DATENSCHUTZAKTUELL
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH
Schweiz
NOV 2025

UNBEKANNTES RISIKO SCHATTEN-IT: BRINGEN SIE LICHT INS DUNKEL

Onlinebereich:
www.kurzlink.ch/privacy

PRIVACYXPERTS

Gesundes Misstrauen ist immer gut

Liebe Leserin, lieber Leser,

als Datenschutzberater sind Sie ein gefragter Ansprechpartner. Schliesslich wollen auch die Mitarbeiter Ihres Unternehmens nach Möglichkeit nichts falsch machen, wenn Personendaten im Spiel sind. Doch manch einer will sich vielleicht eher Ihr „grünes Licht" ergaunern und bleibt bei seinen Informationen nicht ganz bei der Wahrheit.

Gerade wenn eine Sache irgendwie „zu rund" ist oder man nur ganz schnell noch Ihren „Segen" einholen will, sollten Sie misstrauisch sein. Lassen Sie sich kein X für ein U vormachen. Klären Sie alles, was Sie für Ihre Einschätzung brauchen. Dann passt auch Ihre Beratung.

Viele Grüsse

Andreas Würtz,
Rechtsanwalt und Chefredaktor

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

Inhalt

Expertensprechstunde:
https://kurzlink.ch/kontakt-wuertz

Bildnachweise:
Titel: Adobe Stock | BalanceFormCreative
Seite 1: Adobe Stock | greenbutterfly

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

Verantwortlicher Chefredakteur:
RA Andreas Würtz, Freiberg am Neckar
Design: Kreativ Konzept Agentur für Werbung, Bonn
Satz: Deinzer Grafik, Gartow
Druck: Warlich Druck Meckenheim GmbH, Meckenheim
Erscheinungsweise: 16-mal pro Jahr
E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de
(bei Rückfragen bitte Kundennummer angeben)

Alle Angaben wurden mit äusserster Sorgfalt ermittelt und überprüft. Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen. Eine Gewähr kann deshalb nicht übernommen werden.
Im Interesse der Lesbarkeit verzichten wir in unseren Beiträgen auf geschlechtsbezogene Formulierungen. Selbstverständlich sind immer Frauen und Männer gemeint, auch wenn explizit nur eines der Geschlechter angesprochen wird.
Dieses Produkt besteht aus FSC®-zertifiziertem Papier.

Nutzen Sie unsere Anleitung, um Schatten-IT aufzuspüren.

Unbekanntes Risiko Schatten-IT: Bringen Sie Licht ins Dunkel

Als Datenschutzprofi wissen Sie: Für den Schutz aller Daten im Unternehmen ist es unerlässlich, dass Risiken erkannt und angemessene Massnahmen ergriffen werden, um diese zu minimieren. Doch manche Gefahren sind nicht offenkundig und gleichen dennoch einer Zeitbombe. So ist das beispielsweise beim Thema Schatten-IT der Fall. Bringen Sie hier Licht ins Dunkel.

Das ist das Problem

Schatten-IT und Schatten-Software hat nichts mit viel Sonne zu tun. Gemeint sind insbesondere IT-Systeme oder Software, die unerkannt „im Schatten liegen", weil sie von Abteilungen oder Mitarbeitern ohne Wissen und Genehmigung der IT-Abteilung beschafft und eingesetzt werden. Ohne lange grübeln zu müssen, erkennen Sie ganz schnell, dass das früher oder später schiefgehen kann. Schliesslich ist zu bedenken:

- Schatten-IT und Schatten-Software bringen häufig auch eine unklare Sicherheitssituation mit sich. Manchmal wird einfach beschafft, ohne zu wissen, wie es um die Sicherheit der Systeme oder Software bestellt ist. Denn nur weil etwas funktioniert und seinen primären Zweck erfüllt, heisst das nicht, dass damit bearbeitete Daten auch sicher sind.

- Gerade im Zusammenhang mit Personendaten muss bei deren Bearbeitung auf die Sicherheit geachtet werden. Nach Art. 8 Abs. 1 Bundesgesetz über den Datenschutz (DSG) müssen risikoangemessene Schutzmassnahmen ergriffen werden. Und die treffen Ihr Unternehmen als Verantwortlicher und nicht etwa einen Hersteller eines Systems oder einer Software.

- Schatten-IT und Schatten-Software fliegen oft unter dem Radar der IT-Abteilung. Konkret heisst das: Die Profis bekommen überhaupt nicht mit, dass es bestimmte Systeme oder Software gibt, die in eine Update-Strategie einzubeziehen sind. Die Folge: Entsprechende Hard- und Software wird nicht mit den nötigen Updates versorgt. Über die möglicherweise aufkommenden Sicherheitslücken haben Hacker und Cyberkriminelle leichtes Spiel.

- Unbekannte Systeme und Software sind gerade im Zusammenhang mit Personendaten ein grosses Problem: So können nötige Datenschutzvereinbarungen fehlen, etwa im Rahmen einer Auftragsbearbeitung nach Art. 9 DSG. Unter Umständen verwendet der Hersteller Personendaten für eigene Zwecke, ohne dass es hierfür eine Rechtsgrundlage gibt. Auch kann es Probleme mit den Betroffenenrechten geben, etwa im Hinblick auf die nötige Transparenz sowie die Umsetzung der Rechte auf Auskunft oder Löschung. Und solche Datenschutzverstösse können bekanntlich viel Ärger nach sich ziehen und schlimmstenfalls auch ein schmerzhaftes Bussgeld, für das die Portokasse nicht ausreicht.

- Schatten-IT und Schatten-Software können Ihr Unternehmen finanziell ruinieren, etwa nach einem erfolgreichen Angriff von Cyberkriminellen. Denn selbst eine entsprechende Versicherung wird unter Umständen nicht zahlen, weil Ihr Unternehmen grob fahrlässig einen Schaden herbeigeführt hat. Schliesslich hat es nicht dafür gesorgt, dass mögliche Risiken durch Schatten-IT und Schatten-Software ausgeschlossen werden.

