DATENSCHUTZAKTUELL
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH
SEP 2026
Schweiz

KI-RISIKEN RICHTIG BEWERTEN: DARAUF MÜSSEN SIE ACHTEN

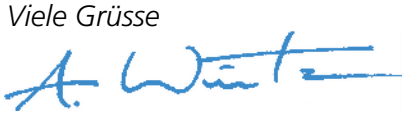
Üben Sie konstruktive Kritik

Liebe Leserin, lieber Leser,

wenn es im Datenschutz nicht rundläuft oder mancher anscheinend macht, was er will, kann das bei Ihnen für viel Frust und Ärger sorgen. Nun könnten Sie aus allen Wolken fallen und Ihrem Ärger Luft machen. Doch auch wenn Standpauken oft Eindruck machen, heisst das nicht, dass sie das Mittel der Wahl sind. Denn schnell können Sie über das Ziel hinausschiessen.

Viel besser ist es, wenn Sie zwar kurz Ihre Enttäuschung oder Verärgerung zum Ausdruck bringen. Gehen Sie dann jedoch direkt in konstruktive Kritik über. Erklären Sie, was falschlief, worauf es ankommt und wie es richtig geht.

Viele Grüsse



Andreas Würtz,
Rechtsanwalt und Chefredaktor

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

Inhalt

Zu Ihrem Onlinebereich:
https://kurzlink.ch/privacy

Live-Talk:
https://kurzlink.ch/live-talk

Expertenhotline:
https://kurzlink.ch/kontakt-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

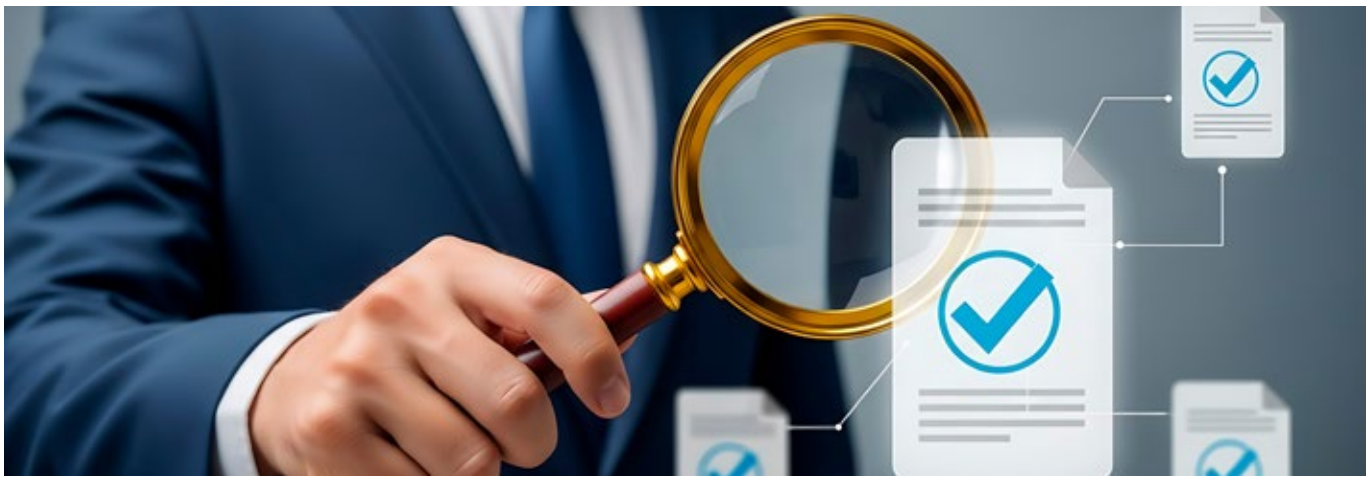
V.i.S.d.P.: Michael Jodda (Adresse s. oben)

Produktmanagement: Franziska Rohrbach, Bonn

Verantwortlicher Chefredaktor:
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: Adobe Stock | M.Dörr & M.Frommherz; Seite 1: Adobe Stock | Yusri Adi; Seite 7: Vera D, generiert mit KI

Erscheinungsweise: 17-mal pro Jahr
E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de
(bei Rückfragen bitte Kundennummer angeben)



Sie sollen auch die Einhaltung der Regelungen zum Datenschutz kontrollieren.

Damit Audits gut gelingen: Machen Sie den Selbstcheck

Zu Ihren Aufgaben nach Art. 10 Abs. 2 Bundesgesetz über den Datenschutz (DSG) zählt nicht nur das Beraten in allen Fragen des Datenschutzes. Sie sollen auch bei der Anwendung der Datenschutzvorschriften mitwirken. Dazu kann zählen, die Regelungen zum Datenschutz beim Verantwortlichen, also im Unternehmen, zu kontrollieren. Hierbei können Sie viel falsch machen.

Auditieren Sie nicht jeden und alles

Sie sollen die Einhaltung des Datenschutzes kontrollieren. Doch das darf nicht dazu führen, dass Sie Ihr Unternehmen lahmlegen. Sie müssen die richtigen Schwerpunkte setzen. Insofern sollten Sie zunächst dort hinschauen, wo die grössten Risiken für die betroffenen Personen liegen. Prio A muss auch haben, wo es in Ihrem Unternehmen unter Datenschutzaspekten eher zu Verstössen, Pannen oder Patzern kommen kann. Denn dann leisten Sie nicht nur dem Datenschutz einen guten Dienst. Sie betreiben auch Risikovorsorge für Ihr Unternehmen.

