DATENSCHUTZAKTUELL AUG 2026

IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH

Themenheft:
TOMs im Praxis-Check

IHRE TOMS AUF DEM PRÜFSTAND – DIESE PUNKTE SOLLTEN SIE JETZT PRÜFEN

Schutzmaßnahmen unter der Lupe

Liebe Leserin, lieber Leser,

technische und organisatorische Maßnahmen (TOMs) müssen mit den tatsächlichen Risiken Schritt halten. Neue Technologien, mobiles Arbeiten und KI-Anwendungen verändern Prozesse und Datenflüsse oft schneller als bestehende Schutzkonzepte.

Dieses Themenheft zeigt Ihnen als Datenschutzbeauftragtem, worauf Sie bei der Überprüfung Ihrer TOMs achten sollten, welche Schwachstellen in der Praxis besonders häufig übersehen werden und wie Sie mit überschaubarem Aufwand für mehr Sicherheit sorgen können.

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

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

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

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

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, 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 | JH Virtuell; Seite 1: Adobe Stock | Robert Kneschke

Erscheinungsweise: 36-mal pro Jahr
E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de
(bei Rückfragen bitte Kundennummer angeben)

Vermeiden Sie Probleme wegen veralteter TOMs.

Ihre TOMs auf dem Prüfstand

TOMs bilden das Fundament eines wirksamen Datenschutzes. In der Praxis entstehen Probleme jedoch häufig nicht, weil TOMs fehlen, sondern weil sie veraltet sind oder im Arbeitsalltag nicht konsequent umgesetzt werden. Neue Arbeitsweisen, Clouddienste und KI-Anwendungen machen eine regelmäßige Überprüfung deshalb wichtiger denn je.

TOMs sind weit mehr als reine IT-Sicherheit

TOMs bewegen sich an der Schnittstelle zwischen Informationssicherheit und Datenschutz. Die Informationssicherheit schützt sämtliche Unternehmensinformationen und verfolgt die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit. Der Datenschutz konzentriert sich dagegen auf personenbezogene Daten und die Rechte der betroffenen Personen. Viele TOMs dienen beiden Bereichen zugleich, etwa Zugriffsbeschränkungen oder Verschlüsselung. Dennoch ist nicht jede Maßnahme der Informationssicherheit automatisch datenschutzrechtlich erforderlich.

TOMs umfassen nicht nur technische Schutzmaßnahmen wie Firewalls, Passwörter oder Verschlüsselung, sondern auch organisatorische Regelungen, etwa Berechtigungskonzepte, Zuständigkeiten oder Prozesse für Datenschutzvorfälle. Welche Maßnahmen erforderlich sind, richtet sich nach den konkreten Risiken der jeweiligen Datenverarbeitung und den tatsächlichen Arbeitsabläufen im Unternehmen.

Erste Bestandsaufnahme statt Detailprüfung

Viele Unternehmen verfügen zwar über dokumentierte TOMs, überprüfen diese jedoch nur unregelmäßig oder passen sie nicht an neue Arbeitsweisen und Risiken an. Sie als Datenschutzbeauftragter sollten regelmäßig prüfen, ob bestehende Maßnahmen noch wirksam sind. Eine Bestandsaufnahme hilft dabei, vorhandene Schutzmaßnahmen zu erfassen und Handlungsbedarf zu erkennen.

Die folgende Checkliste unterstützt Sie dabei, typische Schwachstellen schnell zu identifizieren und einen Überblick über den aktuellen Stand Ihrer TOMs zu gewinnen.

Hinweis: Die folgenden Fragen dienen einer ersten Bestandsaufnahme. Je nach Unternehmensgröße und IT-Landschaft können einzelne Maßnahmen organisationsbezogen oder system- bzw. anwendungsbezogen ausgestaltet sein. Insbesondere Rollen- und Berechtigungskonzepte, Protokollierungen und Zugriffsregelungen werden in der Praxis häufig für einzelne Systeme konkretisiert.

Checkliste: Bestandsaufnahme Ihrer TOMs

Fragestellung	Hintergrundinformationen	In Ordnung?
Gibt es dokumentierte TOMs?	Unternehmen müssen nachvollziehbar festlegen, wie personenbezogene Daten geschützt werden. Fehlen dokumentierte TOMs oder bestehen diese nur aus allgemeinen Standardformulierungen, sollten Sie genauer hinschauen. Wichtig ist vor allem, dass die beschriebenen Maßnahmen tatsächlich zur konkreten Verarbeitung und zu den vorhandenen Risiken passen.	○ Ja ○ Nein
Sind die TOMs aktuell und werden sie regelmäßig überprüft?	Datenschutz ist kein Einmalprojekt. Prozesse, IT-Strukturen und Risiken verändern sich fortlaufend. Veraltete TOM-Dokumente passen daher häufig nicht mehr zu den tatsächlichen Verarbeitungen oder technischen Gegebenheiten im Unternehmen. Prüfen Sie deshalb auch, wann die Unterlagen zuletzt aktualisiert wurden.	○ Ja ○ Nein
Sind Zuständigkeiten klar geregelt?	Nicht immer ist eindeutig festgelegt, wer für Datenschutz, Informationssicherheit, Berechtigungen oder die Bearbeitung von Sicherheitsvorfällen verantwortlich ist. Unklare Verantwortlichkeiten können dazu führen, dass Aufgaben nicht umgesetzt oder Risiken nicht rechtzeitig erkannt werden. Zuständigkeiten sollten daher eindeutig dokumentiert und kommuniziert sein.	○ Ja ○ Nein