Heben Sie die Hand

Als Datenschutzberater haben Sie nicht den Auftrag, die (Datenschutz-)Welt zu retten. Allerdings ist es Teil Ihres Beratungs- und Kontrollauftrags, dass Sie auf realistische Gefahren mit Datenschutzrelevanz hinweisen, und zwar für Ihr Unternehmen. Solche Risiken treten gerade im Zusammenhang mit unbekannter und unkontrolliert eingesetzter Hard- und Software auf. Dabei ist klar: Kommt es zu einer Datenpanne, ist es unerheblich, wer schlussendlich daran schuld ist. Ihr Unternehmen ist dafür verantwortlich. Auch das (Fehl-)Verhalten von Mitarbeitern wird ihm meist zugerechnet.

Sie wollen Schatten-IT und Schatten-Software aufspüren? Kein Problem. Sie brauchen hier nicht das Rad neu zu erfinden. Setzen Sie auf die folgende Schritt-für-Schritt-Anleitung:

Schritt 1: Sammeln Sie Einfälle und Ideen

Starten Sie zunächst damit, dass Sie sich Gedanken zu Ihrem Unternehmen, zur Geschäftstätigkeit und vor allem zu Bereichen machen, in denen Schatten-IT oder Schatten-Software zum Einsatz kommen könnten. Das kann z. B. in der Entwicklung sein. Schatten-Software finden Sie vielleicht im Bereich Vertrieb oder beim Marketing. Denken Sie hier auch an Ihre Beratungen, bei denen man sich mit den zur Verfügung stehenden Mitteln unzufrieden gezeigt hat. Auch unter Datenschutzaspekten Durchgefallenes wird vielleicht dennoch eingesetzt.

Schritt 2: Checken Sie das Verzeichnis von Bearbeitungstätigkeiten

Prüfen Sie die enthaltenen Bearbeitungstätigkeiten. Diese sollten vollständig erfasst sein. Achten Sie auch auf die Aktualität der Angaben. Finden Sie Angaben zu eingesetzten Systemen oder Software, sollten Sie auf Ihnen unbekannte Anbieter oder Produktnamen achten. Überlegen Sie ausserdem, welche Bearbeitungstätigkeiten fehlen könnten oder welche Bearbeitungen ggf. nicht erfasst sind.

Schritt 3: Schauen Sie sich im Unternehmen um

Informieren Sie sich, was in Ihrem Unternehmen läuft. Wichtige Erkenntnisse kann es auch bringen, wenn Sie sich vor Ort umschauen oder mit Mitarbeitern sprechen. Sehen Sie beispielsweise Gerätschaften, die eher privater Natur sind, sollten Sie klären, was es damit auf sich hat. Denn: Auch private Geräte können gefährliche Schatten-IT sein. Nicht anders ist es mit privater Software oder privaten E-Mail- oder Cloud-Lösungen. Für die ist der Unternehmenseinsatz tabu.

Schritt 4: Tauschen Sie sich mit den IT-Kollegen aus

Besprechen Sie sich mit den Kollegen aus der IT-Abteilung. Machen Sie deutlich, dass Schatten-IT und Schatten-Software auch unter Datenschutzaspekten ein grosses Problem sein können. So z. B., wenn es um die Sicherheit der Bearbeitung geht. Bitten Sie um die Einschätzung und Erfahrung der Kollegen zu diesem Thema. Hinterfragen Sie, was man unternimmt, um Schatten-IT und Schatten-Software nicht zum Problem werden zu lassen. Klären Sie, inwieweit verhindert wird, dass Hard- und Software abseits der Prozesse eingesetzt werden.

Schritt 5: Machen Sie ein gemeinsames Risiko-Brainstorming

Identifizieren Sie gemeinsam mit den IT-Kollegen einerseits die Bereiche, wo Schatten-IT und Schatten-Software ein Thema sein könnten. Überlegen Sie ausserdem, welche praktischen Möglichkeiten es gibt, die Sache zu überprüfen.

Schritt 6: Ermitteln Sie die Situation

Hier empfiehlt sich ein mehrstufiger Ansatz. So kann zunächst eine Prüfung der Dokumentation erfolgen. Schauen Sie mit den Kollegen der IT-Abteilung gemeinsam vorhandene Inventarlisten durch. Finden Sie dort offensichtlich veraltete Technik oder veraltete Software, hat man vielleicht in der betreffenden Abteilung schon auf etwas Neueres gewechselt. Eventuell wird Software auch zentral inventarisiert. Hier können die Kollegen meist schnell sagen, ob sie hier Unbekanntes oder Ungenehmigtes vorgefunden haben.

Als nächste Stufe bietet es sich an, dass Sie mit den Kollegen vor Ort nach dem Rechten schauen. Statten Sie den Bereichen einen Besuch ab. Führen Sie dort auch Interviews mit den Führungskräften und Mitarbeitern. Zeigen Sie die Risiken durch Schatten-IT und Schatten-Software auf und hinterfragen Sie, inwieweit man hierauf setzt.

Schritt 7: Identifizieren Sie den Handlungsbedarf

Ist Schatten-IT oder Schatten-Software im Einsatz, ist schnelles Handeln geboten. Klären Sie mit den Kollegen der IT-Abteilung und den betroffenen Bereichen, wie man zügig einen ordnungsgemässen und regelkonformen Zustand erreichen kann. Unter Umständen sollte die betreffende Hard- und Software zunächst einmal ausser Betrieb genommen werden, um Risiken zu minimieren.

Schritt 8: Vereinbaren Sie die nötigen Massnahmen

Achten Sie darauf, dass zügig gehandelt wird. Dabei ist klar: Über dieses Problem zu reden, reicht nicht aus. Es muss gelöst werden. Das geht nur mit den passenden Massnahmen. Damit es keine Missverständnisse darüber gibt, wer verantwortlich ist und was zu tun ist, sollten die Massnahmen konkret festgehalten und verbindlich vereinbart werden.

