DATENSCHUTZAKTUELL
JUNI 2026
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH

**Themenheft: DSFA bei KI**
**Risiken erkennen, richtig bewerten, sicher umsetzen**

# DSFA BEI KI-SYSTEMEN: WANN SIE WIRKLICH ERFORDERLICH IST



Onlinebereich: https://www.privacyxperts.de
E-Mail-Beratung: https://t1p.de/anna-mauch
PRIVACYXPERTS

## *KI im Einsatz – wer behält die Risiken im Blick?*

*Liebe Leserin, lieber Leser,*

*künstliche Intelligenz (KI) erleichtert Prozesse und beschleunigt Entscheidungen. Dabei entstehen Risiken, die nicht immer sofort erkennbar sind.*

*Genau hier ist Ihr Blick als Datenschutzbeauftragter gefragt: Sie müssen entscheiden, wann eine Datenschutz-Folgenabschätzung (DSFA) erforderlich ist und wie sie durchzuführen ist. Gerade bei KI-Systemen gibt es zahlreiche Besonderheiten und Risiken, die Sie kennen sollten. Und dann ist da auch noch die neue KI-Verordnung (KI-VO), die zusätzliche Anforderungen mit sich bringt.*

*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**

**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 | M.Dörr & M.Frommherz;
Seite 1: Adobe Stock | m.mphoto

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

Prüfen Sie bei KI-Systemen, ob eine DSFA erforderlich ist.

# DSFA bei KI-Systemen: Wann Sie tätig werden müssen

**Der Einsatz von KI-Systemen gehört in vielen Unternehmen längst zum Alltag. Damit stellt sich auch immer häufiger die Frage: Ist hier eine DSFA erforderlich? Gerade bei KI-Systemen ist das nicht immer auf den ersten Blick klar. Denn oft gehen mit ihrem Einsatz besondere Risiken einher, die Sie sorgfältig prüfen müssen. Im Folgenden zeigen wir Ihnen, wann eine DSFA erforderlich ist und welche Kriterien in der Praxis entscheidend sind.**

## KI-Systeme bewerten: Wann eine DSFA notwendig ist

Ob beim Einsatz von KI-Systemen eine Datenschutz-Folgenabschätzung (DSFA) erforderlich ist, richtet sich nach Art. 35 Datenschutz-Grundverordnung (DSGVO). Maßgeblich ist, ob eine Verarbeitung – insbesondere unter Einsatz neuer Technologien – voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt.

Die DSGVO ist technologieneutral formuliert: Entscheidend ist nicht der Einsatz von KI als solcher, sondern die damit verbundenen Risiken. KI-Systeme führen daher nicht per se zu einer DSFA, sondern typischerweise dann, wenn sie mit risikobehafteten Verarbeitungsvorgängen verbunden sind – etwa durch Profiling, automatisierte Entscheidungen oder die Verarbeitung großer Datenmengen.

Die DSGVO nennt hierzu typische Fallgruppen. Eine DSFA ist insbesondere erforderlich bei

- Profiling oder sonstiger Bewertung persönlicher Aspekte,
- umfangreicher Verarbeitung besonderer Kategorien personenbezogener Daten,
- systematischer umfangreicher Überwachung öffentlich zugänglicher Bereiche.

Zusätzlich nennt die Datenschutzkonferenz (DSK) in ihrer sogenannten Positivliste unter anderem den Einsatz von KI zur Steuerung der Interaktion mit Betroffenen oder zur Bewertung persönlicher Aspekte als DSFA-pflichtig.

Typische Beispiele sind:

- KI-gestützte Chatbots mit verhaltensabhängiger Interaktion,
- personalisierte Werbung auf Basis von Nutzerprofilen,
- KI-gestützte Bewerberauswahl und Rankingverfahren.

Die Positivliste ist zwar kein Gesetz, wird von den Aufsichtsbehörden aber als maßgeblicher Prüfungsmaßstab herangezogen.

Ergänzend lohnt sich ein Blick auf die Blacklists der Landesdatenschutzbehörden. Sie nennen Verarbeitungstätigkeiten, für die zwingend eine DSFA durchzuführen ist. Auch wenn sie häufig auf öffentliche Stellen zugeschnitten sind, liefern sie wertvolle Anhaltspunkte – insbesondere bei KI-Anwendungen.

Für Sie als Datenschutzbeauftragten gilt: Nutzen Sie Positivliste und Blacklists als Orientierung. Sie ersetzen keine Einzelfallprüfung, geben aber eine klare Richtung vor.

## Schwellwertanalyse: So erkennen Sie ein hohes Risiko

Ist die DSFA-Pflicht nicht bereits eindeutig – etwa durch gesetzliche Regelbeispiele oder eine Positivliste –, erfolgt eine Schwellwertanalyse. Dabei wird geprüft, ob die geplante Verarbeitung voraussichtlich ein hohes Risiko im Sinne von Art. 35 DSGVO mit sich bringt.

In der Praxis ist dies Teil eines festen Prüfprozesses für jede Verarbeitungstätigkeit. Liegt ein sogenannter Listenfall vor, kann die Prüfung entsprechend verkürzt werden.

Orientierung bieten dabei die Kriterien der ehemaligen Artikel-29-Datenschutzgruppe (heute: Europäischer Datenschutzausschuss – EDPB). Maßgebliche Anhaltspunkte sind insbesondere

die Bewertung oder Profiling von Personen, die automatisierte Entscheidungsfindung mit rechtlicher oder vergleichbarer Wirkung, die Verarbeitung großer Datenmengen, eine Zusammenführung unterschiedlicher Datenquellen oder der Einsatz neuer oder innovativer Technologien.

Treffen mehrere dieser Kriterien zu, spricht dies regelmäßig für das Vorliegen eines hohen Risikos. Gerade bei KI-Anwendungen sind häufig mehrere dieser Faktoren gleichzeitig erfüllt, sodass auch außerhalb der ausdrücklich genannten Regelbeispiele und der Positivliste in vielen Fällen eine DSFA durchzuführen ist.