Checkliste: Bestandsaufnahme Ihrer TOMs

Fragestellung	Hintergrundinformationen	In Ordnung?
Existiert ein Rollen- und Berechtigungskonzept?	Nicht jeder Beschäftigte darf auf sämtliche personenbezogenen Daten zugreifen können. Zugriffe sollten konsequent nach dem Need-to-know-Prinzip vergeben werden. Gerade bei sensiblen Daten ist es wichtig, dass Rollen, Berechtigungen und Zuständigkeiten nachvollziehbar geregelt sind.	○ Ja ○ Nein
Werden Berechtigungen regelmäßig überprüft und angepasst?	Besonders problematisch sind unnötige Altberechtigungen oder aktive Zugänge ehemaliger Beschäftigter. Gleiches gilt für Berechtigungen von Auszubildenden oder Mitarbeitenden nach einem internen Rollenwechsel. Dadurch können Sicherheitslücken entstehen, die im Alltag oft unbemerkt bleiben.	○ Ja ○ Nein
Gibt es Vorgaben zu Passwortsicherheit und Authentifizierung?	Unternehmen sollten verbindliche Regelungen zu sicheren Passwörtern, Mehr-Faktor-Authentifizierung und Zugriffsabsicherungen schaffen. Schwache oder mehrfach verwendete Passwörter gehören weiterhin zu den häufigsten Ursachen erfolgreicher Angriffe auf Unternehmenssysteme.	○ Ja ○ Nein
Werden personenbezogene Daten verschlüsselt gespeichert und übertragen?	Prüfen Sie, ob Verschlüsselung sowohl bei der Speicherung als auch bei der Übertragung eingesetzt wird und ob die eingesetzten Verfahren dem Stand der Technik entsprechen. Besonders bei mobilen Geräten, Cloudlösungen oder externen Zugriffen sollte Verschlüsselung selbstverständlich sein.	○ Ja ○ Nein
Existieren funktionierende Back-up- und Wiederherstellungskonzepte?	Daten müssen gegen Verlust abgesichert sein. Wichtig ist nicht nur die Datensicherung selbst, sondern auch die regelmäßige Überprüfung der Wiederherstellbarkeit. Back-ups helfen wenig, wenn sich Daten im Ernstfall nicht zuverlässig zurückspielen lassen.	○ Ja ○ Nein
Gibt es ein Lösch- und Aufbewahrungskonzept?	Personenbezogene Daten dürfen nicht unbegrenzt gespeichert werden. Löschfristen und Zuständigkeiten sollten klar geregelt und praktisch umsetzbar sein. Gerade in gewachsenen IT-Strukturen sammeln sich häufig große Datenbestände an, für die keine klare Löschregelung existiert.	○ Ja ○ Nein
Werden Datenschutzvorfälle strukturiert behandelt?	Unternehmen benötigen klare Prozesse für den Umgang mit Datenschutzverletzungen, Sicherheitsvorfällen und Meldepflichten. Wichtig ist insbesondere, dass Beschäftigte wissen, an wen sie sich im Ernstfall wenden müssen und welche Schritte einzuhalten sind. Meldungen sollten zudem schnellstmöglich erfolgen, damit gesetzliche Fristen – insbesondere die 72-Stunden-Frist nach Art. 33 Datenschutz-Grundverordnung– eingehalten werden können.	○ Ja ○ Nein
Werden Beschäftigte regelmäßig geschult und sensibilisiert?	Viele Datenschutzverstöße entstehen nicht durch technische Schwächen, sondern durch Fehlverhalten, Unsicherheiten oder mangelnde Awareness. Schulungen sollten deshalb regelmäßig stattfinden und möglichst praxisnah gestaltet werden.	○ Ja ○ Nein
Gibt es Regelungen für Homeoffice und mobiles Arbeiten?	Mobile Arbeit bringt zusätzliche Risiken mit sich – etwa ungesicherte Netzwerke, private Geräte oder fehlende Zugriffsbeschränkungen. Unternehmen sollten klare Vorgaben schaffen, wie personenbezogene Daten außerhalb des Unternehmens verarbeitet werden dürfen.	○ Ja ○ Nein
Werden private Geräte oder externe Cloudspeicher genutzt?	Schatten-IT gehört zu den häufigsten Schwachstellen im Unternehmen. Beschäftigte nutzen häufig private Tools oder Speicherdienste, um Arbeitsabläufe zu vereinfachen. Genau dadurch können jedoch erhebliche Datenschutz- und Sicherheitsrisiken entstehen.	○ Ja ○ Nein
Werden Zugriffe und sicherheitsrelevante Ereignisse protokolliert?	Protokollierungen helfen nur dann weiter, wenn diese auch regelmäßig kontrolliert und ausgewertet werden. Unternehmen sollten nachvollziehen können, wer wann auf welche Daten oder Systeme zugegriffen hat.	○ Ja ○ Nein
Existieren physische Schutzmaßnahmen?	Auch Gebäude, Büroräume, Archive oder Serverräume müssen angemessen abgesichert werden, etwa gegen unbefugten Zutritt oder Diebstahl. Datenschutz endet nicht bei der IT, sondern betrifft auch die physische Sicherheit im Unternehmen.	○ Ja ○ Nein
Werden externe Dienstleister datenschutzrechtlich überprüft?	Externe Dienstleister greifen häufig auf personenbezogene Daten zu. Deshalb sollten deren Schutzmaßnahmen kritisch geprüft werden. Verlassen Sie sich dabei nicht ausschließlich auf Zertifikate oder allgemeine Datenschutzversprechen. Prüf- und Auditrechte sollten bereits bei Aufnahme der Geschäftsbeziehung schriftlich vereinbart werden.	○ Ja ○ Nein
Werden Sicherheitsupdates und Patches zeitnah eingespielt?	Veraltete Systeme gehören weiterhin zu den größten Sicherheitsrisiken und werden von Angreifern gezielt ausgenutzt. Sicherheitsupdates sollten daher zeitnah und strukturiert umgesetzt werden.	○ Ja ○ Nein
Gibt es Regelungen zur Nutzung von KI-Systemen?	KI-Anwendungen werden zunehmend im Arbeitsalltag eingesetzt. Ohne klare Vorgaben entstehen schnell Datenschutz-, Geheimhaltungs- und Compliance-Risiken. Unternehmen sollten daher verbindliche Regelungen zur Nutzung schaffen.	○ Ja ○ Nein
Ist geregelt, welche Daten in KI-Systeme eingegeben werden dürfen?	Besonders kritisch ist die Eingabe personenbezogener Daten oder sensibler Unternehmensinformationen in externe KI-Dienste. Beschäftigte unterschätzen häufig, welche Risiken hierdurch entstehen können.	○ Ja ○ Nein
Werden neue Risiken regelmäßig bewertet?	Neue Technologien, Bedrohungen und Arbeitsweisen sollten fortlaufend in die Bewertung der technischen und organisatorischen Maßnahmen einbezogen werden. Risiken verändern sich häufig schneller als bestehende Prozesse.	○ Ja ○ Nein
Werden TOMs auch praktisch kontrolliert oder nur dokumentiert?	Dokumentierte Maßnahmen allein reichen nicht aus. Entscheidend ist, ob diese im Arbeitsalltag tatsächlich umgesetzt und eingehalten werden. Zwischen Theorie und Praxis bestehen häufig erhebliche Unterschiede.	○ Ja ○ Nein
Gibt es Prozesse für das Offboarding von Beschäftigten?	Beim Ausscheiden von Mitarbeitern müssen Zugänge, Berechtigungen, Geräte und externe Zugriffe zeitnah entzogen werden. Erfolgt dies verspätet oder unvollständig, entstehen unnötige Sicherheitsrisiken.	○ Ja ○ Nein
Existieren Notfall- und Krisenkonzepte?	Unternehmen sollten vorbereitet sein, wie bei Cyberangriffen, Systemausfällen oder größeren Datenschutzvorfällen gehandelt wird. Gerade im Ernstfall zeigt sich, ob Prozesse tatsächlich funktionieren.	○ Ja ○ Nein