Schritt 9: Begleiten Sie die Umsetzung

Auch wenn es an das Umsetzen geht, kann Ihr Rat als Datenschutzberater gefragt sein. Wird das Thema „Schatten-IT und Schatten-Software“ bereinigt, müssen ggf. Daten umgezogen oder Datenträger entsorgt werden. Logisch, dass das sicher passieren muss.

Schritt 10: Kontrollieren Sie die Einhaltung

Als Datenschutzberater sollen Sie auch die Einhaltung der Vorschriften zum Datenschutz kontrollieren. Integrieren Sie hier den Punkt „Kontrolle von Schatten-IT und Schatten-Software“. Selbst wenn Sie nicht fündig werden, sollten Sie die Gelegenheit nutzen, um für die diesbezüglichen Gefahren zu sensibilisieren.

Datenschutz positiv vermitteln – so sorgen Sie für die richtige Vermarktung

Datenschutz wird von manchen Menschen eher als lästige Pflicht gesehen und nicht als Chance wahrgenommen. Dabei liegt genau im Datenschutz viel Positives und guter Datenschutz bringt für alle Vorteile, etwa für Unternehmen, Kunden und Beschäftigte. Dass Datenschutz positiv wahrgenommen wird, haben auch Sie in der Hand. Das ist kein Hexenwerk. So können Sie den Datenschutz besser „verkaufen".

Nicht nur wenn Ihr Unternehmen ein neues Produkt auf den Markt bringen will, ist das hier unerlässlich: das Marketing. Nicht anders ist es, wenn Sie das vielleicht bislang eher ungeliebte Thema Datenschutz zu etwas machen wollen, das jeder gut findet und das jeder bereitwillig unterstützt. Beherzigen Sie diese 5 Tipps:

Tipp 1: Setzen Sie auf eine positive Kommunikation

Braucht man Datenschutz wirklich? Bei solch einer Frage muss ein „Na klar" wie aus der Pistole geschossen kommen. Doch diese Antwort sollte nicht nur bei Ihnen kommen. Wichtig ist, dass auch andere im Unternehmen und insbesondere die Entscheidungsträger voll und ganz von dieser Antwort überzeugt sind. Dazu trägt auch bei, dass Sie vom Datenschutz ein positives Bild vermitteln. Machen Sie bei jeder Gelegenheit deutlich, dass gelebter Datenschutz

- **Vorteile im Wettbewerb bringt:** Es ist immer gut, sich von der Konkurrenz abzuheben. Auch Datenschutz kann ein entscheidender Faktor sein.
- **kosteneffizient ist:** Durch gelebten Datenschutz werden Kosten für Schäden und Bussgelder vermieden. Das Geld ist anderswo besser investiert.
- **Vertrauen und Wertschätzung vermittelt:** Kunden und Mitarbeiter wollen, dass ihre Interessen und ihre persönlichen Informationen geschützt sind.
- **die Professionalität Ihres Unternehmens unterstreicht:** Schlampt Ihr Unternehmen im Datenschutz, kann das andere Unternehmen abschrecken.

Tipp 2: Schaffen Sie positive Emotionen

Das Thema Datenschutz muss positive Emotionen auslösen, dass es sich dabei um etwas Gutes und Erstrebenswertes handelt. Das schaffen Sie beispielsweise dadurch, dass Sie bei jeder Gelegenheit Folgendes machen:

- **Betonen Sie immer die Vorzüge:** Werden Sie nicht müde herauszustellen, was Datenschutz bewirkt und welche Benefits er mit sich bringt.
- **Zeigen Sie im Einzelfall die konkreten Vorteile auf:** Das grosse Bild vermitteln ist eine Sache. Viel greifbarer wird manches, wenn Sie etwa bei einem Vorhaben die Vorzüge konkret benennen.
- **Setzen Sie auf den Dominoeffekt:** Egal, ob Projekt oder Menschen, hat man mit Ihnen, Ihrer Arbeit oder dem Datenschutz positive Erfahrungen gemacht, wird man das Positive gern weitergeben. Mundpropaganda funktioniert noch immer ausgezeichnet und ohne dass Sie diese aktiv steuern müssen.

Tipp 3: Entwickeln Sie eine umfassende Kommunikationsstrategie

Ihr Ziel ist, dass Datenschutz präsenter und positiver wahrgenommen wird. Um das zu erreichen, ist eine gute Kommunikationsstrategie unerlässlich. Am besten ist es, wenn Sie sich hier mit den Kommunikationsspezialisten in Ihrem Unternehmen zusammensetzen. Erläutern Sie ganz offen, was Ihr Ziel ist. Die Kollegen können Ihnen nicht nur Strategietipps an sich geben. Sie haben auch einen guten Blick dafür, wie Sie Ihr Thema erfolgreich transportieren können bzw. wie Sie die Beschäftigten am besten erreichen. Auch sind die Kollegen meist die Türöffner schlechthin, wenn es um die Nutzung von Intranet, Mitarbeiterzeitung oder internem E-Mail-Newsletter geht. Etwa ein „Datenschutz-Tipp des Monats" kann eine gute Möglichkeit sein, Datenschutz kurzweilig näherzubringen.

Aber Vorsicht: Achten Sie bei einer solchen Strategie auch auf die Machbarkeit. Haben Sie kaum Zeit? Oder ist Texten bzw. interessante Artikel schreiben nicht Ihr Ding? Dann brauchen Sie jemanden, der das für Sie übernehmen kann. Eventuell sind in einem solchen Fall andere Formen der Kommunikation besser für Sie. So z. B. kurze Schulungen, die Sie rund um die Mittagspause anbieten. Auch eine offene Sprechstunde ist eine Möglichkeit.