## Checkliste: DSFA-pflichtige KI-Systeme erkennen

Die folgende Checkliste dient als Orientierung zur Einschätzung eines hohen Risikos nach Art. 35 DSGVO, ohne starres Punktesystem. Je mehr risikobehaftete Kriterien – insbesondere „rote Flaggen" wie Profiling, automatisierte Entscheidungen, sensible Daten oder intransparente KI-Systeme – vorliegen, desto eher ist eine DSFA erforderlich. Entscheidend bleibt stets die Gesamtabwägung im Einzelfall, insbesondere im Hinblick auf Eingriffsintensität, Schadenspotenzial und Einflussmöglichkeiten der Betroffenen.

| Prüffrage/Konkretisierung | Einordnung / Risikoaspekt (mit Beispiel) | Bewertung |
|---|---|---|
| Werden Personen durch das System bewertet, eingestuft oder priorisiert? | Klassischer DSFA-Auslöser (z. B. automatisches Ranking von Bewerbern anhand von Lebenslaufdaten) | ○ Ja ○ Nein |
| Werden persönliche Aspekte analysiert (z. B. Verhalten, Leistung, Interessen, Zuverlässigkeit)? | Profiling im weiteren Sinne (z. B. Auswertung von Klickverhalten zur Erstellung von Nutzerprofilen im Onlineshop) | ○ Ja ○ Nein |
| Fließen die KI-Ergebnisse unmittelbar in Entscheidungen ein? | Direkte Eingriffsintensität (z. B. automatisierte Entscheidung über Kreditvergabe ohne weitere Prüfung) | ○ Ja ○ Nein |
| Besteht die Gefahr fehlerhafter oder „halluzinierter" Ergebnisse? | Fehlerrisiko (z. B. KI generiert unzutreffende Inhalte oder Bewertungen) | ○ Ja ○ Nein |
| Haben die Entscheidungen rechtliche oder vergleichbar erhebliche Auswirkungen? | Zentrale Schwelle (z. B. Ablehnung eines Versicherungsvertrags oder Kündigung eines Vertrags) | ○ Ja ○ Nein |
| Ist die menschliche Kontrolle nur formal oder eingeschränkt? | Scheinbare Kontrolle (z. B. Mitarbeitende bestätigen KI-Vorschläge regelmäßig ohne eigene Prüfung) | ○ Ja ○ Nein |
| Werden große Datenmengen verarbeitet oder analysiert? | Skaleneffekt (z. B. Auswertung großer Mengen an Kunden-, Nutzungs- und Transaktionsdaten) | ○ Ja ○ Nein |
| Werden Daten aus verschiedenen Quellen zusammengeführt oder verknüpft? | Profilbildung (z. B. Verknüpfung von CRM-Daten mit Social-Media-Informationen) | ○ Ja ○ Nein |
| Erfolgt eine systematische oder dauerhafte Beobachtung? | Überwachungsnähe (z. B. kontinuierliches Tracking des Nutzerverhaltens über mehrere Sitzungen hinweg) | ○ Ja ○ Nein |
| Werden besondere Kategorien personenbezogener Daten verarbeitet? | Hohe Sensibilität (z. B. Auswertung von Gesundheitsdaten in einer Fitness- oder Gesundheits-App) | ○ Ja ○ Nein |
| Werden sensible Rückschlüsse aus scheinbar neutralen Daten gezogen? | Verdeckte Risiken (z. B. Ableitung von Gesundheitszuständen aus Bewegungs- oder Kaufdaten) | ○ Ja ○ Nein |
| Ist die Funktionsweise nicht vollständig nachvollziehbar („Blackbox")? | Intransparenz (z. B. Einsatz komplexer Machine-Learning-Modelle ohne erklärbare Entscheidungslogik) | ○ Ja ○ Nein |
| Besteht die Gefahr unkontrollierter Nutzung durch Mitarbeitende? | Organisationsrisiko (z. B. Nutzung privater KI-Tools für Unternehmensdaten) | ○ Ja ○ Nein |
| Ist nicht sichergestellt, dass Betroffenenrechte erfüllt werden können? | DSGVO-Risiko (z. B. keine Möglichkeit zur Löschung oder Auskunft) | ○ Ja ○ Nein |
| Handelt es sich um eine neue Technologie im Unternehmen? | Neuheitsrisiko (z. B. erstmaliger Einsatz eines KI-Systems im Recruiting oder Marketing) | ○ Ja ○ Nein |
| Steuert oder beeinflusst das KI-System die Interaktion mit Betroffenen? | DSK-Positivliste (z. B. Chatbot, der Kundenanfragen automatisiert beantwortet und lenkt) | ○ Ja ○ Nein |
| Ist die Nutzung nicht ausreichend geregelt oder dokumentiert? | Governance-Problem (z. B. fehlende Richtlinien zum KI-Einsatz) | ○ Ja ○ Nein |
| Wird ein extern betriebenes KI-System oder ein Cloud-Dienst eingesetzt? | Kontrollverlust (z. B. Nutzung eines cloudbasierten KI-Tools zur Text- oder Datenanalyse) | ○ Ja ○ Nein |
| Besteht keine vollständige Transparenz über Datenflüsse? | Drittanbieterrisiko (z. B. unklare Speicherung oder Weiterverarbeitung durch den Anbieter) | ○ Ja ○ Nein |
| Erfolgen Datenübermittlungen in Drittländer? | Drittlandrisiko (z. B. Verarbeitung auf Servern außerhalb der EU, etwa in den USA) | ○ Ja ○ Nein |
| Besteht die Gefahr systematischer Verzerrungen (Bias)? | Diskriminierungsrisiko (z. B. Benachteiligung bestimmter Gruppen durch fehlerhafte Trainingsdaten) | ○ Ja ○ Nein |
| Fehlt es an ausreichender Protokollierung der Verarbeitung? | Nachweisproblem (z. B. keine Dokumentation der KI-Entscheidungen) | ○ Ja ○ Nein |
| Können fehlerhafte Ergebnisse erhebliche Auswirkungen haben? | Schadenspotenzial (z. B. falsche Risikobewertung führt zu Vertragsablehnung) | ○ Ja ○ Nein |
| Besteht die Gefahr der Manipulation von Trainingsdaten oder Modellen? | Sicherheitsrisiko (z. B. gezielte Beeinflussung von Trainingsdaten) | ○ Ja ○ Nein |

# DSFA richtig durchführen: So gehen Sie strukturiert vor

**Nach der ersten Einordnung stellt sich in der Praxis schnell die nächste Frage: Wie führen Sie die DSFA strukturiert und prüfungssicher durch? Gerade bei KI-Anwendungen zeigt sich, dass die praktische Umsetzung oft anspruchsvoller ist als die gesetzlichen Vorgaben.**

## DSFA sinnvoll in bestehende Abläufe integrieren

Die DSGVO gibt zwar keinen festen Ablauf vor, verlangt aber eine systematische und nachvollziehbare Prüfung. Ihre Aufgabe besteht daher darin, diesen Rahmen in ein praktikables Verfahren zu überführen und die relevanten Informationen im Unternehmen zusammenzuführen.[BS1]

**Wichtig dabei:** Idealerweise ist die DSFA in einen bestehenden Prüfprozess eingebettet, der sich auf die jeweilige Verarbeitungstätigkeit, das konkrete Vorhaben oder den zugrunde liegenden Prozess bezieht. So vermeiden Sie parallele Prüfstrukturen und Mehrarbeit – und stellen sicher, dass auf bereits vorhandene Informationen zurückgegriffen werden kann.