Wo TOMs im Arbeitsalltag häufig scheitern

Auch wenn Sie die Fragen der vorherigen Checkliste überwiegend mit „Ja" beantworten konnten, bedeutet das noch nicht automatisch, dass die TOMs im Unternehmensalltag tatsächlich wirksam funktionieren. Gerade im Datenschutz entstehen Probleme häufig nicht durch einzelne gravierende Fehler, sondern durch viele kleine organisatorische Schwachstellen im Alltag. Werden Berechtigungen nie überprüft, Dienstleister nicht kontrolliert oder neue KI-Tools unbemerkt genutzt, entstehen schnell erhebliche Risiken für Unternehmen.

Viele Schwachstellen bleiben im Alltag lange unbemerkt

Viele Probleme bleiben unbemerkt, weil Schutzmaßnahmen zwar grundsätzlich existieren, in der Praxis jedoch nicht konsequent umgesetzt oder regelmäßig überprüft werden. Genau deshalb lohnt sich der Blick auf typische Praxisfallen, die Datenschutzbeauftragten im Unternehmensalltag immer wieder begegnen.

Deshalb sollten Sie als Datenschutzbeauftragter TOMs nicht nur formal dokumentieren, sondern regelmäßig hinterfragen, wie diese tatsächlich gelebt werden. Oft zeigt sich erst im Arbeitsalltag, wo die eigentlichen Schwachstellen liegen.

Die folgende Übersicht zeigt typische Praxisfallen, die Datenschutzbeauftragte trotz grundsätzlich vorhandener TOMs immer wieder übersehen – und wie sich diese Risiken häufig bereits mit einfachen Maßnahmen deutlich reduzieren lassen.

Übersicht: Typische Praxisfallen bei TOMs

Praxisfalle	Warum das problematisch ist	Das können Sie tun
Berechtigungen wachsen über Jahre unkontrolliert an.	Beschäftigte sammeln im Laufe der Zeit häufig immer mehr Zugriffsrechte an. Alte Berechtigungen bleiben bestehen und werden selten hinterfragt.	Prüfen Sie regelmäßig bestehende Berechtigungen und lassen Sie nicht mehr benötigte Zugriffe entfernen.
Gemeinsam genutzte Accounts	Werden Benutzerkonten gemeinsam verwendet, lässt sich häufig nicht mehr nachvollziehen, wer tatsächlich auf Daten zugegriffen hat.	Setzen Sie sich für die Nutzung personenbezogener Benutzerkonten ein und hinterfragen Sie Sammelaccounts kritisch.
Löschkonzepte existieren nur auf dem Papier.	Häufig sind zwar Löschfristen definiert, technisch oder organisatorisch werden diese jedoch nicht zuverlässig umgesetzt.	Lassen Sie sich die praktische Umsetzung von Löschprozessen regelmäßig nachweisen.
Homeoffice-Regeln werden im Alltag umgangen.	Beschäftigte nutzen private Geräte, unsichere Netzwerke oder speichern Daten lokal ab, um Arbeitsabläufe zu vereinfachen.	Überprüfen Sie, ob die Vorgaben für Homeoffice tatsächlich eingehalten werden, und sensibilisieren Sie die Beschäftigten regelmäßig.
Schatten-IT bleibt lange unbemerkt.	Private Cloudspeicher, Messenger oder externe Tools werden häufig genutzt, ohne dass Datenschutz oder IT hiervon wissen.	Fragen Sie regelmäßig nach neu eingesetzten Tools und stimmen Sie sich eng mit der IT-Abteilung ab.
KI-Systeme werden spontan genutzt.	Inhalte werden schnell in KI-Tools kopiert, ohne dass klar ist, welche Daten dort verarbeitet oder gespeichert werden.	Prüfen Sie den Einsatz von KI-Anwendungen und etablieren Sie klare Nutzungsregeln.
Datenschutzvorfälle werden zu spät gemeldet.	Beschäftigte erkennen Vorfälle oft nicht oder wissen nicht, an wen sie sich wenden müssen.	Kontrollieren Sie, ob Meldewege bekannt sind, und führen Sie regelmäßige Sensibilisierungsmaßnahmen durch.
Dienstleister werden nach Vertragsabschluss kaum noch geprüft.	Veränderungen bei Unterauftragnehmern, KI-Funktionen oder Datenflüssen bleiben dadurch häufig unbemerkt.	Überprüfen Sie Auftragsverarbeiter regelmäßig und fordern Sie aktuelle Informationen zu deren TOMs sowie vorhandene Zertifizierungen (z. B. TISAX oder ISO 27001) an.
Administratorrechte werden zu großzügig vergeben.	Dauerhafte oder unnötige Adminrechte erhöhen das Risiko interner Fehlhandlungen erheblich.	Fragen Sie nach dem Berechtigungskonzept und prüfen Sie, ob Administratorrechte auf das notwendige Maß beschränkt sind.
TOM-Dokumente werden jahrelang nicht aktualisiert.	Prozesse, Software und Arbeitsweisen verändern sich deutlich schneller als bestehende Dokumentationen.	Kontrollieren Sie regelmäßig, ob die TOM-Dokumentation noch den tatsächlichen Verhältnissen und dem Stand der Technik entspricht.
Offboarding-Prozesse werden nicht konsequent umgesetzt.	Beim Ausscheiden von Beschäftigten bleiben Zugänge und Berechtigungen teilweise länger aktiv als erforderlich. Dadurch entstehen vermeidbare Sicherheitsrisiken.	Prüfen Sie stichprobenartig, ob Zugänge nach dem Ausscheiden tatsächlich deaktiviert und Berechtigungen vollständig entzogen werden.
Sicherheitsupdates werden zu spät eingespielt.	Veraltete oder ungepatchte Systeme zählen zu den häufigsten Einfallstoren für Cyberangriffe. Sicherheitslücken sind Angreifern oft bereits bekannt.	Lassen Sie sich Patch- und Updateprozesse erläutern und überprüfen Sie regelmäßig, ob Sicherheitsupdates zeitnah umgesetzt werden.
Neue Software wird eingeführt, ohne die TOMs anzupassen.	Prozesse, Datenflüsse und Risiken verändern sich häufig durch neue Anwendungen oder Funktionen. Die TOM-Dokumentation bildet diese Änderungen jedoch oft nicht mehr ab.	Kontrollieren Sie, ob bei technischen oder organisatorischen Änderungen auch die TOMs und die übrige Datenschutzdokumentation aktualisiert werden.