Tipp 4: Setzen Sie Erfolge ins rechte Licht

Wann haben Sie zuletzt über Positives rund um den Datenschutz in Ihrem Unternehmen informiert? Wenn Sie sich nicht mehr daran erinnern können, heisst es, die Ärmel hochkrempeln. Ändern Sie das schleunigst. Schliesslich tragen Sie als Datenschutzberater entscheidend dazu bei, dass es diese Erfolge gibt. Feiern Sie Erfolge und berichten Sie anlassbezogen. Ansonsten bekommt das Management überhaupt nicht mit, dass gemeinsam mit dem ausländischen Dienstleister nach zähen Verhandlungen endlich das Thema Auftragsbearbeitung abgehakt werden kann. Im Übrigen sollten Sie Erfolgsberichte zum regelmässigen Bestandteil Ihrer Rücksprachen machen. Dabei müssen Sie sich nicht selbst loben. Erwähnen Sie einfach, dass Sie stolz auf das Erreichte sind.

Tipp 5: Sparen Sie nicht mit Lob

Lob weiss jeder zu schätzen. Dabei ist ein Lob nicht nur Wertschätzung. Es ist Antrieb für weitere Unterstützung und zugleich Motivation für andere. Ist etwas richtig gut gelaufen oder hat man Sie tatkräftig unterstützt, sollten Sie Ihr Lob nicht nur gegenüber den betreffenden Personen aussprechen. Platzieren Sie Ihr Lob auch anderswo, etwa an höherer Stelle. Das wirkt dann besonders nachhaltig.

Vorsicht, Mythen: Entzaubern Sie die Cyberversicherung Ihres Unternehmens

Hat Ihr Unternehmen eine Versicherung für Cybersicherheitsvorfälle, etwa für den Fall, dass Hacker zuschlagen, Cyberkriminelle Daten klauen bzw. zwecks Lösegelderpressung verschlüsseln? Wenn dem so ist, kann diese im Fall der Fälle hilfreich sein. Doch meist wiegt man sich in falscher Sicherheit. Gut, wenn Sie auf Stolperfallen hinweisen und mit Mythen rund um Cybersecurity-versicherungen aufräumen.

Eine Versicherung ist nur eine Säule in der Gesamtstrategie

Die Angst vor Cybersecurityvorfällen ist in vielen Unternehmen gross. Klar, dass man sich mit dem Abschluss einer entsprechenden Versicherung schnell etwas wohler fühlt. Und die „Rundum-sorglos-Versprechen" aus Gesprächen mit dem Versicherungsvertreter oder aus der Werbebroschüre klingen besonders beruhigend. Doch meist ist diese Wohlfühlatmosphäre schnell verflogen, wenn Sie auf einige typische Punkte hinweisen, die oftmals nicht bedacht und auch in keinem Verkaufsgespräch thematisiert werden. So z. B.:

- Entscheidend ist der tatsächlich vereinbarte Versicherungsumfang. Der ist meist nicht so umfassend, wie der Versicherungsnehmer meint. Viele Anforderungen, Auflagen oder Beschränkungen fallen erst auf, wenn der Vertrag und die Vertragsbedingungen intensiv geprüft werden.
- Das Unternehmen muss sich dennoch anstrengen. Ihr Unternehmen kommt aus der Verantwortung für risikoangemessene Schutzmassnahmen nicht heraus. Das betrifft den Schutz aller Systeme, Computer und Daten im Unternehmen. Passen die Schutzmassnahmen nicht oder nimmt man es etwa mit Updates nicht so genau, freut das die Versicherung. Sie muss meist nämlich nicht zahlen. Denn der Versicherungsnehmer hat gegen seine Obliegenheitspflichten verstossen. Auch hier lohnt der Blick in die Versicherungsbedingungen.
- Versicherungen sind keine Wohlfahrtsvereine. Ganz im Gegenteil. Wie jedes Unternehmen sind sie verpflichtet, Gewinn zu erwirtschaften. Dazu dürfen sie keine Risiken eingehen, die zu ihren Lasten gehen. Also schauen sie vor dem Vertragsschluss genau hin bzw. stellen ganz konkrete Fragen. Die sollten auch zutreffend beantwortet werden, wenn Ihr Unternehmen seinen Versicherungsschutz nicht riskieren will.

Tragen Sie zum umfassenden Risikomanagement bei

Mit einer Versicherungspolice in der Schublade meint manch ein Unternehmen, für den Fall der Fälle gut gerüstet zu sein. Doch meist wiegt man sich in falscher Sicherheit. Umso wichtiger ist, dass Sie als Datenschutzberater ein Auge darauf haben, was Ihr Unternehmen in Sachen Cybersecurity unternimmt. Teil dessen kann es sein, dass Sie zwecks Risikobewertung auch eine Versicherung unter die Lupe nehmen.

Bei einem Gespräch mit den zuständigen Kollegen können Sie auch mit typischen Mythen aufräumen. Setzen Sie auf die folgende Checkliste:

Sprechen Sie mit dem Risk-Owner
Unter Umständen gibt es in Ihrem Unternehmen jemanden, der sich um das Risikomanagement kümmert. Führen Sie am besten zunächst mit diesen Personen ein Gespräch. Klären Sie, wie man mit den Risiken durch Cyberkriminelle umgeht und inwieweit eine Versicherung besteht. Sprechen Sie an, inwieweit geprüft wurde, ob der vereinbarte Versicherungsschutz zum tatsächlichen Bedarf und zu den tatsächlichen Gegebenheiten passt. Will man hier nicht mit Ihnen reden oder meint man, dass Sie das alles nichts angehe, können Sie auf Art. 10 Bundesgesetz über den Datenschutz verweisen. Abhängig von den vereinbarten Leistungen kann ein Versicherungsschutz auch eine organisatorische Massnahme sein, um die Sicherheit der Bearbeitung von Personendaten zu gewährleisten. Und ob hier alles risikoangemessen ist, sollen Sie im Rahmen Ihres Beratungs- und Mitwirkungsauftrags eben auch kontrollieren. Beissen Sie auf Granit, sprechen Sie mit dem Risk-Owner. Das ist derjenige, der das Risiko verantwortet. Das ist schlussendlich die Unternehmensleitung.