## Schritt für Schritt: So setzen Sie die DSFA um

Die DSFA folgt keinem festen Schema. Die DSGVO gibt Ihnen aber einen klaren Rahmen, an dem Sie sich orientieren können.

### Schritt 1: Prüfen Sie, ob eine DSFA erforderlich ist

Ob eine DSFA erforderlich ist, haben wir bereits auf Seite 1–2 dargestellt. Entscheidend ist, ob die geplante Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen mit sich bringt (Art. 35 Abs. 1 DSGVO).

### Schritt 2: Verarbeitung und Zwecke beschreiben

Im nächsten Schritt ist die geplante Verarbeitung möglichst konkret zu beschreiben. Dazu gehören insbesondere:

- Zweck der Verarbeitung,
- Kategorien betroffener Personen,
- Kategorien personenbezogener Daten,
- Datenquellen und Empfänger,
- wesentliche Abläufe der Verarbeitung.

Besonderheit bei KI-Systemen: Bereits diese Beschreibung kann in der Praxis anspruchsvoll sein. Vor allem bei KI-Anwendungen erschweren die komplexe Funktionsweise und die häufig eingeschränkte Nachvollziehbarkeit („Blackbox") eine detaillierte Darstellung. Für die DSFA genügt es jedoch in der Regel, den geplanten Einsatz, die Datenflüsse und die Zwecke der Verarbeitung so konkret wie möglich zu beschreiben.

### Schritt 3: Prüfen Sie die Rechtsgrundlagen

Anschließend ist zu klären, auf welche Rechtsgrundlage(n) die Verarbeitung gestützt wird (z. B. Einwilligung, Vertragserfüllung oder berechtigtes Interesse). Auch hier zeigen sich in der Praxis typische Spannungsfelder. Gerade bei datenintensiven Anwendungen wie KI-Systemen steht die umfassende Datenauswertung häufig im Konflikt mit den Anforderungen der DSGVO.

Insbesondere im Hinblick auf den Grundsatz der Datenminimierung ist sorgfältig zu prüfen, welche Daten tatsächlich erforderlich sind und ob Alternativen wie Anonymisierung oder Pseudonymisierung in Betracht kommen.

### Schritt 4: Bewerten Sie Notwendigkeit und Verhältnismäßigkeit

Die Verarbeitung muss erforderlich und verhältnismäßig sein. Dabei ist zu prüfen:

- Ist die Verarbeitung zur Zweckerreichung geeignet?
- Gibt es weniger eingriffsintensive Alternativen?
- Steht der Nutzen in einem angemessenen Verhältnis zu den Eingriffen?

### Schritt 5: Risiken für Betroffene analysieren

Kern der DSFA ist die Risikobewertung. Dabei sind insbesondere Eintrittswahrscheinlichkeit und Schwere möglicher Schäden zu berücksichtigen. Typische Risiken können sein:

- unbefugter Zugriff auf Daten,
- Fehlverarbeitungen oder unzutreffende Ergebnisse,
- Einschränkungen der Betroffenenrechte,
- Diskriminierung oder Benachteiligung durch verzerrte Trainingsdaten.

### Schritt 6: Legen Sie Maßnahmen zur Risikominimierung fest

Abschließend sind geeignete technische und organisatorische Maßnahmen (TOM) festzulegen, um die identifizierten Risiken zu reduzieren.

Sie sollten vor allem darauf achten, dass die Maßnahmen dem Risiko angemessen sind und wirksam umgesetzt werden. Dazu zählen insbesondere:

- Zugriffskontrollen und Berechtigungskonzepte,
- interne Richtlinien und Prozesse,
- Lösch- und Speicherfristen,
- Transparenz- und Informationsmaßnahmen.

Können die Risiken trotz dieser Maßnahmen nicht ausreichend reduziert werden, müssen Sie die zuständige Aufsichtsbehörde konsultieren (Art. 36 DSGVO).

# KI-Risiken richtig bewerten: Darauf müssen Sie achten

**Für Sie als Datenschutzbeauftragten steht bei der DSFA die systematische Bewertung von Risiken im Mittelpunkt. Beim Einsatz von KI-Systemen zeigt sich jedoch schnell, dass sich diese Bewertung nicht ohne Weiteres auf klassische Verarbeitungssituationen übertragen lässt. KI-Systeme sind häufig komplex, dynamisch und in ihrer Funktionsweise nur eingeschränkt nachvollziehbar. Dadurch entstehen neue Risikokonstellationen, die bei der Durchführung einer DSFA besonders berücksichtigt werden müssen.**

## KI-spezifische Risiken: Diese Besonderheiten müssen Sie kennen

Die folgende Übersicht zeigt typische Besonderheiten, die bei der Risikobewertung von KI-Systemen eine Rolle spielen. Sie unterstützt Sie dabei, über klassische Datenschutzrisiken hinaus auch KI-spezifische Risiken systematisch zu erfassen und geeignete Maßnahmen abzuleiten.

Entscheidend ist dabei nicht die abstrakte Risikoerkennung, sondern die konkrete Anwendung im Einzelfall. Gerade bei KI-Systemen entstehen Risiken oft im Zusammenspiel mehrerer Faktoren und müssen daher ganzheitlich bewertet werden.