Externe Dienstleister: Hier sollten Sie genauer hinschauen

Unternehmen arbeiten heute in nahezu allen Bereichen mit externen Dienstleistern zusammen. Cloudanbieter, Softwareanbieter, externe IT-Dienstleister, Supportunternehmen oder Hostinganbieter greifen dabei häufig auf personenbezogene Daten zu oder verarbeiten diese im Auftrag des Unternehmens. Dabei wird in der Praxis häufig unterschätzt: Die datenschutzrechtliche Verantwortung geht regelmäßig über das eigene Unternehmen hinaus.

Die Verantwortung bleibt beim Unternehmen

Auch wenn personenbezogene Daten durch externe Dienstleister verarbeitet werden, bleibt das Unternehmen weiterhin dafür verantwortlich, dass angemessene TOMs bestehen und personenbezogene Daten ausreichend geschützt werden. Besonders relevant wird dies, wenn Dienstleister wiederum eigene Unterauftragnehmer einsetzen. Denn dadurch entstehen schnell komplexe Verarbeitungsketten, bei denen Unternehmen oft nur noch eingeschränkt nachvollziehen können,

- wer tatsächlich Zugriff auf personenbezogene Daten erhält,
- wo Daten verarbeitet werden und
- welche Schutzmaßnahmen dort tatsächlich bestehen.

Hinzu kommt, dass Unternehmen die bereitgestellten Informationen häufig zwar sammeln, jedoch nicht ausreichend bewerten. Gerade größere Cloud- oder Softwareanbieter stellen umfangreiche Datenschutzunterlagen, Zertifizierungen und Sicherheitsberichte zur Verfügung. Diese Dokumente vermitteln schnell den Eindruck eines hohen Datenschutzniveaus.

Ob die beschriebenen Maßnahmen tatsächlich zu den konkret genutzten Leistungen und den verarbeiteten personenbezogenen Daten passen, wird jedoch häufig nicht näher hinterfragt.

Sie als Datenschutzbeauftragter sollten deshalb nicht nur prüfen, ob Informationen vorliegen, sondern auch, ob diese für die jeweilige Verarbeitung tatsächlich aussagekräftig sind.

Checkliste: Diese Punkte sollten Sie bei Dienstleistern & Subunternehmen prüfen

Fragestellung	Hintergrundinformationen	In Ordnung?
Liegt ein aktueller Auftragsverarbeitungsvertrag vor?	Unternehmen sollten prüfen, ob ein AV-Vertrag vorhanden ist und ob dieser noch zu den tatsächlichen Verarbeitungen und eingesetzten Systemen passt.	○ Ja ○ Nein
Sind die TOMs des Dienstleisters ausreichend konkret beschrieben?	Allgemeine Aussagen wie „Wir schützen Daten nach dem Stand der Technik" reichen häufig nicht aus. Maßnahmen sollten nachvollziehbar und praxisnah beschrieben werden. Sofern dies nicht durch geeignete Zertifizierungen nachgewiesen wird, erfolgt die Beschreibung der TOMs typischerweise in einer Anlage zum Vertrag.	○ Ja ○ Nein
Werden Unterauftragnehmer offengelegt?	nternehmen sollten nachvollziehen können, wer tatsächlich Zugriff auf personenbezogene Daten erhält und in welchen Ländern die Verarbeitung erfolgt. Veränderungen bei eingesetzten Unterauftragnehmern sollten transparent kommuniziert werden.	○ Ja ○ Nein
Existiert ein Informationsprozess für neue Subunternehmen?	Dienstleister sollten nicht unbegrenzt neue Unterauftragnehmer einsetzen dürfen, ohne dass das Unternehmen hierüber informiert wird.	○ Ja ○ Nein
Werden Daten außerhalb der EU verarbeitet?	Gerade bei Cloud- und KI-Diensten erfolgen Verarbeitungen häufig in Drittländern. Hier sollten zusätzliche Schutzmaßnahmen geprüft werden.	○ Ja ○ Nein
Existieren SCCs oder weitere Transfermechanismen?	Erfolgt eine Datenübermittlung in Drittländer, sollten Standardvertragsklauseln oder andere geeignete Garantien vorhanden sein.	○ Ja ○ Nein
Werden KI-Systeme oder KI-Funktionen eingesetzt?	Viele moderne Dienste nutzen inzwischen KI-Funktionen im Hintergrund – etwa für Analyse, Support oder Automatisierung. Unternehmen sollten dies transparent nachvollziehen können.	○ Ja ○ Nein
Ist geregelt, ob Daten zu Trainingszwecken verwendet werden dürfen?	Besonders kritisch ist die Frage, ob eingegebene Daten zum Training von KI-Systemen genutzt werden. Die Verwendung solcher Daten zu Trainingszwecken sollte grundsätzlich ausgeschlossen und vertraglich eindeutig geregelt werden.	○ Ja ○ Nein
Existieren klare Löschregelungen?	Unternehmen sollten nachvollziehen können, wann und wie personenbezogene Daten beim Dienstleister gelöscht werden.	○ Ja ○ Nein
Werden Sicherheitsvorfälle zeitnah gemeldet?	Gerade bei externen Dienstleistern ist wichtig, dass Datenschutzverletzungen oder Sicherheitsvorfälle unverzüglich kommuniziert werden, da diese Meldepflichten des Verantwortlichen auslösen können.	○ Ja ○ Nein
Existieren Audit- oder Kontrollrechte?	Unternehmen sollten zumindest stichprobenartig überprüfen können, ob vereinbarte Schutzmaßnahmen tatsächlich umgesetzt werden.	○ Ja ○ Nein
Werden Zugriffe und Berechtigungen beim Dienstleister kontrolliert?	Auch beim Dienstleister sollten Rollen, Berechtigungen und Zugriffe nachvollziehbar geregelt sein. Unternehmen sollten sicherstellen, dass nur berechtigte Personen Zugriff auf personenbezogene Daten erhalten und Berechtigungen regelmäßig überprüft werden.	○ Ja ○ Nein

Verlassen Sie sich nicht blind auf TOM-Dokumente und Zertifikate

In der Praxis zeigt sich häufig: Viele Unternehmen verlassen sich bei Dienstleistern zu stark auf allgemeine Datenschutzversprechen, Zertifikate oder standardisierte TOM-Dokumente. Ob die beschriebenen Maßnahmen tatsächlich zur konkreten Verarbeitung passen, wird dagegen oft nicht ausreichend geprüft.