CHECKLISTE: Mythen bei der Cybersecurityversicherung

Mythos	Das sollten Sie dazu erläutern	Besprochen?
Die Cyberversicherung deckt alles ab.	› „Alles" ist schon mal garantiert falsch und sollte Sie stutzig machen. Hinterfragen Sie, was die Kollegen genau damit meinen. Denn Sie wissen vielleicht auch aus privater Erfahrung: Geht es im Schadensfall darum, dass eine Versicherung zahlen soll, nimmt die es mit dem Versicherungsumfang meist ganz genau. › Schauen Sie gemeinsam in den konkreten Versicherungsschutz, aber auch in die Versicherungsbedingungen. Nicht selten enthalten Sie nur so ein umfassendes Bild des tatsächlichen Versicherungsschutzes.	☐ Ja ☐ Nein
Mit der Versicherung vermeiden wir Schlimmeres.	› Das ist zwar meist nicht falsch. Doch ganz richtig ist es auch nicht. Oft sind die Folgen von Cybersecurityvorfällen nicht vorher- und absehbar. Insofern passt ggf. die Versicherung auch nicht. › Folgeschäden werden oft nicht bedacht. Das können Schadensersatzforderungen von Geschäftspartnern oder Imageschäden sein. Auch das ist meist nicht abgesichert.	☐ Ja ☐ Nein

CHECKLISTE: Mythen bei der Cybersecurityversicherung		
Die Versicherung zahlt alle Schäden in voller Höhe.	› Eine Deckung für Schäden in unbegrenzter Schadenshöhe dürfte wohl kaum eine Versicherung zusichern. Schliesslich können gerade durch Cybersecurityvorfälle erhebliche Schäden drohen. › Bringen Sie auch immer die Datenschutzkomponente ins Spiel. Cybersecurityvorfälle haben meist auch Datenschutzrelevanz. Geraten Daten in falsche Hände, können Betroffene Schadensersatz fordern. Auch Bussgelder können drohen. Nicht selten sind gerade die vom Versicherungsschutz ausgenommen.	☐ Ja ☐ Nein
Mit den Angaben im Antrag für eine Versicherung muss man es nicht so genau nehmen.	› Wer so denkt, der kann sich das Geld für eine Versicherung auch sparen. Denn das ist der Grund Nummer eins, damit eine Versicherung nicht zahlen muss. Das Risiko für die Versicherung wird meist aufgrund der Angaben des Unternehmens bewertet. Flunkert Ihr Unternehmen beispielsweise bei Sicherheitsmassnahmen und sind diese Ursache für den Schaden, wird man genau auf die falschen Angaben abstellen und weniger bzw. nicht zahlen. Der Vertrag kann von der Versicherung ggf. wegen arglistiger Täuschung angefochten werden. Schliesslich hat Ihr Unternehmen böswillig über die Risikosituation getäuscht. › Lassen Sie sich doch einmal die Angaben aus dem Antrag nennen und machen Sie einen Realitätscheck. Eventuell sehen Sie schnell, dass das sich aus dem Antrag ergebende Soll nicht zum tatsächlichen Ist passt. Dann sollte schnellstens eine Anpassung erfolgen. › Das Ausfüllen und Bestätigen von Massnahmen sind nicht Ihre Sache als Datenschutzberater. Das muss die IT-Abteilung bzw. die Unternehmensleitung erledigen und auch verantworten.	☐ Ja ☐ Nein
Dank der Versicherung müssen wir weniger Aufwand in Sachen Sicherheit treiben.	› Versicherungen drücken in der Regel kein Auge zu, weil Ihr Unternehmen schon ein langjähriger Kunde ist oder weil man Verständnis für die Situation hat. Es stehen die nackten Fakten im Vordergrund. Was vereinbart wurde, muss umgesetzt werden, damit die Versicherung im Fall der Fälle tatsächlich leistet. › Generell darf ein Unternehmen nicht die Hände in den Schoss legen, gerade in Sachen Schutzmassnahmen. Die müssen risikoangemessen und wirksam umgesetzt sein. Selbst fehlende Awareness bei Mitarbeitern oder unpassende Notfallpläne können die Leistungspflicht der Versicherung zu Fall bringen. › Klären Sie für einzelne Leistungen oder Anforderungen, wie man im Unternehmen damit umgeht bzw. wie man diesen nachkommt. Insofern können Regelungen oder Prozesse erforderlich sein.	☐ Ja ☐ Nein
Im Fall der Fälle sind wir auf der sicheren Seite.	› Das ist Ihr Unternehmen garantiert nicht. Die Versicherung mag zwar finanziell einspringen oder bestimmte Tätigkeiten übernehmen. Das kann jedoch einige Zeit in Anspruch nehmen, auch wenn es eigentlich ziemlich schnell gehen sollte. › Gerade bei Cybersecurityvorfällen muss Ihr Unternehmen schnell handeln. Aber auch hier ist Vorsicht geboten. Ggf. macht die Versicherung auch hierzu Vorgaben. Eventuell legt sie fest, welche externen Spezialisten beauftragt werden dürfen. Hält sich Ihr Unternehmen nicht daran, bleibt es schlimmstenfalls auf den Kosten sitzen.	☐ Ja ☐ Nein
Die Versicherung zahlt schnell und unkompliziert.	› Wer hierauf hofft, hofft wahrscheinlich vergeblich. Bevor Versicherungen zahlen, prüfen diese, ob sie zahlen müssen. Das kann auch dazu führen, dass etwa Gutachter und IT-Spezialisten eingebunden werden, die die Sicherheitsmassnahmen Ihres Unternehmens unter die Lupe nehmen. Das kann dauern. Stellt sich heraus, dass diese nicht passen oder dass Ihr Unternehmen grob fahrlässig gebotene Massnahmen nicht ergriffen hat, gibt es ggf. keinen Cent. › Selbst wenn die Versicherung grundsätzlich zahlt, kann dies zunächst nur eine Abschlagszahlung sein. Die reicht ggf. nicht aus, um alles Nötige zu veranlassen.	☐ Ja ☐ Nein
Schadensersatzforderungen, Bussgelder und Lösegeldzahlungen werden von der Versicherung übernommen.	› Schauen Sie mit den Kollegen in den Versicherungsvertrag und die Versicherungsbedingungen. Oft werden solche Kosten nicht übernommen, sprich, Ihr Unternehmen bleibt darauf sitzen. › Eventuell wurde von den Kollegen ein solcher Kostenpunkt nicht bedacht. Hinterfragen Sie, wie man damit umgehen will. Dabei ist klar: Die Einstellung „Es wird schon irgendwie gut gehen“ ist schon allein unter Risikoaspekten für das Unternehmen nicht akzeptabel.	☐ Ja ☐ Nein
Die Versicherungssumme ist richtig bemessen und reicht vollkommen aus.	› Lassen Sie keinen Zweifel aufkommen: Alles wird teurer. Selbst wenn die Versicherungssumme automatisch angepasst wird, kann das dennoch schnell zu einer Unterversicherung führen, wenn Kosten schneller steigen als die Versicherungssumme. › Gerade wenn das Unternehmen wächst, muss die Versicherung entsprechend nachgezogen werden. Schauen Sie sich daher an, wann die letzte Bewertung bzw. Anpassung erfolgt ist.	☐ Ja ☐ Nein
Veränderungen im Unternehmen haben keinen Einfluss auf die Versicherung.	› Auch hierbei handelt es sich um einen gravierenden Denkfehler. Mit Veränderungen im Unternehmen verändern sich auch die Risiken. Und Versicherungen versichern immer nur die bekannten und vereinbarten Risiken. Setzt Ihr Unternehmen auf neue Technik oder spart es bei der IT-Sicherheit, kann sich die Risikosituation komplett ändern. Nicht anders ist es, wenn Ihr Unternehmen einen Onlineshop aufbaut, von dem die Versicherung bislang nichts weiss. › Machen Sie Veränderungen in der letzten Zeit aus. Lassen Sie sich erklären, wie sich das auf die Sicherheitssituation im Unternehmen ausgewirkt hat. Hinterfragen Sie auch, wie man sich hier mit der Versicherung bezüglich des Versicherungsschutzes abgestimmt hat.	☐ Ja ☐ Nein