Auf das richtige Mindset kommt es an

Audits sind prinzipiell immer ein Frage-Antwort-Gespräch. Sie fragen nach etwas, Sie bekommen eine Antwort und wollen ggf. Belege sehen. Dann prüfen Sie, ob das Ist zum Soll passt, etwa zum DSG oder zu internen Vorschriften. Damit Audits viel bringen, kommt es jedoch auf Ihr Mindset an, sprich Ihre grundlegende Einstellung. Ihnen muss es darum gehen, dass der Datenschutz bestmöglich umgesetzt wird. Insofern sollte Ihnen nicht daran gelegen sein, die Geprüften abzustrafen. Besser ist es, wenn Sie auch beim Audit den Fokus auf das Beraten legen. Denn die Erfahrung zeigt, dass Beratungsaudits auch bei erheblichen Defiziten von den Geprüften leichter akzeptiert werden. Man ist eher bereit, die Defizite zügig anzugehen.

Arbeiten Sie an Ihren Soft Skills

Für ein gutes Audit brauchen Sie viel fachliches Wissen. Doch daneben müssen Sie auch die weichen Faktoren berücksichtigen, etwa rund um Gesprächsführung oder geschicktes Vorgehen. Damit Ihnen das gelingt, sollten Sie bei jedem Audit die Punkte der folgenden Checkliste umsetzen. Machen Sie den Selbstcheck.

Selbstcheck: Schlaues Vorgehen bei Audits

Aspekte	Darauf sollten Sie achten	Umgesetzt?
Vorbereitung		
Bereits bei der Auditplanung gehe ich risikoorientiert vor?	› Setzen Sie konsequent auf Risikoorientierung. Gibt es Bereiche oder Bearbeitungen mit geringem Risiko, müssen Sie Audits nicht komplett entfallen lassen. Sie können etwa auf Kurzaudits oder die Beantwortung eines kurzen Fragenkatalogs setzen. › Idealerweise haben Sie eine detaillierte Auditplanung, aus der Risiken und abgeleitete Schwerpunkte für Audits hervorgehen. Als lebendes Dokument können Sie auch unterjährig die Prioritäten verschieben. Halten Sie die Gründe für eine Änderung der Prioritäten oder Bewertungen fest.	○ Ja ○ Nein