**Tabelle: Besonderheiten der Risikobewertung bei KI-Systemen**

| Risikobereich | Beschreibung/typische Ausprägung | Mögliche technische und organisatorische Maßnahmen (TOM) |
|---|---|---|
| Intransparente Entscheidungslogik („Blackbox“) | Die Funktionsweise des KI-Systems ist für Verantwortliche und Betroffene nur eingeschränkt nachvollziehbar. Es bleibt unklar, welche Faktoren konkret zu einem bestimmten Ergebnis geführt haben, wie einzelne Eingaben gewichtet wurden und welche Entscheidungslogik oder Modellarchitektur zugrunde liegt. Dies erschwert sowohl die interne Kontrolle als auch die rechtliche Bewertung der Verarbeitung. | Einsatz erklärbarer Modelle (Explainable AI), detaillierte Dokumentation von Modellen und Entscheidungslogik, interne Prüf- und Freigabeprozesse sowie regelmäßige Audits |
| Fehlende Erklärbarkeit gegenüber Betroffenen | Entscheidungen oder Ergebnisse können gegenüber Betroffenen nicht verständlich oder nachvollziehbar begründet werden. Dies ist insbesondere bei automatisierten Entscheidungen problematisch, da Betroffene ihre Rechte (z. B. Widerspruch oder Überprüfung) nicht effektiv wahrnehmen können. | Entwicklung von Transparenzkonzepten, verständliche und adressatengerechte Erläuterungen, Schulung von Mitarbeitenden im Umgang mit erklärungsbedürftigen KI-Ergebnissen |
| Verzerrte Trainingsdaten | Trainingsdaten enthalten bestehende Ungleichheiten, Vorurteile oder strukturelle Verzerrungen, die vom Modell übernommen und teilweise verstärkt werden. Diese Verzerrungen sind häufig nicht offensichtlich und können sich erst im Betrieb zeigen. | Systematische Prüfung und Bereinigung von Trainingsdaten, Diversitäts- und Qualitätschecks, regelmäßige Modellvalidierung sowie Dokumentation der Datengrundlage |
| Diskriminierungsrisiken (Bias) | Das System führt zu systematischen Benachteiligungen oder Bevorzugungen bestimmter Personengruppen, etwa aufgrund von Geschlecht, Alter, Herkunft oder sozioökonomischen Faktoren, auch ohne explizite Programmierung solcher Effekte. | Durchführung strukturierter Bias-Tests, kontinuierliches Monitoring auf Diskriminierung, Anpassung von Modellen, Schwellenwerten und Entscheidungsregeln |
| Unzutreffende oder fehlerhafte Ergebnisse („Halluzinationen“) | KI-Systeme erzeugen plausibel wirkende, aber sachlich falsche oder irreführende Inhalte und Bewertungen, die ohne weitere Prüfung übernommen werden können und zu erheblichen Fehlentscheidungen führen. | Implementierung von Plausibilitätsprüfungen, Vier-Augen-Prinzip, verpflichtende menschliche Endkontrolle sowie klare Freigabeprozesse |
| Dynamische Systemveränderungen („Model Drift“) | Das Verhalten des Systems verändert sich im Zeitverlauf durch neue Daten, veränderte Nutzung oder Nachtrainingsprozesse, sodass Ergebnisse nicht mehr stabil, konsistent oder vorhersehbar sind. Risiken entstehen häufig schleichend. | Regelmäßige Re-Validierung und Re-Training unter kontrollierten Bedingungen, kontinuierliches Monitoring, Versionierung und Dokumentation von Modellständen |
| Unklare Datenflüsse | Es ist nicht vollständig transparent, welche Daten wann, wie und durch wen verarbeitet, gespeichert oder weitergegeben werden. Besonders bei externen KI-Diensten oder komplexen Systemlandschaften besteht ein erhöhtes Risiko intransparenter Datenverarbeitung. Häufig fehlen zudem klare Informationen zu Datenflüssen, Speicherorten und beteiligten Dritten, sodass eine vollständige Nachvollziehbarkeit nur eingeschränkt möglich ist. | Durchführung detaillierter Datenflussanalysen, Abschluss und Kontrolle von AV-Verträgen, klare Beschränkung und Dokumentation von Datenübermittlungen |