Das sind die typischen Hotspots fehlender Schutzmassnahmen

Guter Datenschutz im Unternehmen hängt oft davon ab, dass die stattfindenden Bearbeitungen von Personendaten sicher sind. Doch sicher ist nicht gleich sicher und viel hilft nicht automatisch viel. Ihr Unternehmen muss risikoangemessene technische und organisatorische Massnahmen ergreifen. Vielleicht gibt es auch bei Ihnen Bereiche, wo das nicht so wirklich passt.

Schutz ist unerlässlich

Damit nichts durchs Raster fällt, sollten Sie immer wieder überlegen, wo es „unbekannte" Bearbeitungen geben könnte bzw. wo die Schutzmassnahmen eventuell nicht passen, veraltet oder nicht mehr risikoangemessen sind. Gehen Sie in drei Schritten vor:

1. Schritt: Prüfen Sie das Verzeichnis von Bearbeitungstätigkeiten

Damit verschaffen Sie sich einen ersten Überblick. Schauen Sie, wo viele Personendaten bearbeitet werden oder wo sensible Informationen im Spiel sind. Dabei sollten Sie sich nicht allein darauf verlassen, was Sie an Einträgen vorfinden. Eventuell fehlt so einiges.

2. Schritt: Finden Sie Bereiche mit möglichen Lücken

Machen Sie ein kleines Brainstorming und notieren Sie sich alle Einfälle zu relevanten Fragen, wie z. B.:

- Wo gibt es weisse Flecken auf meiner Datenschutzlandkarte des Unternehmens?
- Welche Bereiche arbeiten viel mit Personendaten?
- Wo gibt es grosse Veränderungen, etwa bei Bearbeitungen, Personal oder Technik?
- Bei welchen Bereichen habe ich als Datenschutzberater ein ungutes Gefühl?

Ausserdem können Sie die unten stehende Checkliste mit Schwerpunkten nutzen, bei denen man als Datenschutzberater im Unternehmen oft fündig werden kann.

3. Schritt: Gehen Sie risikoorientiert auf die Suche

Bei Ihrer Suche werden Sie vielleicht so manches an bislang unbekannten Bearbeitungen finden. Notieren Sie jeden Fund. Bewerten Sie dann jedoch, wo Ihre Beratung bzw. der Handlungsbedarf für das Unternehmen am dringendsten ist, und schätzen Sie das Risiko fehlender Beratung ein. Orientieren Sie sich hier an folgenden Fragen:

- **Hat die Bearbeitung Aussenwirkung?**
Gemeint sind hier alle Datenbearbeitungen, die nach draussen gerichtet und die für andere sichtbar sind. So z. B. ein Onlineshop oder ein auf künstlicher Intelligenz (KI) basierter Chatbot. Der Aussenbezug an sich sorgt schon allein für ein erhöhtes Risiko. Da wären nicht nur die Betroffenen, Medien und die Datenschutzaufsicht. Denken Sie vor allem auch an Cyberkriminelle, die hier einen Angriffspunkt für ihre Machenschaften haben.

- **Birgt die Bearbeitung besondere oder höhere Risiken?**
Das kann der Fall sein, wenn etwa Profile gebildet oder besonders schützenswerte Personendaten (Art. 5 Buchst. c Bundesgesetz über den Datenschutz (DSG)) bearbeitet werden. Kommt es hier zu einer Verletzung des Schutzes, muss Ihr Unternehmen bei entsprechendem Risiko für die Betroffenen den EDÖB (Art. 24 Abs. 1 DSG) und ggf. auch die Betroffenen (Art. 24 Abs. 4 DSG) informieren.