Bereite ich Audits frühzeitig und umfassend vor?	› Audits wollen gut durchdacht und entsprechend geplant werden. › Kündigen Sie Audits rechtzeitig an und stellen Sie sicher, dass erforderliche Gesprächspartner auch tatsächlich verfügbar sind. › Machen Sie sich Gedanken zum Auditumfang und zur -tiefe. Legen Sie konkret den Fokus fest.	○ Ja ○ Nein
Informationen zur auditierten Einheit bzw. zum auditierten Thema fordere ich vorab an?	› Verschaffen Sie sich einen Überblick über die Situation im zu prüfenden Bereich. Sie sollten wissen, was man dort macht. › Prüfen Sie das Verzeichnis von Bearbeitungstätigkeiten. Damit haben Sie einen Überblick über die bekannten bzw. dokumentierten Bearbeitungstätigkeiten. › Holen Sie vorab Informationen im Bereich ein, etwa zur Datenschutzsituation vor Ort.	○ Ja ○ Nein
Bei den relevanten Vorschriften und Regelwerken bin ich sattelfest?	› Bei den Themen, die Sie prüfen, müssen Sie sich auskennen. Das umfasst vor allem die datenschutzrechtlichen Rahmenbedingungen. › Prüfen Sie vorab auch die internen Vorschriften und Prozesse. Diese beschreiben das Soll, gegen das Sie prüfen können.	○ Ja ○ Nein
Mit den Auditierten führe ich rechtzeitig ein Vorgespräch?	› Klären Sie in einem Gespräch darüber auf, worauf Sie es abgesehen haben, was Sie prüfen wollen und wie man sich vorbereiten sollte. Das vermeidet Stress und Frust beim Audit. › Nehmen Sie Bedenken oder Wünsche ernst. Passt Ihr Audit gerade überhaupt nicht in den Terminplan, sollten Sie darüber nachdenken, es ausnahmsweise zu verschieben.	○ Ja ○ Nein
Stimme ich mit der Unternehmensleitung meine Prüfung ab?	› Erläutern Sie, was Sie prüfen wollen. Ggf. können Sie Hinweise, Wünsche oder Empfehlungen in Ihr Audit einfliessen lassen. › Die Abstimmung mit der Unternehmensleitung kann auch ein „Türöffner" sein, wenn man in einem Bereich ein Audit generell ablehnt.	○ Ja ○ Nein
Es ist festgelegt, was ich anhand welcher Belege wie prüfen will?	› Denken Sie immer daran, dass Datenschutzrelevantes aufgrund der Rechenschaftspflicht nachweisbar sein muss. › Setzen Sie auch hier auf Risikoorientierung. Nicht alles muss immer schriftlich nachweisbar sein. Auch „gelebte Praxis" kann im Einzelfall ausreichen.	○ Ja ○ Nein
Ich plane ausreichend Zeit für die Durchführung des Audits ein?	› Nicht nur das Antworten auf Ihre Fragen braucht Zeit. Das gilt auch für die Sichtung von Nachweisen oder die Durchführung von Begehungen. › Planen Sie grosszügig und mit Puffer. Niemand ist Ihnen böse, wenn ein Audit früher beendet ist.	○ Ja ○ Nein
Prüfung		
Ich habe jederzeit meinen gesetzlichen Auftrag vor Augen?	› Sie sollen die Umsetzung der Anforderungen zum Datenschutz kontrollieren. Sie sind dabei nicht die Datenschutzpolizei, die jeden Verstoss ahnden muss. › Beherzigen Sie stets, dass Sie risikoorientiert arbeiten sollen. Das gilt auch für Prüfungen.	○ Ja ○ Nein
Ich arbeite meinen festgelegten Fragenkatalog konsequent ab?	› Fragen, die Sie vorab festgelegt haben, sollten Sie auch tatsächlich stellen. › Wollen Sie Fragen übergehen, notieren Sie den entsprechenden Grund.	○ Ja ○ Nein
Ich gestalte die Befragung so, dass alle Auditierten umfassend antworten können?	› Lassen Sie die Geprüften reden und nehmen Sie sich zurück. › Geben Sie die nötige Zeit, um Antworten zu durchdenken.	○ Ja ○ Nein
Bei Aspekten, die ich nicht beurteilen kann, hole ich Expertenwissen ein?	› Sie können sich nicht bei allem auskennen. Sind Sie sich unsicher, fragen Sie die zuständigen Spezialisten. › Dokumentieren Sie, wen Sie einbezogen haben und was man Ihnen geraten hat.	○ Ja ○ Nein
Erkenntnisse und Feststellungen halte ich sofort fest?	› Verschieben Sie das nicht auf später. Denn was nicht gleich notiert wird, wird ggf. vergessen oder bleibt in falscher Erinnerung. › Haben Sie immer etwas parat, um Notizen oder Fotos zu machen. Auch Sprachnotizen sind hilfreich.	○ Ja ○ Nein
Abschlussbesprechung		
Direkt nach dem Audit bespreche ich mit den Auditierten das Ergebnis?	› Lassen Sie die Geprüften nicht im Ungewissen. Nehmen Sie sich die Zeit für ein kurzes Abschlussgespräch. › Idealerweise können Sie bereits einen vorläufigen Bericht zur Verfügung stellen.	○ Ja ○ Nein
Ich lasse andere Auffassungen zu?	› Viele Dinge kann man unterschiedlich sehen. Geben Sie Gelegenheit zur Stellungnahme. › Notieren Sie andere Sichtweisen. Lassen Sie diese im Bericht nicht unerwähnt.	○ Ja ○ Nein
Es werden erste Massnahmen festgelegt?	› Bereits in der Abschlussbesprechung können erste Massnahmen vereinbart werden. › Denken Sie daran, Verantwortlichkeiten und Termine für das weitere Vorgehen festzulegen.	○ Ja ○ Nein
Bericht		
Ich halte alle wesentlichen Berichtsaspekte direkt nach dem Audit fest?	› Beschreiben Sie objektiv, was geprüft wurde, welche Nachweise es gibt und worin Defizite bestehen. › Erwähnen Sie auch Positives. Das motiviert alle Kolleginnen und Kollegen für die Zukunft und trägt zur Datenschutzakzeptanz bei. › Achten Sie generell auf einen positiven Grundton. Vermeiden Sie Vorwürfe. Bleiben Sie sachlich und immer freundlich und zugewandt.	○ Ja ○ Nein
Defizite und Mängel habe ich nach ihrem Schweregrad bewertet?	› Machen Sie eine Einschätzung, ob Defizite gering, mittel oder gravierend sind. Das unterstreicht den Handlungsbedarf. › Orientieren Sie sich hier an den Massstäben der internen Revision.	○ Ja ○ Nein
Empfehlungen zur Behebung der Defizite oder Mängel spreche ich im Bericht aus?	› Geben Sie Hinweise, wie aus Ihrer Sicht Defizite behoben werden können. Allerdings sollten Sie auch andere Wege zum Ziel zulassen. › Achten Sie hier auf Realitätsbezug. Die Umsetzung muss für die Mitarbeiter und Mitarbeiterinnen möglich und machbar sein.	○ Ja ○ Nein

Datenabfluss: Setzen Sie jetzt auf diese 10 Tipps

Die Beschäftigten Ihres Unternehmens wissen: Geht es um Fragen mit Datenschutzrelevanz, dann sind sie bei Ihnen an der richtigen Adresse. Das gilt umso mehr, wenn Beschäftigte vermuten, dass Daten in falsche Hände geraten sind. In diesem Fall muss schnell gehandelt werden.