Zertifizierungen oder Testate können zwar ein wichtiger Hinweis auf etablierte Sicherheitsprozesse sein. Sie ersetzen jedoch keine datenschutzrechtliche Prüfung. Entscheidend bleibt immer, ob die Schutzmaßnahmen tatsächlich zur konkreten Verarbeitung personenbezogener Daten passen und im Arbeitsalltag wirksam umgesetzt werden.

Wussten Sie schon?

Auch eine ISO/IEC-27001-Zertifizierung bedeutet nicht automatisch, dass die TOMs eines Dienstleisters für Ihre konkrete Verarbeitung ausreichend sind. Die Zertifizierung ersetzt keine eigene Prüfung, ob die Maßnahmen zu Ihren Verarbeitungstätigkeiten und Risiken passen.

Cloud- und KI-Dienste verdienen besondere Aufmerksamkeit

Besondere Aufmerksamkeit verdienen derzeit Cloud- und KI-Dienste. Anders als klassische IT-Dienstleistungen basieren diese Angebote häufig auf komplexen technischen Infrastrukturen mit zahlreichen Unterauftragnehmern. Zudem werden Funktionen regelmäßig erweitert oder verändert. Dadurch können sich Datenflüsse, Speicherorte oder Verarbeitungsvorgänge verändern, ohne dass dies auf den ersten Blick erkennbar ist. Unternehmen sollten deshalb regelmäßig prüfen, ob neue Funktionen eingeführt wurden und welche Auswirkungen diese auf die Verarbeitung personenbezogener Daten haben. Dies gilt insbesondere für Analysefunktionen, Automatisierungen und KI-Komponenten, die zunehmend in bestehende Anwendungen integriert werden.

Praxisbeispiel: Änderungen bleiben oft unbemerkt

Ein Unternehmen nutzte einen etablierten Cloud-Dienst zur Zusammenarbeit an Dokumenten. Bei der ursprünglichen datenschutzrechtlichen Prüfung wurden die vorhandenen Zertifizierungen und TOM-Dokumente als ausreichend angesehen. Einige Monate später aktivierte der Anbieter zusätzliche KI-Funktionen, die Inhalte analysierten und teilweise durch weitere Unterauftragnehmer verarbeiten ließen. Die Änderungen waren zwar in den Nutzungsbedingungen dokumentiert, wurden intern jedoch nicht wahrgenommen. Erst bei einer späteren Überprüfung wurde festgestellt, dass sich die tatsächlichen Datenflüsse erheblich verändert hatten. Das Beispiel zeigt, dass Datenschutzprüfungen nicht mit dem Vertragsabschluss enden dürfen. Gerade bei Cloud- und KI-Diensten können sich Verarbeitungsvorgänge jederzeit ändern.

Typische Warnsignale bei TOM-Dokumenten

Nicht jedes professionell wirkende TOM-Dokument bietet automatisch ein gutes Datenschutzniveau. Gerade bei standardisierten Unterlagen sollten Sie als Datenschutzbeauftragter aufmerksam werden.

Typische Warnsignale sind beispielsweise:

- sehr allgemeine Formulierungen,
- fehlende Angaben zu konkreten Maßnahmen,
- keine Aussagen zu Unterauftragnehmern,
- keine Regelungen zu KI-Systemen,
- veraltete Dokumente oder
- identische TOMs für völlig unterschiedliche Dienstleistungen.

Gerade hier lohnt sich ein genauer Blick.

Muster: So können Sie bei Dienstleistern nachhaken

Betreff: Rückfragen zu technischen und organisatorischen Maßnahmen

Sehr geehrte Damen und Herren,

im Rahmen unserer datenschutzrechtlichen Überprüfung Ihrer technischen und organisatorischen Maßnahmen bitten wir um kurze Ergänzung bzw. Konkretisierung zu den von Ihnen bereitgestellten Unterlagen.

Insbesondere bitten wir um Informationen zu folgenden Punkten:

- Welche Unterauftragnehmer bzw. Subdienstleister setzen Sie derzeit ein?
- In welchen Ländern erfolgt die Verarbeitung personenbezogener Daten?
- Werden KI-Systeme oder KI-Funktionen im Rahmen Ihrer Dienstleistungen eingesetzt?
- Ist ausgeschlossen, dass eingegebene Daten zu Trainingszwecken von KI-Systemen verwendet werden?
- Wie werden Berechtigungen und Zugriffe auf personenbezogene Daten kontrolliert?
- Wie erfolgt die Löschung personenbezogener Daten nach Vertragsende?
- Innerhalb welcher Fristen informieren Sie über Datenschutz- oder Sicherheitsvorfälle?
- Wie häufig werden Ihre technischen und organisatorischen Maßnahmen überprüft und aktualisiert?

Vielen Dank vorab für Ihre Rückmeldung.

Mit freundlichen Grüßen

[Unternehmen/Datenschutzbeauftragter]

Das ist wichtig für die Praxis

Dokumentieren Sie Rückfragen und Antworten des Dienstleisters. So können Sie im Streitfall nachweisen, dass Sie Ihrer Kontrollpflicht nachgekommen sind. Dies gilt insbesondere bei großen IT-Dienstleistern, die häufig nur begrenzte Einblicke in ihre Sicherheitsmaßnahmen gewähren. Umso wichtiger ist es, dokumentieren zu können, welche Informationen Sie angefordert und welche Nachweise Sie eingeholt haben.

Darüber hinaus empfiehlt es sich, die Ergebnisse der Prüfung strukturiert festzuhalten. Dokumentieren Sie beispielsweise, wann die Prüfung erfolgt ist, welche Unterlagen vorlagen, welche Rückfragen gestellt wurden und ob sich daraus weiterer Handlungsbedarf ergeben hat. Eine solche Dokumentation erleichtert spätere Folgeprüfungen erheblich und unterstützt zugleich den Nachweis der datenschutzrechtlichen Rechenschaftspflicht.

10 KI-Mythen, die Ihre TOMs gefährden

Viele der zuvor dargestellten Schwachstellen zeigen sich derzeit besonders häufig beim Einsatz von KI-Systemen – etwa Schatten-IT, unkontrollierte Datenflüsse oder unzureichend geprüfte Dienstleister. KI stellt bestehende TOMs zunehmend auf den Prüfstand. Durch neue KI-Anwendungen und integrierte KI-Funktionen verändern sich Datenflüsse und Risikolagen oft erheblich. Datenschutzbeauftragte sollten daher regelmäßig prüfen, ob die vorhandenen TOMs diese Entwicklungen ausreichend berücksichtigen.