| | | |
|---|---|---|
| Unklare Herkunft der Trainingsdaten | Die Herkunft, Qualität und rechtliche Zulässigkeit der Trainingsdaten ist nicht eindeutig nachvollziehbar oder dokumentiert. Dies kann zu Verstößen gegen Datenschutz- oder Urheberrecht führen. | Sorgfältige Anbieterprüfung (Due Diligence), vertragliche Zusicherungen zur Datenherkunft, umfassende Dokumentation der verwendeten Datensätze |
| Umfangreiche Datenverarbeitung | Es werden große Mengen personenbezogener Daten verarbeitet oder analysiert, häufig auch in aggregierter Form, wodurch das Risiko für die Rechte und Freiheiten der Betroffenen deutlich erhöht wird. | Umsetzung von Datenminimierung, Pseudonymisierung und Zweckbindung, Beschränkung auf erforderliche Daten sowie Zugriffsbeschränkungen |
| Zusammenführung mehrerer Datenquellen | Daten aus unterschiedlichen Quellen werden kombiniert, wodurch umfassende Profile entstehen und neue, teils sensible Rückschlüsse möglich werden, die ursprünglich nicht beabsichtigt waren. | Sicherstellung der Zweckbindung, Begrenzung der Datenzusammenführung, differenzierte Zugriffskonzepte und regelmäßige Überprüfung der Datenintegration |
| Automatisierte Entscheidungsfindung | Entscheidungen werden ganz oder teilweise automatisiert auf Basis von KI-Ergebnissen getroffen, ohne dass eine ausreichende menschliche Kontrolle oder Plausibilisierung erfolgt. | Implementierung von „Human in the Loop"-Ansätzen, klare Entscheidungsprozesse, definierte Eingriffs- und Übersteuerungsmöglichkeiten |
| Nur formale menschliche Kontrolle | Eine vorgesehene menschliche Kontrolle findet faktisch nicht statt, da Ergebnisse aus Effizienzgründen routinemäßig ungeprüft übernommen werden („Automation Bias"). | Schulung der Mitarbeitenden, verbindliche Prüfprozesse, klare Verantwortlichkeiten und Stichprobenkontrollen |
| Eingeschränkte Betroffenenrechte | Auskunfts-, Lösch- oder Widerspruchsrechte können aufgrund fehlender Transparenz, komplexer Systeme oder technischer Einschränkungen nicht effektiv umgesetzt werden. | Etablierung klarer Prozesse zur Wahrung von Betroffenenrechten, Verbesserung der Systemtransparenz und Dokumentation |
| Zweckänderung der Datenverarbeitung | Daten werden für andere Zwecke verwendet als ursprünglich vorgesehen, etwa zur Weiterverarbeitung als Trainingsdaten oder für neue Analysen, ohne ausreichende Rechtsgrundlage. | Klare Zweckdefinition, getrennte Verarbeitung, regelmäßige Prüfung und Dokumentation der Rechtsgrundlagen |
| Sicherheitsrisiken (z. B. Data Poisoning) | Systeme können durch gezielte Manipulation von Trainingsdaten oder Modellen beeinflusst werden, was zu fehlerhaften oder verzerrten Ergebnissen führt. | Umsetzung technischer Sicherheitsmaßnahmen, Zugriffskontrollen, Monitoring und Schutzmechanismen gegen Manipulation |
| Abhängigkeit von externen Anbietern | KI-Systeme werden über externe Dienstleister betrieben, wodurch die Kontrolle über Datenverarbeitung, Sicherheitsstandards und Modellverhalten eingeschränkt ist. | Abschluss und Kontrolle von AV-Verträgen, Durchführung von Anbieter-Audits, Auswahl vertrauenswürdiger Anbieter |
| Drittlandübermittlungen | Daten werden bei Nutzung von KI-Diensten in Drittländer übertragen, ggf. ohne angemessenes Datenschutzniveau oder ausreichende Garantien. | Einsatz von Standardvertragsklauseln, Durchführung von Transfer Impact Assessments, bevorzugt Nutzung von EU-basiertem Hosting |
| Fehlende Dokumentation | Verarbeitung, Entscheidungslogik und Datenflüsse sind nicht ausreichend dokumentiert, was die Nachvollziehbarkeit und Rechenschaftspflicht erheblich erschwert. | Durchführung und Pflege einer DSFA, Verzeichnis von Verarbeitungstätigkeiten, interne Richtlinien und Dokumentationspflichten |
| Risiken im laufenden Betrieb | Risiken entstehen oder verändern sich erst im praktischen Einsatz, etwa durch neue Daten, veränderte Nutzung oder externe Einflüsse. | Laufendes Monitoring, regelmäßige Überprüfung und Aktualisierung der DSFA sowie kontinuierliche Risikoanalyse |
| Memorization (Wiedergabe von Trainingsdaten) | Das System kann Inhalte aus Trainingsdaten reproduzieren, einschließlich personenbezogener oder sensibler Informationen, ohne dass dies beabsichtigt ist. | Einsatz von Filtermechanismen, Auswahl geprüfter Modelle, konsequente Datenminimierung und Zugriffsbeschränkungen |
| Overreliance / Automatisierungsbias | Nutzer verlassen sich zu stark auf KI-Ergebnisse und hinterfragen diese nicht mehr kritisch, was zu Fehlentscheidungen und Kontrollverlust führen kann. | Schulungen, klare Nutzungsvorgaben, verpflichtende kritische Prüfung und Dokumentation von Entscheidungen |
| Fehlende Zweckkontrolle bei generativer KI | Eingaben können ungewollt für Trainings- oder andere Zwecke verwendet werden, insbesondere bei offenen oder cloudbasierten Systemen. | Einschränkung von Eingaben, Nutzung datenschutzkonformer Systeme, klare Richtlinien zur Verwendung |
| Unkontrollierte Nutzung („Shadow AI") | Mitarbeitende nutzen KI-Tools ohne Freigabe oder klare Vorgaben, wodurch Kontroll-, Sicherheits- und Compliance-Risiken entstehen. | Einführung verbindlicher KI-Richtlinien, Freigabeprozesse, Schulungen und Sensibilisierung |
| Prompt-Leakage / Datenabfluss | Sensible Informationen werden über Eingaben (Prompts) in externe Systeme übertragen und dort gespeichert oder weiterverarbeitet. | Richtlinien zur Dateneingabe, technische Sperren, Sensibilisierung der Mitarbeitenden |
| Fehlende Lösch- und Kontrollmöglichkeiten | Einmal verarbeitete Daten lassen sich nicht oder nur eingeschränkt löschen oder kontrollieren, insbesondere bei Modelltraining oder externen Systemen. | Anbieterprüfung, vertragliche Regelungen, konsequente Datensparsamkeit und Datenkontrolle |
| Geringe Robustheit | Systeme reagieren empfindlich auf ungewöhnliche, fehlerhafte oder manipulierte Eingaben und liefern dadurch unzuverlässige oder inkonsistente Ergebnisse. | Durchführung von Robustheitstests, Monitoring, Absicherung gegen Missbrauch und Fehlverhalten |
| Fehlende Governance-Strukturen | Es bestehen keine klaren Zuständigkeiten, Prozesse oder Verantwortlichkeiten für den Einsatz, die Überwachung und die Weiterentwicklung von KI-Systemen im Unternehmen. | Einführung von KI-Governance-Strukturen, klare Verantwortlichkeiten, etablierte Kontroll- und Freigabemechanismen |

# So vermeiden Sie typische Fehler bei der DSFA

**In der Praxis zählt vor allem die Umsetzung. Gerade bei KI-Systemen entstehen Fehler selten bei der rechtlichen Einordnung, sondern durch unklare Prozesse, fehlende Abstimmung und eine unzureichende Risikobewertung. Umso wichtiger ist es für Sie als Datenschutzbeauftragten, typische Stolperfallen frühzeitig zu erkennen und gezielt zu vermeiden. Die folgenden Beispiele zeigen Ihnen, wo in der Praxis besonders häufig Probleme entstehen – und wie Sie diesen begegnen können.**

Die folgende Übersicht zeigt typische Fehler bei der DSFA – insbesondere im Zusammenhang mit KI-Systemen. Damit können Sie Schwachstellen frühzeitig erkennen und erhalten zugleich konkrete Hinweise für die richtige Umsetzung in der Praxis.