Gründe für einen Datenabfluss kann es viele geben. Es muss nicht ein Angriff von Cyberkriminellen sein. Auch ein falsch konfigurierter Onlineshop oder ein Server können Informationen für Unbefugte offenlegen oder abrufbar machen. Meldet sich ein Beschäftigter bei Ihnen, können Sie viel dazu beitragen, dass sich ein möglicher Schaden in Grenzen hält. Beherzigen Sie dazu diese Tipps:

Tipp Nr. 1: Hören Sie zu und strahlen Sie Ruhe aus

Weil die Sache eilt, wird man Sie wahrscheinlich per Telefon kontaktieren. Nehmen Sie die Sache und den Anrufer ernst. Beruhigen Sie ihn. Drücken Sie das auch so aus. Auch bestätigende oder positive Formulierungen helfen dabei, den „erhöhten Blutdruck" aus der Sache zu nehmen. Wichtig ist zudem: Hören Sie zu. Wimmeln Sie auf keinen Fall den Anrufer ab. Das kann nach hinten losgehen und unter Umständen sind dann gerade Sie die Ursache dafür, dass nicht schnell gehandelt wird.

Tipp Nr. 2: Klären Sie die Situation

Lassen Sie sich konkret schildern, was passiert ist bzw. worauf die Wahrnehmung des Anrufers beruht. Um möglichst viele Informationen zu erhalten, sollten Sie W-Fragen nutzen, und zwar so wie auch eine Rettungsleitstelle sich einen Überblick über eine Situation verschaffen würde. Fragen Sie etwa: Was ist passiert? Wer hat was und wie bemerkt? Welche und wessen Daten sind betroffen? Wer ist für die betroffene Bearbeitung verantwortlich?

Tipp Nr. 3: Stossen Sie die sofortige Eindämmung an

Gibt es spezifische Notfall- oder Incident-Response-Pläne, sollten Sie die dort vorgegebenen Prozesse starten. Weichen Sie nach Möglichkeit nicht davon ab. Hakt es jedoch irgendwo, etwa weil ein Ansprechpartner nicht verfügbar ist, sollten Sie die Sache pragmatisch handhaben.

Fehlen entsprechende Pläne, gilt: Veranlassen Sie unverzüglich, dass der Datenabfluss gestoppt wird. Ihr erster Ansprechpartner wird hier die IT-Abteilung oder eine Fachabteilung sein. Diese müssen sofort das Nötige veranlassen und beispielsweise IT-Systeme vom Internet trennen oder Zugriffsrechte einschränken. Die betroffenen Systeme oder Bearbeitungen dürfen erst wieder online gehen, wenn ein erneuter Datenabfluss ausgeschlossen ist.

Tipp Nr. 4: Berufen Sie ein Reaktionsteam ein

Gerade wenn die Sache grösser ist, kommen Sie nicht drum herum, alles Relevante im Team abzustimmen und die nächsten Massnahmen festzulegen. Neben IT- und Fachabteilung können auch die Unternehmenskommunikation oder die Rechtsabteilung relevante Teilnehmer sein. Auch einen Vertreter der Unternehmensleitung sollten Sie nicht vergessen.

Tipp Nr. 5: Ermitteln Sie Umfang und Schutzbedarf

Einerseits sollten Sie das tatsächliche Vorliegen eines Vorfalls bewerten. Andererseits ist es unerlässlich, das Ausmass des Vorfalls zu bewerten. Dabei spielt nicht nur die Zahl der betroffenen Personen eine Rolle. Prüfen Sie auch die Menge und Sensibilität der betroffenen Daten. Denn klar ist: Je sensibler und schadensträchtiger die Daten sind, desto entschlossener muss Ihr Unternehmen handeln.

Tipp Nr. 6: Bewerten Sie die Risiken

Analysieren Sie, welche Gefahren für betroffene Personen. Bewerten Sie dann das Risiko auf Basis der Faustformel „Schadenshöhe x Eintrittswahrscheinlichkeit". Hohe Risiken müssen schnellstens angegangen werden. Dokumentieren Sie die Risikoanalyse.

Tipp Nr. 7: Prüfen Sie die Melde- und Infopflichten

Bewerten Sie gemeinsam, inwieweit eine Meldung nach Art. 24 Bundesgesetz über den Datenschutz (DSG) so rasch als möglich an den EDÖB erforderlich ist, weil die Verletzung zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen kann.

Tipp Nr. 8: Bereiten Sie nötige Entscheidungen vor

Als Datenschutzberater sind Sie nicht in der Entscheidungs- und Umsetzungsverantwortung. Belassen Sie diese beim Unternehme. Sprechen Sie allerdings Empfehlungen aus, etwa gegenüber der Unternehmensleitung. Unterstützen Sie beratend bei der Entscheidungsfindung, etwa bezüglich einer Meldung oder Presseinformation.

Tipp Nr. 9: Begleiten Sie die Sache bis zum Abschluss

Datenabflüsse haben wie alle Datenpannen höchste Priorität. Räumen Sie der Sache Vorrang vor anderen Themen und Terminen ein. Stehen Sie für kurzfristige Termine bereit und begleiten Sie die festgelegten Massnahmen fortlaufend.

Tipp Nr. 10: Dokumentieren Sie alles Wichtige

Alles Relevante sollte festgehalten werden, etwa Sachverhalt, Bewertungen, Begründungen, Entscheidungen und Massnahmen. Dokumentieren Sie auch Ihre Beratung.