CHECKLISTE: Typische Fundorte für Defizite bei Schutzmassnahmen

Schwerpunkt	Erläuterung	Geprüft?
Internet, Online	Prüfen Sie die Webseite oder den Onlineshop Ihres Unternehmens. Gerade Webseiten sind schnell neu erstellt und ggf. wissen Sie nichts davon. Schauen Sie auf typische Schwachstellen. So z. B., ob eine aktuelle Verschlüsselung zum Einsatz kommt, Passwörter nicht im Klartext gespeichert werden und die eingesetzte Software auf aktuellem Stand ist. Hinterfragen Sie auch, wie man mit Zahlungsinformationen beim Onlineshop umgeht.	☐ Ja ☐ Nein
Apps	Auch hier sind angemessene Schutzmassnahmen unerlässlich. Schauen Sie, wie man das bei Apps sicherstellt. Oft ist hier entscheidend, dass Sie die Probe aufs Exempel machen, um Unzulänglichkeiten zu entdecken.	☐ Ja ☐ Nein
KI	Werden in diesem Zusammenhang auch Personendaten bearbeitet, muss das volle Programm der DSGVO eingehalten werden. Auch die Schutzmassnahmen müssen passen.	☐ Ja ☐ Nein
Marketing	Werbemassnahmen können Datenschutzrisiken bergen: Prüfen Sie beispielsweise den E-Mail-Newsletter Ihres Unternehmens, und zwar von der Registrierung bis zur Abbestellung. Auch bei genutzter Software oder eingesetzten Dienstleistern muss die Sicherheit gewährleistet sein.	☐ Ja ☐ Nein
IT	Gern wird hier auf neue Technologien oder günstigere Anbieter bzw. Dienstleister gesetzt. Doch dabei darf die Sicherheit der Bearbeitung nicht auf der Strecke bleiben.	☐ Ja ☐ Nein
Personal	Hier wird viel mit Personendaten gearbeitet und oft geht man dabei neue Wege. Denken Sie etwa an das Bewerber- und Personalmanagement, bei dem zunehmend auf moderne Systemlösungen und KI gesetzt wird.	☐ Ja ☐ Nein

Wie ist diese Panne in der Poststelle einzuschätzen?

FRAGE: Bei unserer Poststelle kam es zu einem Missgeschick mit Tragweite. So liess sich ein Mitarbeiter einen Arztbrief an seine Firmenanschrift schicken. Dieser Brief war auch entsprechend mit „persönlich/vertraulich" gekennzeichnet. Allerdings wurde das von einem Mitarbeiter der Poststelle übersehen. Er öffnete den Brief und versah ihn mit einem Eingangsstempel. Erst jetzt bemerkte er das Malheur. Er brachte den Brief persönlich zum Empfänger und schilderte die Sache. Doch der Mitarbeiter hatte null Verständnis. Im Gegenteil: Er meldete sich bei mir und beschwerte sich über die aus seiner Sicht schwerwiegende Datenpanne. Ich solle mich darum kümmern, dass das nicht nochmals passiert. Ausserdem erwartet er, dass die Sache der Aufsichtsbehörde gemeldet wird. Auch der betreffende Mitarbeiter der Poststelle meldete sich bei mir. Er versicherte mir, dass er vom Brief nicht wirklich etwas zur Kenntnis genommen habe. Direkt als er sein Missgeschick bemerkte, packte er den Brief in den Umschlag und brachte ihn zum Empfänger. Was meinen Sie: Wie ist die Sache einzuschätzen?

ANTWORT: Zunächst einmal sollten Sie als Datenschutzberater die Angelegenheit sachlich und nüchtern betrachten. Denn im Ergebnis dürfte alles nur halb so schlimm sein. Und gemeldet werden muss wohl auch nichts. Relevant ist nämlich Folgendes:

- Machen Sie sich klar: Zwar ist es unschön, dass die Sache passiert ist. Allerdings ist es auch hier wie so oft: Wo Menschen arbeiten, da können Fehler passieren. Dabei muss keine böse Absicht im Spiel sein. Vieles passiert im Eifer des Gefechts oder einfach aus Unachtsamkeit.
- Es gibt zunächst wohl kaum Gründe, daran zu zweifeln, dass der Mitarbeiter der Poststelle tatsächlich den Brief aus Versehen öffnete und, nachdem er seinen Fehler bemerkte, ihn sofort wieder in den Umschlag packte.
- Dass es durch das Öffnen des Briefes tatsächlich zu einer merklichen Beeinträchtigung des Persönlichkeitsrechts bzw. des Rechts auf Schutz sensibler Informationen gekommen ist, ist eher unwahrscheinlich. Zumal wenn der Mitarbeiter nur kurz auf das Anschriftenfeld schaute und seinen Fehler bemerkte. Ausserdem gab es wohl nur für eine einzelne Person die Möglichkeit der Kenntnisnahme. Insofern ist die Tragweite selbst dann gering, wenn der betreffende Mitarbeiter auf der ersten Seite des Briefes mehr zur Kenntnis genommen hätte.
- Zwar ist die Panne an sich als Datenschutzverstoss zu sehen, weil durch Unachtsamkeit ggf. sensible Personendaten zur Kenntnis genommen wurden. Allerdings besteht für Ihr Unternehmen keine Pflicht, diese Datenpanne nach Art. 24 Bundesgesetz über den Datenschutz zu melden, da kein Risiko für die Rechte und Freiheiten des Betroffenen, hier des Empfängers des Briefs, zu erwarten ist. So hatte nur eine Person für einen kurzen Moment die Möglichkeit zur Kenntnisnahme. Diese Person hat die Persönlichkeitsverletzung auch nicht dadurch verstärkt, dass sie den vollen Inhalt zur Kenntnis genommen bzw. eine Kopie angefertigt oder anderen Personen von dem Inhalt berichtet hat.