## Übersicht: Typische Fehler bei der DSFA

| Problem | Typische Folge in der Praxis | Bessere Vorgehensweise |
|---|---|---|
| DSFA wird zu spät durchgeführt. | Die DSFA erfolgt erst kurz vor oder nach Einführung des Systems. Risiken werden zu spät erkannt, Maßnahmen können nicht mehr sinnvoll umgesetzt werden oder führen zu Verzögerungen im Projekt. | Verankern Sie die DSFA als festen Bestandteil des Projektablaufs und führen Sie sie bereits bei der Auswahl des Tools oder der Freigabe neuer Prozesse durch. Stellen Sie sicher, dass bei jeder Einführung eines KI-Systems mit Personenbezug automatisch geprüft wird, ob eine DSFA erforderlich ist, und binden Sie den Datenschutz frühzeitig ein. In der Praxis zeigt sich, dass verspätete DSFAs häufig zu erheblichen Projektverzögerungen oder nachträglichen Anpassungen führen, die vermeidbar gewesen wären. |
| Fehlende Governance-Strukturen | Es fehlen klare Zuständigkeiten, verbindliche Prozesse und transparente Entscheidungswege für den Einsatz und die Kontrolle von KI-Systemen. Ohne eine funktionierende Governance lassen sich Risiken weder systematisch erkennen noch wirksam steuern und überwachen. | Etablieren Sie eine klare KI-Governance mit definierten Rollen, Zuständigkeiten und Entscheidungswegen. Ergänzen Sie diese durch verbindliche Prozesse und Kontrollmechanismen und verzahnen Sie die Struktur eng mit bestehenden Datenschutz- und Compliance-Systemen. |
| Fokus nur auf das Tool statt auf die konkrete Anwendung | Es wird nur das KI-System bewertet, nicht aber der konkrete Einsatz im Unternehmen. Dadurch werden Risiken unterschätzt oder falsch eingeordnet. | Prüfen Sie nicht nur die technischen Eigenschaften des Tools, sondern den konkreten Einsatz im Unternehmen. Dokumentieren Sie den Use Case, insbesondere welche Daten verarbeitet werden, wie Ergebnisse genutzt werden und welche Auswirkungen auf Betroffene entstehen können. |
| Fehlende Einbindung der IT und Fachabteilungen | Technische Abläufe, Datenflüsse oder Systemgrenzen werden nicht vollständig verstanden. Risiken bleiben unentdeckt oder werden falsch bewertet. | Führen Sie die DSFA interdisziplinär durch und binden Sie IT, Fachabteilungen und ggf. weitere Stellen strukturiert ein. Stellen Sie sicher, dass technische Abläufe, Datenflüsse und tatsächliche Nutzung vollständig erfasst und bewertet werden. |
| Unzureichendes Verständnis der KI-Funktionsweise | Komplexe Modelle werden vereinfacht dargestellt oder gar nicht hinterfragt. Risiken wie „Blackbox", Bias oder Modellverhalten werden nicht erkannt. | Sorgen Sie für ein belastbares Grundverständnis des Systems, insbesondere zu Eingaben, Funktionsweise, Trainingsprozessen und bekannten Grenzen. Ziehen Sie bei Bedarf interne oder externe Fachleute hinzu, um Risiken realistisch einschätzen zu können. |
| „Human in the Loop" nur formal umgesetzt | Menschliche Kontrolle ist zwar vorgesehen, erfolgt aber in der Praxis nicht ernsthaft. KI-Ergebnisse werden routinemäßig übernommen. | Definieren Sie konkrete Kontrollprozesse und stellen Sie sicher, dass zuständige Personen ausreichend Zeit, Fachkenntnis und Entscheidungsspielraum haben. Dokumentieren Sie die Überprüfung von KI-Ergebnissen nachvollziehbar und fördern Sie eine Kultur aktiver Kontrolle. In der Praxis scheitert eine wirksame Kontrolle häufig daran, dass Zeit, Fachkenntnis oder klare Verantwortlichkeiten fehlen. |
| Blindes Vertrauen in Anbieter | Aussagen des KI-Anbieters werden ungeprüft übernommen (z. B. „DSGVO-konform"). Risiken bei Trainingsdaten, Datenflüssen oder Modellverhalten bleiben unbeachtet. | Behandeln Sie Anbieterangaben als Ausgangspunkt und prüfen Sie diese kritisch. Fordern Sie detaillierte Informationen zur Datenverarbeitung, zu Trainingsprozessen und Sicherheitsmaßnahmen an und sichern Sie zentrale Aspekte vertraglich ab. |
| Unklare Datenflüsse und Datenverarbeitung | Es ist nicht transparent, welche Daten verarbeitet, gespeichert oder weitergegeben werden, insbesondere bei Cloud- oder KI-Diensten. | Erstellen Sie eine vollständige und nachvollziehbare Darstellung der Datenflüsse. Berücksichtigen Sie dabei Datenquellen, Empfänger, Speicherorte, Zugriffe sowie mögliche Weitergaben an Dritte oder Unterauftragnehmer. |
| Trainingsdaten und deren Herkunft werden nicht geprüft. | Es bleibt unklar, ob Trainingsdaten rechtmäßig erhoben wurden oder Verzerrungen enthalten. Risiko von Datenschutzverstößen und Diskriminierung. | Klären Sie systematisch die Herkunft, Qualität und Nutzung der Trainingsdaten. Dokumentieren Sie, ob eigene, Kunden- oder Anbieterdaten verwendet werden und ob Trainings- oder Nachtrainingsprozesse stattfinden. |
| Risiken durch Bias und Diskriminierung werden unterschätzt. | Systematische Benachteiligungen werden nicht erkannt, obwohl sie sich aus Daten oder Modelllogik ergeben. | Prüfen Sie gezielt auf mögliche Verzerrungen und Diskriminierungsrisiken. Führen Sie Testläufe, Stichproben und Vergleichsbewertungen durch und legen Sie Verfahren zum Umgang mit auffälligen Ergebnissen fest. |