KI-Risiken richtig bewerten: Darauf müssen Sie achten

Für Sie als Datenschutzberater 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 Bearbeitungssituationen 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 Personen 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 Bearbeitung.	Einsatz erklärbarer Modelle (Explainable AI), detaillierte Dokumentation von Modellen und Entscheidungslogik, interne Prüf- und Freigabeprozesse sowie regelmässige Audits
Fehlende Erklärbarkeit gegenüber betroffenen Personen	Entscheidungen oder Ergebnisse können gegenüber betroffenen Personen nicht verständlich oder nachvollziehbar begründet werden. Dies ist insbesondere bei automatisierten Entscheidungen problematisch, da betroffenen Personen 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 bearbeitet, gespeichert oder weitergegeben werden. Besonders bei externen KI-Diensten oder komplexen Systemlandschaften besteht ein erhöhtes Risiko intransparenter Datenbearbeitung. 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 Datenbearbeitung	Es werden grosse Mengen Personendaten bearbeitet oder analysiert, häufig auch in aggregierter Form, wodurch das Risiko für die Rechte und Freiheiten der betroffenen Personen 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 Datenbearbeitung	Daten werden für andere Zwecke verwendet als ursprünglich vorgesehen, etwa zur weiter Bearbeitung als Trainingsdaten oder für neue Analysen, ohne ausreichende Rechtsgrundlage.	Klare Zweckdefinition, getrennte Bearbeitung, 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 Datenbearbeitung, 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	Bearbeitung, Entscheidungslogik und Datenflüsse sind nicht ausreichend dokumentiert, was die Nachvollziehbarkeit und Rechenschaftspflicht erheblich erschwert.	Durchführung und Pflege einer DSFA, Verzeichnis von Bearbeitungstätigkeiten, 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 Personendaten 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 weiterbearbeitet.	Richtlinien zur Dateneingabe, technische Sperren, Sensibilisierung der Mitarbeitenden
Fehlende Lösch- und Kontrollmöglichkeiten	Einmal bearbeitete 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

Wer schreibt, der bleibt: Machen Sie Ihre Arbeit belegbar

Sie kennen vielleicht die geflügelten Worte aus der Überschrift: Auch wenn mancher das gerne einfach so dahinsagt, steckt viel Wahres darin. Kann man die eigene Arbeit belegen, wird es für andere schwierig, einem an den Karren zu fahren. Das gilt gerade für Sie als Datenschutzberater.

Dokumentieren ist wichtig

Für Datenschutzberater besteht keine gesetzliche Verpflichtung, die Arbeit belegbar zu machen. Allerdings liegt genau das in Ihrem Eigeninteresse. Können Sie belegen, wie Sie bei einer bestimmten Frage beraten haben, wird es schwer, das Gegenteil zu behaupten. Zudem bringen Sie Konsistenz in Ihre Beratung oder in Ihre Kontrollen, wenn Sie auch nach Jahren noch nachvollziehen können, wie Sie die Dinge gesehen haben.

Allerdings liegt auf der Hand, dass Sie nicht immer einfach alles dokumentieren können. Damit Sie die richtige Wahl treffen und geschickt beim Dokumentieren vorgehen, sollten Sie die folgenden Tipps beherzigen:

Tipp 1: Setzen Sie auf Risikoorientierung

Sie können nicht alles dokumentieren. Das wäre weder zeitlich möglich, noch wäre es zielführend. Wichtig ist daher, dass Sie sich auf Sachverhalte, Beratungen und Kontrollen zu Bearbeitungen mit hohem Risiko- oder Schadenspotenzial konzentrieren. Auch ein mulmiges Gefühl kann entscheidend sein, um etwas genau festzuhalten.

Am besten Sie orientieren sich an folgender Faustformel: Dokumentieren Sie immer dann, wenn es datenschutzrechtlich kritisch, komplex, knifflig oder heikel werden kann. Bagatellanfragen oder Alltagsthemen können Sie unter den Tisch fallen lassen.

Tipp 2: Halten Sie Komplexes schriftlich fest

Gerade wenn man Sie nicht gern mit Informationen versorgt, Ihnen vielleicht auch ein X für ein U vormachen will oder wenn es kompliziert wird, ist wichtig: Halten Sie im Detail den Sachverhalt fest. Lassen Sie sich im Zweifel bestätigen, dass Ihre Darstellung zutreffend ist. Erst dann beginnen Sie mit Ihrer Beratung, die Sie auf genau diesen Sachverhalt zuschneiden. Dieses Vorgehen hat einen entscheidenden Vorteil: Ist der Sachverhalt fixiert, kann Ihnen später niemand vorwerfen, dass Sie etwas falsch verstanden hätten.

Tipp 3: Standardisieren Sie Ihre Dokumentation

Damit Ihnen das Dokumentieren leichter von der Hand geht und Sie nicht mal dies und mal jenes vergessen, können Sie auf ein Formular setzen. Erstellen Sie sich eine Vorlage, die Sie ausgedruckt im Termin handschriftlich befüllen können. Sie können sich auch eine E-Mail-Vorlage bauen oder eine Standardseite in einer Notizsoftware wie z. B. Microsoft OneNote. Nehmen Sie alle wichtigen Aspekte auf, die es zu dokumentieren gilt. So z. B.:

- alles Relevante zu einem Termin (insbesondere Zeitpunkt, Teilnehmer, Anlass, Thema)
- Sachverhalt und relevante Aspekte
- Ihre Bewertung und Empfehlungen
- Entscheidungen, Massnahmen und Fristen.

