Sie die Risiken beim Einsatz von KI im Unternehmen

Alles verschlüsselt? Machen Sie den Praxischeck