| | | |
|---|---|---|
| Fehlende oder unzureichende Risikobewertung | Risiken werden nur oberflächlich beschrieben oder nicht differenziert bewertet, etwa ohne Betrachtung von Eintrittswahrscheinlichkeit und Schadenshöhe. | Bewerten Sie Risiken strukturiert und nachvollziehbar anhand von Eintrittswahrscheinlichkeit und Schadenspotenzial. Begründen Sie die Einstufung und berücksichtigen Sie auch mittelbare Auswirkungen. |
| Maßnahmen bleiben zu abstrakt. | Es werden allgemeine Maßnahmen genannt („Zugriff beschränken"), ohne konkrete Umsetzung. | Beschreiben Sie Maßnahmen so konkret, dass ihre Umsetzung überprüfbar ist. Legen Sie Verantwortlichkeiten, Fristen, Prüfintervalle sowie technische oder organisatorische Details fest und vermeiden Sie rein allgemeine Formulierungen. |
| Fehlende Berücksichtigung von Betroffenenrechten | Prozesse zur Auskunft, Löschung oder Berichtigung sind nicht vorgesehen oder praktisch nicht umsetzbar. | Prüfen Sie frühzeitig, wie Betroffenenrechte im konkreten System umgesetzt werden können. Stellen Sie sicher, dass Daten, Entscheidungsgrundlagen und Prozesse so dokumentiert sind, dass Auskunft, Löschung oder Berichtigung tatsächlich durchgeführt werden können. |
| Unzureichende Dokumentation | Die DSFA ist unvollständig oder nicht nachvollziehbar dokumentiert. Im Prüfungsfall fehlen Nachweise. | Dokumentieren Sie nicht nur das Ergebnis, sondern auch den Weg dorthin. Halten Sie Annahmen, Bewertungen, Beteiligte und Abwägungen nachvollziehbar fest, sodass auch Dritte die DSFA prüfen und verstehen können. |
| Keine Aktualisierung der DSFA | Die DSFA wird einmal erstellt und danach nicht mehr überprüft. Veränderungen im System oder Einsatz bleiben unberücksichtigt. | Legen Sie feste Anlässe für eine Überprüfung fest, etwa bei Änderungen von System, Datenquellen oder Nutzung. Integrieren Sie die DSFA in bestehende Prozesse, sodass Anpassungen regelmäßig und strukturiert erfolgen. |
| Risiken im laufenden Betrieb werden ignoriert. | Modellverhalten verändert sich, etwa durch neue Daten, Feintuning oder geänderte Nutzung, ohne dass dies erkannt oder bewertet wird. | Etablieren Sie ein kontinuierliches Monitoring mit regelmäßigen Stichproben, Fehleranalysen und Rückmeldungen aus dem Betrieb. Definieren Sie klare Schwellenwerte, ab denen eine Neubewertung oder Anpassung zwingend erfolgt, und verankern Sie dies in bestehenden Kontrollprozessen. |
| Unkontrollierte Nutzung von KI („Shadow AI") | Mitarbeitende nutzen eigenständig KI-Anwendungen außerhalb definierter Prozesse, etwa durch Eingabe sensibler Daten. Dadurch entstehen Datenschutzrisiken sowie Gefahren für Geschäftsgeheimnisse und vertrauliche Informationen. | Führen Sie klare Regeln zur Nutzung von KI-Tools ein und ergänzen Sie diese durch Schulungen, Freigabeprozesse und technische Schutzmaßnahmen. Stellen Sie zugleich praxistaugliche, freigegebene Alternativen bereit, um Ausweichverhalten zu vermeiden und die Nutzung zu kanalisieren. |
| Sensible Daten werden unkontrolliert in KI-Systeme eingegeben. | Vertrauliche oder personenbezogene Daten gelangen über Prompts in externe Systeme und werden dort weiterverarbeitet. | Definieren Sie klare Vorgaben, welche Daten eingegeben werden dürfen und welche nicht. Sensibilisieren Sie Mitarbeitende durch Schulungen und Praxisbeispiele und unterstützen Sie dies – soweit möglich – durch technische Schutzmechanismen oder Filter. |
| Zweck und Rollenverteilung sind intern unklar. | Niemand kann sauber erklären, wofür das System eingesetzt wird, wer entscheidet und wer die Verantwortung trägt. Dadurch werden Bewertungen widersprüchlich und Maßnahmen nicht umgesetzt. | Legen Sie Zweck, Rollen und Verantwortlichkeiten frühzeitig fest und dokumentieren Sie diese verbindlich. Stellen Sie sicher, dass Entscheidungs-, Prüf- und Freigabeprozesse klar geregelt und im Alltag tatsächlich gelebt werden. |
| Abgrenzung zwischen Testbetrieb und Produktivbetrieb fehlt. | Systeme werden zunächst „nur testweise" eingesetzt, verarbeiten aber bereits echte personenbezogene Daten. Risiken werden deshalb zu spät ernst genommen. | Definieren Sie klare Regeln für Test-, Pilot- und Produktivbetrieb und machen Sie diese verbindlich. Prüfen Sie vorab Datennutzung, Schutzmaßnahmen und Alternativen wie Pseudonymisierung und berücksichtigen Sie auch Testumgebungen in der DSFA. |
| Ergebnisse und Restrisiken werden intern nicht kommuniziert. | Fachbereiche nutzen das System weiter, ohne die festgestellten Risiken oder Grenzen zu kennen. Maßnahmen werden dadurch umgangen oder ignoriert. | Kommunizieren Sie die Ergebnisse der DSFA zielgruppengerecht und verständlich. Geben Sie klare Vorgaben dazu, was zulässig ist, wo Grenzen liegen und welche Prüf- und Freigabeschritte zwingend einzuhalten sind. |
| Keine klaren Kriterien für Abbruch oder Nachsteuerung | Auch bei auffälligen Fehlleistungen läuft das System unverändert weiter, weil niemand weiß, wann eine Nutzung gestoppt oder angepasst werden muss. | Definieren Sie vorab klare Kriterien und Trigger für Anpassung, Neubewertung oder Aussetzung der Nutzung. Dazu gehören z. B. Fehlentscheidungen, Beschwerden, Sicherheitsvorfälle oder auffällige Nutzungsmuster. |
| Interne Richtlinien bestehen nur auf dem Papier. | Es gibt zwar Vorgaben zur KI-Nutzung, diese sind den Mitarbeitenden aber nicht bekannt oder werden im Alltag nicht umgesetzt. | Verknüpfen Sie Richtlinien mit Schulungen, Praxisbeispielen und klaren Verantwortlichkeiten. Ergänzen Sie dies durch regelmäßige Kontrollen, um sicherzustellen, dass die Vorgaben im Alltag tatsächlich angewendet werden. |
| Unklare Nutzung von Daten für KI-Training | Es bleibt offen, ob eingegebene Daten für Trainingszwecke verwendet oder gespeichert werden. | Klären Sie vertraglich und technisch, ob und in welchem Umfang Daten für Trainingszwecke genutzt werden. Beschränken oder schließen Sie dies soweit möglich aus und dokumentieren Sie verbleibende Risiken transparent. |
| Fehlende Transparenz bei Verarbeitungsorten und Drittlandtransfers | Es bleibt unklar, an welchen Standorten personenbezogene Daten verarbeitet werden und ob dabei Übermittlungen in Drittländer erfolgen. | Klären Sie alle relevanten Verarbeitungsorte und prüfen Sie mögliche Drittlandtransfers sowie die hierfür bestehenden rechtlichen Garantien. Dokumentieren Sie diese Aspekte nachvollziehbar in der DSFA. |
| Unklarer Verbleib von Daten auf eigenen Systemen | Es ist nicht nachvollziehbar, ob und welche Daten intern gespeichert, weiterverarbeitet oder mit anderen Systemen verknüpft werden. | Analysieren Sie interne Datenflüsse umfassend und legen Sie klare Konzepte für Speicherung, Weiterverarbeitung, Zugriff und Löschung fest. Berücksichtigen Sie dabei auch Schnittstellen zu anderen Systemen. |
| Ungeeignete oder unsichere Systemeinstellungen | Standardkonfigurationen werden übernommen, ohne datenschutzrelevante Einstellungen anzupassen (z. B. Speicherung von Eingaben, Trainingsnutzung). | Prüfen und konfigurieren Sie Systeme aktiv und bewusst. Deaktivieren Sie nicht erforderliche Funktionen wie Trainingsnutzung oder unnötige Datenspeicherung und dokumentieren Sie die gewählten Einstellungen nachvollziehbar. |