Tipp 4: Dokumentieren Sie Prüfungen und Audits

Entsprechende Berichte sind Ihre zentralen Nachweisdokumente, etwa gegenüber der Unternehmensleitung. Bei jeder Prüfung sollten Sie festhalten, was Sie geprüft haben, welche Belege Sie vorgefunden haben und welche Schlüsse gezogen wurden.

Zudem sollten Sie dokumentieren, welche Massnahmen mit wem vereinbart wurden und bis wann diese umzusetzen sind. Solche Berichte können Sie um Fotos, Screenshots oder andere Nachweise ergänzen, um Ihre Feststellungen zu belegen. Bewahren Sie Ihre Berichte mindestens bis zum nächsten Audit auf, um prüfen zu können, ob man aus früheren Fehlern tatsächlich gelernt hat.

Tipp 5: Setzen Sie bei Brisantem auf Unterzeichnetes

Ist etwas heikel, etwa weil man gegen Ihren Rat handeln will, sollten Sie ein Protokoll erstellen, das von den Beteiligten handschriftlich zu unterzeichnen ist. Das kann einerseits noch einmal zum Umdenken führen.

Ist das nicht der Fall, haben Sie andererseits einen Nachweis, der „gerichtsfest" ist. Schliesslich lässt sich die Bestätigung von Inhalten durch Unterschrift kaum anzweifeln.

Tipp 6: Dokumentieren Sie Pannen akribisch

Hier kann es immer dazu kommen, dass später einmal der EDÖB als Datenschutzaufsichtsbehörde nachfragt. Und der kann auch Ihre Beratung und Ihr Handeln unter die Lupe nehmen.

Dokumentieren Sie daher genau, wer wann wen informiert hat, welche Bewertung Sie vorgenommen haben und welche Entscheidungen von wem getroffen wurden.

Tipp 7: Haben Sie ein Auge auf die Zukunftsfähigkeit

Egal, wie Sie dokumentieren, denken Sie daran, dass Sie die Informationen ggf. in Zukunft brauchen werden. Nutzen Sie also Standardsoftware und Standardformate. Denken Sie auch an Back-ups. Alternativ ist manchmal auch Handgeschriebenes, das selbstverständlich in einer Schrift verfasst sein sollte, die auch später noch leserlich ist oder Ausgedrucktes die bessere bzw. dauerhaftere Lösung.

Braucht unser Newsletter eigene Datenschutzhinweise?

FRAGE: Kürzlich hat sich eine Betroffener bei uns wegen unseres E-Mail-Newsletters beschwert. Wir würden gegen den Datenschutz verstossen, weil der Newsletter keine Informationen zum Datenschutz enthält. In diesem Zusammenhang fragen wir uns: Braucht unser E-Mail-Newsletter tatsächlich eigene Datenschutzhinweise?

ANTWORT: Egal, ob Ihr Unternehmen die Registrierung für den Newsletter auf der Webseite, in einem Onlineshop oder in einer Smartphone-App anbietet. In der Regel zielt dies auf die Bearbeitung von Personendaten ab, etwa der E-Mail-Adresse und des Namens des Empfängers.

Bei der Erhebung muss informiert werden

Will Ihr Unternehmen Personendaten bearbeiten, muss es für die erforderliche Transparenz sorgen. Werden die Personendaten bei der betroffenen Person erhoben, müssen die Informationen nach Art. 19 Bundesgesetz über den Datenschutz (DSG) mitgeteilt werden. Und nun kommt das Entscheidende: Die Informationen müssen zum Zeitpunkt der Beschaffung der Daten gegeben werden. Die betroffene Person muss also vorab wissen können, was mit ihren Personendaten passiert. Dadurch wird die betroffene Person in die Lage versetzt, sich für oder gegen eine Bearbeitung ihrer Daten zu entscheiden.

Einmalige Information reicht aus

Das DSG sieht keine mehrmalige Information der betroffenen Person vor. Es reicht die Information zum Zeitpunkt der Beschaffung aus. Das hat für Ihren Fall zur Folge, dass bei der Registrierung für den Newsletter die Möglichkeit zur Kenntnisnahme der relevanten Informationen gegeben werden muss. Dazu kann beispielsweise ein Link zu den Datenschutzhinweisen gesetzt werden. Über diesen werden der betroffenen Person die nötigen Informationen bereitgestellt.

Im Ergebnis besteht also keine Pflicht, im Newsletter selbst Datenschutzhinweise zu integrieren. Allerdings kann es aus pragmatischen Gründen sinnvoll sein, neben einer Abmeldemöglichkeit auch einen Link zu den Datenschutzhinweisen Ihres Unternehmens aufzunehmen. Eventuell kommt es dann gar nicht zu Anfragen von betroffenen Personen, weil sie den Umgang mit den Personendaten jederzeit über die Datenschutzhinweise nachvollziehen können.

Wie kann ich meinen Chef zum Kauf eines neuen Schredders bewegen?