Klassische TOMs reichen oft nicht aus

Viele bestehende TOMs wurden ursprünglich für klassische IT-Systeme entwickelt. Dort lassen sich Datenflüsse, Zugriffe und Verarbeitungsschritte meist nachvollziehen. KI-Systeme funktionieren dagegen häufig dynamischer, intransparenter und verändern sich deutlich schneller. Bestehende TOMs sollten deshalb gezielt um KI-bezogene Schutzmaßnahmen ergänzt werden. Besonders kritisch ist, dass viele Risiken im Arbeitsalltag zunächst kaum auffallen. KI wird häufig spontan genutzt, neue Funktionen automatisch aktiviert und externe Tools aus Zeitdruck eingesetzt.

Hinzu kommt: Viele Unternehmen wissen inzwischen nicht mehr genau, an welchen Stellen KI bereits genutzt wird. Moderne Office-Programme, CRM-Systeme, Supporttools und Kommunikationsplattformen integrieren KI-Funktionen oft direkt in bestehende Software. Dadurch verändern sich Datenflüsse oft unbemerkt.

Mythos 1: „Unsere bisherigen TOMs reichen auch für KI-Systeme aus."

Viele Unternehmen übertragen bestehende Schutzmaßnahmen schlicht auf KI-Anwendungen. Das klingt praktisch, greift aber häufig zu kurz. KI-Systeme bringen zusätzliche Risiken mit sich, etwa unkontrollierte Dateneingaben, schwer nachvollziehbare Datenflüsse oder die mögliche Nutzung eingegebener Inhalte zu Trainingszwecken. Hinzu kommt, dass sich Funktionen und Verarbeitungsprozesse bei KI-Anwendungen oft deutlich schneller verändern als bei klassischen IT-Systemen.

So machen Sie es besser: Ergänzen Sie Ihre TOMs um klare KI-Regeln. Legen Sie fest, welche KI-Tools genutzt werden dürfen, welche Daten eingegeben werden dürfen und wie neue KI-Anwendungen freigegeben werden. Sensibilisieren Sie zudem die Beschäftigten regelmäßig für die besonderen Risiken beim Einsatz von KI-Systemen.

Mythos 2: „KI ist vor allem ein technisches Thema."

Natürlich braucht es technische Schutzmaßnahmen. In der Praxis entstehen viele KI-Risiken jedoch nicht durch fehlende Technik, sondern durch unklare Vorgaben im Arbeitsalltag. Beschäftigte nutzen KI-Systeme häufig spontan: Eine E-Mail wird eingefügt, ein Vertrag hochgeladen, eine Tabelle ausgewertet. Oft fehlt dabei das Bewusstsein, welche Daten verarbeitet werden. Besonders problematisch ist, dass Beschäftigte KI häufig als „normales Arbeitstool" wahrnehmen und Risiken deshalb unterschätzen. Genau dadurch gelangen personenbezogene Daten oder interne Informationen schnell in externe Systeme.

So machen Sie es besser: Setzen Sie nicht nur auf technische Sperren, sondern vor allem auf verständliche organisatorische Regeln. Beschäftigte sollten wissen, welche KI-Systeme freigegeben sind, welche Daten nicht eingegeben werden dürfen und wann Datenschutz oder IT einzubinden sind.

Mythos 3: „Wenn der Anbieter gute TOMs hat, sind wir abgesichert."

TOM-Dokumente von KI-Anbietern wirken oft professionell. Trotzdem sollten Unternehmen genau prüfen, ob die beschriebenen Maßnahmen zur konkreten Nutzung passen. Gerade bei KI-Systemen können Unterauftragnehmer, Speicherorte, Trainingsmechanismen oder neue Funktionen eine große Rolle spielen.

Viele Unternehmen verlassen sich hier zu stark auf Zertifikate oder allgemeine Datenschutzversprechen.

So machen Sie es besser: Prüfen Sie Anbieter-TOMs gezielt auf KI-spezifische Punkte: Werden Eingaben gespeichert? Werden Daten zu Trainingszwecken genutzt? Welche Unterauftragnehmer sind eingebunden? In welchen Ländern findet die Verarbeitung statt? Gibt es Konfigurationsmöglichkeiten für mehr Datenschutz?

Mythos 4: „Ein KI-Verbot löst das Problem."

Ein pauschales Verbot wirkt auf den ersten Blick konsequent. In der Praxis führt es aber häufig dazu, dass Beschäftigte KI trotzdem nutzen – nur eben mit privaten Accounts oder kostenlosen Tools außerhalb jeder Kontrolle. Genau daraus entsteht sogenannte Shadow AI (Schatten-KI).

Dadurch verlieren Unternehmen schnell den Überblick darüber,

- welche Daten verarbeitet werden,
- wo Daten gespeichert werden und
- welche Dienste tatsächlich genutzt werden.

So machen Sie es besser: Schaffen Sie sichere und praktikable Alternativen. Legen Sie fest, welche KI-Anwendungen genutzt werden dürfen, für welche Zwecke sie geeignet sind und welche Daten dort verarbeitet werden dürfen. Kommunizieren Sie diese Vorgaben klar und verständlich. So behalten Unternehmen eher die Kontrolle, als wenn sie nur verbieten.

Mythos 5: „Unsere Beschäftigten geben schon keine sensiblen Daten ein."

Viele Datenschutzprobleme entstehen nicht absichtlich, sondern im Arbeitsalltag. Beschäftigte wollen Zeit sparen und kopieren schnell Inhalte in ein KI-Tool: Kundennachrichten, Bewerbungsunterlagen, Vertragsentwürfe, Gesprächsnotizen oder interne Reports. Dass darin personenbezogene oder vertrauliche Informationen enthalten sind, wird oft erst zu spät erkannt. Häufig fehlt zudem das Bewusstsein dafür, welche Daten als sensibel oder schutzwürdig einzustufen sind.

Gerade bei KI-Systemen unterschätzen viele Beschäftigte außerdem, dass eingegebene Inhalte möglicherweise gespeichert, weiterverarbeitet oder zu Trainingszwecken genutzt werden können.

So machen Sie es besser: Formulieren Sie klare Eingaberegeln. Personenbezogene Daten, vertrauliche Unternehmensinformationen und Geschäftsgeheimnisse sollten grundsätzlich nicht in externe KI-Systeme eingegeben werden, sofern deren Nutzung nicht ausdrücklich freigegeben und datenschutzrechtlich geprüft wurde. Sensibilisieren Sie Beschäftigte regelmäßig für die damit verbundenen Risiken.

Mythos 6: „KI in bestehender Software ist kein eigenes Thema."