# Neue Vorgaben: So wirkt sich die KI-VO auf Ihre DSFA aus

**Mit der KI-VO (EU AI Act) entsteht ein eigenständiger Rechtsrahmen für KI der die DSGVO ergänzt und den Fokus stärker auf Grundrechtsrisiken legt. Die KI-VO gilt schrittweise; zentrale Pflichten greifen ab dem 2.8.2026. Für Sie bedeutet das: Die Anforderungen an den KI-Einsatz steigen – auch im Rahmen der DSFA. Zugleich zeigt die Diskussion um den „Digitalen Omnibus", dass die Verzahnung der Digitalregeln weiter zunimmt. Die DSFA wird damit immer wichtiger, um diese Anforderungen gebündelt zu bewerten.**

## Praxisfolgen: Das müssen Sie jetzt im Blick haben

Die DSFA bleibt dabei weiterhin das zentrale Instrument zur Risikobewertung – sie wird durch die KI-VO nicht ersetzt. Allerdings wird sie künftig häufiger erforderlich sein, insbesondere bei Hochrisiko-KI-Systemen. Zudem kommt mit dem sogenannten Fundamental Rights Impact Assessment (FRIA) eine zusätzliche Prüfung hinzu, die über den Datenschutz hinausgeht und weitere Grundrechtsrisiken einbezieht.

Für Ihre Arbeit heißt das vor allem: Die Bewertung von KI-Ssystemen wird breiter und technischer ausgestaltet; Datenschutz, IT und Regulatorien greifen künftig noch enger ineinander.

## Das ändert sich konkret: Diese Punkte sind neu

Die KI-VO führt nicht zu einer „neuen DSFA", verändert aber deren inhaltliche Anforderungen und die praktische Durchführung:

### Punkt 1: Breiterer Risikobegriff

Die klassische DSFA fokussiert auf Risiken für die Rechte und Freiheiten betroffener Personen im Sinne der DSGVO. Mit der KI-VO erweitert sich der Blickwinkel faktisch: Künftig müssen auch darüber hinausgehende Risiken stärker berücksichtigt werden. Dazu zählen insbesondere:

- Diskriminierung und Verzerrungen (Bias),
- Auswirkungen auf Chancengleichheit und gesellschaftliche Teilhabe,
- systematische Fehlentscheidungen oder Fehlsteuerungen,
- sicherheitsrelevante Risiken und Missbrauchspotenziale.

Praxisfolge: Auch wenn diese Aspekte nicht vollständig im klassischen DSGVO-Risikobegriff aufgehen, werden sie bei der DSFA zu KI-Systemen faktisch mitgedacht werden müssen.

### Punkt 2: Stärkerer Technikbezug

Die KI-VO stellt deutlich höhere Anforderungen an das Verständnis und die Dokumentation der technischen Funktionsweise von KI-Systemen. Aspekte wie Trainingsdaten, Modelllogik oder Validierungsverfahren rücken stärker in den Fokus. Für die DSFA bedeutet das insbesondere:

- genauere Betrachtung der Datenbasis (z. B. Trainingsdaten, Input-Daten)
- Bewertung von Modellverhalten und Entscheidungslogiken
- Berücksichtigung von Test-, Validierungs- und Monitoringprozessen

Praxisfolge: Datenschutzbeauftragte werden sich stärker als bisher mit technischen Fragestellungen auseinandersetzen müssen. Ohne enge Zusammenarbeit mit IT und Fachbereichen ist eine belastbare DSFA bei KI-Systemen kaum noch möglich.

### Punkt 3: Lebenszyklus-Ansatz

Während die DSFA in der Praxis häufig als einmalige Prüfung vor Beginn der Verarbeitung verstanden wird, verfolgt die KI-VO einen klaren Lebenszyklusansatz. Risiken sollen nicht nur initial bewertet, sondern kontinuierlich überwacht und neu bewertet werden.

Praxisfolge: Die DSFA entwickelt sich bei KI-Systemen faktisch zu einem laufenden Prozess. Änderungen am Modell, neue Datenquellen oder veränderte Einsatzbedingungen müssen regelmäßig Anlass für eine Aktualisierung der Bewertung sein.

### Punkt 4: Dokumentation und Nachvollziehbarkeit

Die KI-VO bringt umfangreiche Dokumentationspflichten mit sich, insbesondere für Hochrisiko-KI-Systeme. Diese betreffen unter anderem die Systembeschreibung, Datenbasis, Funktionsweise und Risikobewertung. Für die DSFA bedeutet das

- eine bessere Informationsgrundlage, aber auch
- deutlich höhere Anforderungen an die Dokumentation selbst.

Die Rechenschaftspflicht („Accountability") wird damit weiter gestärkt: Entscheidungen und Bewertungen müssen nachvollziehbar, konsistent und prüfbar dokumentiert werden.

### Punkt 5: Mehr menschliche Kontrolle

Die KI-VO fordert ausdrücklich eine wirksame menschliche Aufsicht („Human Oversight"). Diese darf nicht nur formal vorgesehen sein, sondern muss tatsächlich funktionieren.

Praxisfolge für die DSFA:

- Kontrollmechanismen müssen konkret beschrieben werden.
- Verantwortlichkeiten müssen klar zugeordnet sein.
- Es ist zu prüfen, ob die Kontrolle in der Praxis tatsächlich wirksam ausgeübt werden kann.

Rein formale oder faktisch wirkungslose Kontrollmodelle werden künftig nicht mehr ausreichen.

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.



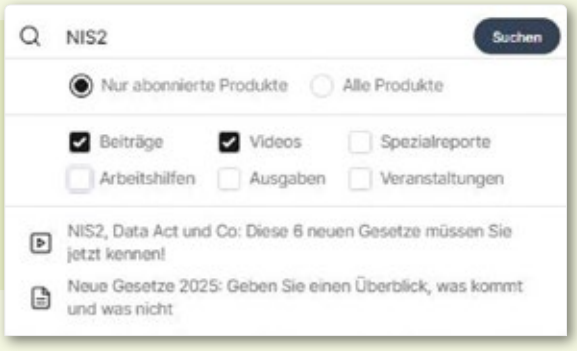
### Tipp:

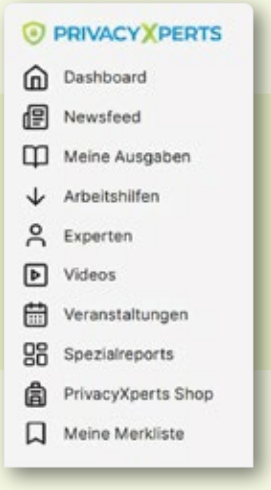
Setzen Sie die für Sie wichtigsten Ausgaben, Beiträge und Arbeitshilfen auf Ihre Merkliste. So haben Sie Ihre TOP-Themen immer schnell im Blick.

### 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!

**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**