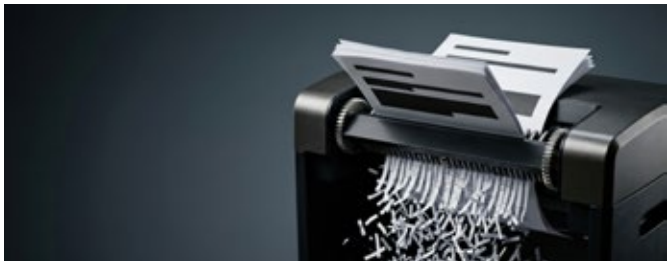
FRAGE: Bei meinem sehr sparsamen Chef habe ich einen „historischen" Aktenvernichter entdeckt. Den will er weiter nutzen, auch wenn dieser nur einen relativ breiten „Spaghettischnitt" beherrscht. Wie kann ich ihn von einer Neuanschaffung überzeugen?

ANTWORT: Argumentieren Sie zunächst mit dem Datenschutz bzw. rechtlichen Pflichten. Damit Personendaten nicht von Unbefugten zur Kenntnis genommen werden können, müssen risikoangemessene Schutzmassnahmen ergriffen werden. Das ergibt sich aus dem Bundesgesetz über den Datenschutz (DSG), konkret aus Art. 8 Abs. 1.

Daher muss auch bei einem Schredder dessen Funktion zum Schutzbedarf passen. Schon bei normalen Personendaten wäre ein Schredder mit „Spaghettischnitt" nicht risikoangemessen. Eine so geschredderte Seite lässt sich relativ leicht wieder zusammensetzen. Streifenschnitt entspricht meist der Sicherheitsstufe 1 und ist ungeeignet. Geraten Daten so in falsche Hände, kann das zu viel Ärger führen. Empfehlen Sie die Anschaffung eines Schredders, der Mikroschnitt (Sicherheitsstufe 5) beherrscht, sodass ein Zusammensetzen von Seiten praktisch unmöglich ist.

Argumentieren Sie mit der Steuer

Überzeugend kann allenfalls auch folgendes Argument sein: Ein Schredder kann in der Regel als geringwertiges Wirtschaftsgut im Jahr der Anschaffung komplett als Betriebsausgabe abgesetzt werden. Insofern ist der „Schmerz" der Kosten geringer. Dem Datenschutz erweist Ihr Chef jedoch einen grossen Dienst.



BGH: Registergericht muss Unterschriften entfernen

Als jemand mit viel Datenschutz-Know-how wissen Sie: Beim Bearbeiten von Personendaten muss auf Datensparsamkeit geachtet werden. Sind Daten nicht erforderlich, darf die Bearbeitung nicht stattfinden. Genau das meint nun auch der Bundesgerichtshof (BGH), das höchste deutsche Zivilgericht, zu Einträgen im Handelsregister (Beschluss vom 18.2.2026, Az. II ZB 2/25).

Das führte zum Rechtsstreit

Ausgangspunkt des Rechtsstreits sind im „Gemeinsamen Registerportal der Länder" veröffentlichte gesellschaftsrechtliche Dokumente zu einer als „GmbH & Co. KG" eingetragenen Firma. In der Dokumentenansicht des Registers waren zwei Dokumente zu finden. Diese enthielten unter anderem die händischen Unterschriften sowie Privatanschriften der Geschäftsführer der an der Firma beteiligten Gesellschaften.

Die beiden Geschäftsführer der beteiligten Unternehmen stellten den Antrag beim Registergericht, dass die betreffenden Dokumente ausgetauscht werden sollten. Die Ersatzdokumente sollten nicht mehr ihre Privatanschriften und ihre Unterschriften enthalten. Stattdessen sollten in den neuen Dokumenten nur die Anschriften der an der Firma beteiligten Gesellschaften enthalten sein. Ferner sollten die Unterschiften durch einen „gez."-Vermerk mit getipptem Namen ersetzt werden.

Antragsteller wollen sich schützen

Aus Sicht der Antragsteller gab es gute Gründe für einen Austausch der veröffentlichten Dokumente. So bestehe ein Risiko, Opfer von Straftaten zu werden. Jedermann hätte die Möglichkeit, die Dokumente mit Privatanschrift und Unterschrift einzusehen. Mit den gesammelten Daten könnten Kriminelle Profile erstellen und in krimineller Absicht nutzen.

Vor dem BGH erfolgreich

Das Registergericht sah kein Problem in der Veröffentlichung der Dokumente und der enthaltenen Daten. Es lehnte die Anträge ab. Also reichten die Antragsteller Beschwerde beim Hanseatischen Oberlandesgericht (OLG) ein. Doch auch dort blieben sie ohne Erfolg. Das OLG entschied, dass das Registergericht die Anträge zu Recht abgelehnt hatte. Auf einen möglichen Austauschanspruch aus Art. 17 Abs. 1 Buchst. b Datenschutz-Grundverordnung (DSGVO) komme es nicht an. Denn die Antragsteller hätten kein rechtliches Interesse am Austausch der Dokumente. Das Risiko krimineller Machenschaften bestehe auch nach einem Austausch der Dokumente.

Die Entscheidung des OLG wollten die Antragsteller so nicht akzeptieren. Also zogen sie vor den BGH. Dort hatten sie mit ihren Argumenten Erfolg. Der BGH hob die Entscheidung des OLG auf und verwies die Sache an das Registergericht zurück. Dabei wurde die Verpflichtung ausgesprochen, den Austausch der veröffentlichten Dokumente gegen Dokumente ohne Privatanschriften und Unterschriften zuzulassen.