Viele Unternehmen denken bei KI nur an eigenständige Tools. Tatsächlich werden KI-Funktionen aber zunehmend direkt in bestehende Software integriert – etwa in Office-Anwendungen, CRM-Systeme, Supporttools oder Videokonferenzdienste. Dadurch können sich Datenflüsse verändern, ohne dass dies sofort auffällt.

Besonders kritisch ist dabei, dass neue KI-Funktionen häufig automatisch aktiviert oder bei Updates ergänzt werden. Unternehmen bemerken deshalb teilweise gar nicht, dass zusätzliche Daten verarbeitet oder externe Dienste eingebunden werden.

So machen Sie es besser: Prüfen Sie nicht nur neue KI-Tools, sondern auch neue Funktionen in vorhandener Software. Hinterfragen Sie bei Updates, ob KI-Komponenten aktiviert wurden, ob zusätzliche Daten verarbeitet werden und ob neue Unterauftragnehmer eingebunden sind.

Mythos 7: „KI-TOMs müssen nur einmal geprüft werden."

KI-Systeme entwickeln sich deutlich schneller als klassische Software. Anbieter ändern Funktionen, Datenflüsse und Nutzungsbedingungen häufig. Schutzmaßnahmen, die heute ausreichen, können morgen schon lückenhaft sein. Hinzu kommt, dass neue KI-Funktionen oft unbemerkt integriert werden. Gerade deshalb sollten Unternehmen KI-TOMs nicht als Ergebnis einer einmaligen Prüfung verstehen, sondern als fortlaufenden Prozess.

So machen Sie es besser: Überprüfen Sie regelmäßig, ob eingesetzte KI-Systeme noch zur ursprünglichen Bewertung passen. Besonders wichtig ist eine erneute Prüfung bei neuen Funktionen, geänderten Datenflüssen, neuen Unterauftragnehmern oder erweiterten Einsatzbereichen. Prüfen Sie dabei auch, ob die eingesetzten TOMs weiterhin dem Stand der Technik entsprechen, insbesondere da technische und organisatorische Schutzmaßnahmen zunehmend selbst auf KI-basierte Verfahren zurückgreifen.

Mythos 8: „Protokollierung ist bei KI nicht so wichtig."

Gerade bei KI-Anwendungen ist oft schwer nachvollziehbar, welche Informationen eingegeben und wofür Ergebnisse verwendet wurden. Fehlt jede Nachvollziehbarkeit, können Unternehmen problematische Nutzungen kaum erkennen oder aufklären.

Besonders bei sensiblen Prozessen oder personenbezogenen Daten kann dies erhebliche Risiken verursachen.

So machen Sie es besser: Prüfen Sie, ob und in welchem Umfang eine datenschutzkonforme Protokollierung sinnvoll ist. Besonders bei sensiblen Einsatzbereichen sollten Unternehmen nachvollziehen können, welche KI-Systeme genutzt werden, wer Zugriff hat und ob Vorgaben eingehalten werden.

Mythos 9: „KI-Ausgaben werden schon richtig sein."

Gerade weil KI-Systeme oft professionell und überzeugend formulieren, werden Ergebnisse im Arbeitsalltag schnell ungeprüft übernommen. Dabei können KI-Ausgaben fehlerhaft, veraltet, diskriminierend oder datenschutzrechtlich problematisch sein. Besonders kritisch wird dies, wenn Entscheidungen oder externe Kommunikation unmittelbar auf KI-Ergebnissen basieren.

Hinzu kommt: Viele Unternehmen regeln zwar die Nutzung von KI-Systemen, nicht jedoch den Umgang mit den erzeugten Ergebnissen.

So machen Sie es besser: Legen Sie klare Prozesse für die Prüfung von KI-Ausgaben fest. Beschäftigte sollten wissen, wann Ergebnisse kontrolliert, freigegeben oder manuell überprüft werden müssen. Gerade bei sensiblen Themen, personenbezogenen Daten oder externen Veröffentlichungen sollte KI nicht ohne menschliche Kontrolle eingesetzt werden.

Mythos 10: „Datenschutzbeauftragte müssen KI nicht aktiv begleiten."

In vielen Unternehmen werden KI-Anwendungen direkt durch Fachabteilungen eingeführt – häufig ohne frühzeitige Einbindung von Datenschutz oder IT. Dadurch werden Risiken oft erst erkannt, wenn Systeme bereits genutzt werden oder personenbezogene Daten verarbeitet wurden. Besonders problematisch ist dabei, dass KI-Projekte häufig sehr dynamisch verlaufen und sich Funktionen oder Einsatzbereiche schnell verändern.

Merken Sie sich

KI erfordert nicht völlig neue TOMs. Bestehende Schutzmaßnahmen müssen jedoch um klare Nutzungsregeln, Freigabeprozesse, Anbieterprüfungen und regelmäßige Kontrollen ergänzt werden.

So machen Sie es besser: Datenschutzbeauftragte sollten möglichst frühzeitig in KI-Projekte eingebunden werden – nicht erst nach der Einführung. Sinnvoll sind klare Freigabeprozesse, regelmäßige Abstimmungen mit IT und Fachabteilungen sowie feste Ansprechpartner für KI-Themen.

4-Wochen-Aktionsplan: So bringen Sie Ihre TOMs auf Stand

TOMs lassen sich im Unternehmensalltag nur selten „nebenbei“ überprüfen. Wer alle TOMs gleichzeitig prüfen will, verliert schnell den Überblick. Sinnvoller ist es, strukturiert und schrittweise vorzugehen. Bereits mit überschaubarem Aufwand lassen sich häufig erhebliche Schwachstellen erkennen und erste Verbesserungen umsetzen. Der folgende 4-Wochen-Aktionsplan greift die zentralen Prüffelder dieses Themenhefts auf – von der allgemeinen TOM-Prüfung über typische Praxisfallen bis hin zu Dienstleistern und KI-Systemen. So können Sie die in diesem Themenheft identifizierten Schwachstellen systematisch prüfen und Schritt für Schritt beheben.

Woche 1: Verschaffen Sie sich einen Überblick

Starten Sie mit der vorhandenen Dokumentation. Nutzen Sie zunächst die Checkliste auf Seite 1–2 dieses Themenhefts als erste Bestandsaufnahme. Prüfen Sie, welche TOM-Unterlagen im Unternehmen existieren, wann diese zuletzt aktualisiert wurden und ob sie noch zu den tatsächlichen Verarbeitungen passen. Gerade ältere Dokumente enthalten häufig allgemeine Standardformulierungen, die mit den aktuellen Arbeitsabläufen kaum noch übereinstimmen.