So urteilte der BGH

Aus Sicht des BGH lagen die Richter der Vorinstanz falsch. Für die Beschwerdeführer besteht ein Anspruch auf Austausch der Dokumente nach Art. 17 Abs. 1 DSGVO i. V. m. § 9 Abs. 7 Handelsregisterverordnung (HRV). Art. 17 Abs. 1 DSGVO setzt kein rechtliches Interesse an einer Löschung voraus. Es müssen nur die Voraussetzungen erfüllt sein. Gründe, nach denen eine Löschung unterbleiben kann, sind abschliessend in Art. 17 Abs. 3 DSGVO geregelt. Darüber hinaus kann den Antragstellern kein missbräuchliches Verhalten angelastet werden. Insbesondere soll mit der betreffenden Handlung kein ungerechtfertigter Vorteil erlangt werden.

Austausch kommt Löschen gleich

Es ist für den Löschanspruch nach Art. 17 DSGVO nicht erforderlich, dass dieser für die Löschung eines personenbezogenen Datums aus allen Speicherbeständen geltend gemacht wird. Ein Betroffener kann den Umfang seines Löschungsrechts weitgehend selbst bestimmen und auch selektiv vorgehen. Der geforderte Austausch der Dokumente ist vom Löschungsanspruch aus Art. 17 Abs. 1 DSGVO umfasst. Der Erfolg einer Löschung, sprich das Unbrauchbarmachen der Daten, kann auch durch einen Austausch von Dokumenten erfolgen.

Verarbeitung nicht gerechtfertigt

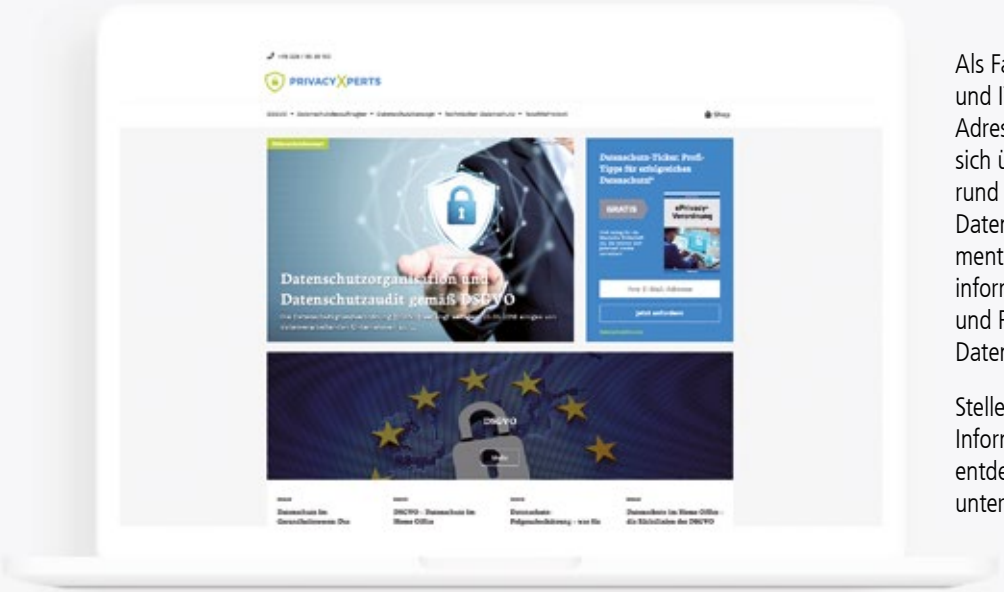
Ein Grund zur Löschung gemäss Art. 17 Abs. 1 Buchst. b DSGVO und für einen Dokumentenaustausch liegt nach § 9 Abs. 7 HRV vor. Die bisherige Verarbeitung der betreffenden Daten lässt sich nicht auf eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO stützen. Insbesondere besteht keine Verpflichtung, mehr Daten zu verarbeiten als für Registerzwecke erforderlich sind. Gründe für einen Ausschluss der Löschung nach Art. 17 Abs. 3 DSGVO fehlen. Insbesondere besteht kein öffentliches Interesse, das einer Bereinigung der Registerordner entgegensteht.

§

In der Schweiz gelten die gleichen Grundsätze

Für das Bearbeiten von Personendaten bedarf es immer einer Rechtfertigung. Werden mehr Daten als erforderlich bearbeitet, kann das einen Löschanspruch betroffener Personen auslösen. Eventuell kann es im Einzelfall reichen, bestimmte Informationen auszutauschen. Das sollte dann geprüft werden.

„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**

Erstellt für Schweizer Datenschutzberater
und für alle mit Aufgaben im Datenschutz
in der Schweiz von:

PRIVACYXPERTS

Telefon: +49 2 28 95 50 150
Fax: +49 2 28 36 96 480
E-Mail: kundendienst@privacyxperts.de
Internet: kurzlink.ch/privacy

Ein Unternehmensbereich des VNR Verlags
für die Deutsche Wirtschaft AG
Theodor-Heuss-Strasse 2–4
53177 Bonn, Deutschland

Vorschau:

Schutz vor Cybercrime:
Stärken Sie die erste Verteidigungslinie

USB-Sticks:
Beugen Sie mit 10 Regeln Datenpannen vor