Sichten Sie außerdem:

- Richtlinien,
- Berechtigungskonzepte,
- Löschregelungen,
- Homeoffice-Vorgaben,
- AV-Verträge und Sicherheitskonzepte sowie Regelungen zur Nutzung von Cloud- und KI-Diensten.

Notieren Sie direkt, wo Unterlagen fehlen, veraltet sind oder nicht mehr zum aktuellen Stand der Technik passen.

Woche 2: Prüfen Sie die Umsetzung im Arbeitsalltag

Im nächsten Schritt sollten Sie die tatsächliche Umsetzung der Maßnahmen überprüfen. Denn gerade bei TOMs zeigt sich häufig: Dokumentation und Praxis stimmen nicht immer überein.

Sprechen Sie deshalb mit Beschäftigten und Fachabteilungen. Lassen Sie sich typische Arbeitsabläufe zeigen und prüfen Sie stichprobenartig:

- Berechtigungen,
- Löschroutinen,
- Homeoffice-Regelungen,
- mobile Geräte,
- Meldewege für Datenschutzvorfälle,
- die tatsächliche Nutzung von Cloud- und KI-Diensten.

Orientieren Sie sich dabei insbesondere an den typischen Praxisfallen auf Seite 3. Besonders dort finden sich Schwachstellen, die trotz vorhandener TOM-Dokumentation häufig übersehen werden.

Gerade kurze Praxisprüfungen liefern oft wertvollere Erkenntnisse als umfangreiche Dokumentationen. Und sie zeigen, wo tatsächlich Handlungsbedarf besteht.

Woche 3: Nehmen Sie Dienstleister genauer unter die Lupe

Externe Dienstleister gehören inzwischen zu den größten Risikofaktoren im Datenschutz. Gleichzeitig verlassen sich viele Unternehmen zu stark auf Zertifikate oder standardisierte TOM-Dokumente.

Prüfen Sie deshalb insbesondere:

- eingesetzte Unterauftragnehmer,
- Drittlandtransfers,
- Kontrollrechte,
- Löschregelungen sowie
- den Einsatz von KI-Funktionen oder Clouddiensten.

Nutzen Sie hierfür die Checkliste auf Seite 4–5 und stellen Sie bei Bedarf gezielte Rückfragen anhand des dort enthaltenen Musterschreibens.

Scheuen Sie sich nicht, bei unklaren Angaben gezielt nachzufragen. Viele Schwachstellen werden erst sichtbar, wenn konkrete Rückfragen gestellt werden.

Woche 4: Klären Sie die tatsächliche KI-Nutzung im Unternehmen

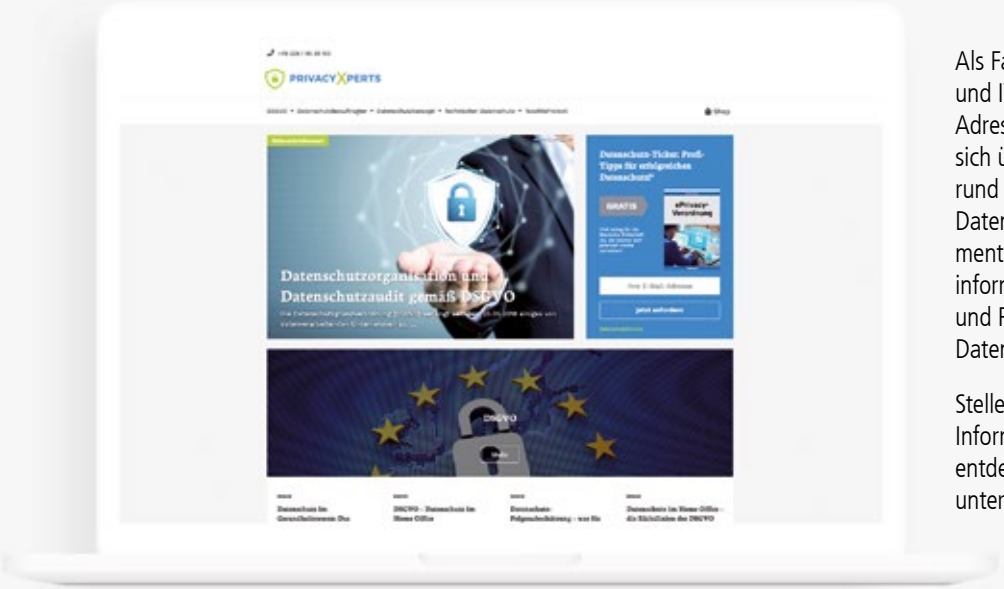
In vielen Unternehmen wird KI bereits deutlich intensiver genutzt als Verantwortlichen bewusst ist. Beschäftigte verwenden KI-Anwendungen für Texte, Übersetzungen, Auswertungen oder Recherchen – häufig spontan und ohne klare Vorgaben.

Sprechen Sie deshalb aktiv mit Fachabteilungen:

- Welche KI-Systeme werden genutzt?
- Welche Daten werden dort eingegeben?
- Gibt es private oder kostenlose KI-Accounts?
- Werden KI-Funktionen innerhalb bestehender Software verwendet?
- Nutzen Beschäftigte weitere KI-Tools, die bislang nicht offiziell freigegeben wurden?

Die auf Seite 6–7 dargestellten KI-Irrtümer bieten hierfür gute Anhaltspunkte. Prüfen Sie insbesondere, ob die dort beschriebenen Risiken auch in Ihrem Unternehmen bestehen. Prüfen Sie außerdem, ob zusätzliche KI-bezogene TOMs erforderlich sind – etwa Richtlinien, Freigabeprozesse oder Vorgaben zu sensiblen Dateneingaben.

„Datenschutz aktuell“ ist ein Produkt der PrivacyXperts-Familie!



Als Fachverlag für Beratung im Bereich Datenschutz und IT-Security sind Sie bei uns genau an der richtigen Adresse, wenn es um Ihre Themen geht. Lassen Sie sich über unsere Fachinformationsdienste und Portale rund um neue EU-Verordnungen, aktuelle Urteile zum Datenschutzrecht oder über die umfangreichen Dokumentationspflichten für Datenschutzverantwortliche informieren. So erhalten Sie nützliche Informationen und Praxistipps für Ihre Arbeit und sind beim Thema Datenschutz bestens aufgestellt.

Stellen Sie eine direkte Verbindung zu verlässlichen Informationen und aktuellen Entwicklungen her und entdecken Sie viele weitere Datenschutz-Produkte unter **www.privacyxperts.de/shop**

Schnell und effektiv Mitarbeiter schulen!

Jetzt Mitarbeiterinformation bestellen

https://t1p.de/gmxhs

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