So reagieren Sie auf die Beschwerde

Sprechen Sie mit den Kollegen von der Poststelle und machen Sie klar, dass es in Zukunft nicht mehr zu einem solchen Patzer kommen sollte. Fehler können passieren, allerdings sollten sie sich nicht wiederholen. Reden Sie auch mit dem betroffenen Mitarbeiter und erläutern Sie die relevanten Aspekte. Bitten Sie um Verständnis, dass auch mal etwas schiefgehen kann. Sein Persönlichkeitsrecht wurde allenfalls nur minimal beeinträchtigt. Geben Sie zudem folgende Empfehlung: Sensible private Post lässt man sich besser nicht an den Arbeitsplatz schicken.

Kann ein veralteter Eintrag im Verzeichnis gelöscht werden?

FRAGE: Bei uns führen wir das Verzeichnis von Bearbeitungstätigkeiten nach Art. 12 Bundesgesetz über den Datenschutz elektronisch als Tabelle. Ich habe die Eintragungen durchgesehen. Dabei habe ich Bearbeitungstätigkeiten entdeckt, die es so nicht mehr gibt. Ich frage mich nun: Kann ein solcher Eintrag gelöscht werden, um das Verzeichnis wieder übersichtlicher zu machen?

ANTWORT: Mit dem Löschen sollten Sie vorsichtig sein. Unter Umständen hat ein solcher Eintrag noch seine Berechtigung, auch wenn die Bearbeitungstätigkeit so nicht mehr existiert. So kann ein Eintrag noch wichtig sein, wenn Daten zwar nicht mehr aktiv bearbeitet werden, jedoch etwa aufgrund von Aufbewahrungspflichten weiter vorgehalten werden müssen. Auch muss Ihr Unternehmen ggf. gegenüber dem EDÖB auskunftsfähig sein. Verstösse können nämlich meist bis zu drei Jahre verfolgt werden. Insofern kann ein Eintrag für eine frühere Bearbeitungstätigkeit von grosser Bedeutung sein. Um die Übersichtlichkeit zu erhöhen, können Sie verschiedene Massnahmen ergreifen. Sie können die entsprechenden Bearbeitungstätigkeiten in eine Tabelle mit beendeten Bearbeitungen auslagern. Wollen Sie das nicht, können Sie bei gängigen Tabellenprogrammen die entsprechenden Bereiche ausblenden. Alternativ können Sie die Einträge auch einfach durchstreichen. Idealerweise vermerken Sie auch das Ende der Bearbeitungstätigkeit.

OLG Köln: Meta darf KI mit öffentlichen Daten trainieren

Damit künstliche Intelligenz (KI) gute Ergebnisse liefert, bedarf es eines gut trainierten Sprachmodells, des Large-Language-Models. Meta, als Betreiber von Facebook und Instagram, will sein Sprachmodell mit öffentlichen Inhalten der Mitglieder trainieren. Geht das? Das Oberlandesgericht (OLG) Köln in Deutschland sagt Ja (Urteil vom 23.5.2025, Az. 15 UKI 2/25).

Das ging dem Verfahren voraus

Meta will den Nutzern seiner sozialen Netzwerke KI-Services anbieten, etwa zum Beantworten von Fragen oder zum Formulieren von Inhalten. Das Sprachmodell soll auch regionale Gepflogenheiten berücksichtigen. Daher will Meta die bei den sozialen Netzwerken von Nutzern öffentlich eingestellten Inhalte verwenden, um sein Sprachmodell zu trainieren. Umfasst sind damit z. B. Profilbilder, Aktivitäten auf Facebook-Seiten, öffentliche Kommentare oder Bewertungen sowie Fotos und Videos.

Zunächst informierte Meta im März 2024 die zuständige irische Datenschutzaufsichtsbehörde (DPC) über das Vorhaben und im Sommer 2024 die Nutzer. Nach Bedenken der DPC und einer Abmahnung durch deutsche Verbraucherschützer wurde das Vorhaben auf Eis gelegt und überarbeitet. Es wurden unter anderem Hinweise des Europäischen Datenschutzausschusses berücksichtigt. Meta wurde erneut bei der DPC vorstellig. Von der Behörde gab es weitere Empfehlungen, die von Meta umgesetzt wurden, z. B. ein Widerspruchsrecht für Nutzer sowie die Deidentifizierung der Daten.

Zum 27.5.2025 beabsichtigte Meta, mit der Verwendung der öffentlichen Daten für das Training des Sprachmodells zu beginnen. Hierüber informierte Meta die Öffentlichkeit am 14.4.2025. Nutzern wurde das Recht eingeräumt, der Nutzung ihrer öffentlichen Daten für das KI-Training zu widersprechen.

Verbraucherschützer ziehen vor Gericht

Am 30.4.2025 mahnten deutsche Verbraucherschützer Meta wegen des Vorhabens ab. Aus deren Sicht ist die Verwendung der öffentlichen Daten der Nutzer für das Training des Sprachmodells datenschutzrechtlich unzulässig. Insbesondere lasse sich das nicht auf ein überwiegendes berechtigtes Interesse (Art. 6 Abs. 1 Satz 1 Buchst. f Datenschutz-Grundverordnung (DSGVO)) stützen. Auch liege ein weiterer Verstoss vor, und zwar gegen Art. 5 Abs. 2 des Gesetzes über digitale Märkte, kurz GdM (englisch Digital Markets Act (DMA)). Weil Meta sein Vorgehen für zulässig hält, akzeptierte man die Abmahnung nicht. Also klagten die Verbraucherschützer vor dem OLG und forderten die Untersagung der Datenbearbeitung. Das OLG verhandelte die Sache im Eilverfahren. Bei der im Eilverfahren stattfindenden summarischen Prüfung, also einer nicht in die Tiefe gehenden Bewertung, urteilte das Gericht zugunsten von Meta.

So entschied das Gericht

Zunächst stellen die Richter fest: Es ist nicht von einem Verstoss gegen Art. 5 Abs. 2 GdM auszugehen. Es findet keine Zusammenführung von Daten im Rechtssinne statt. Das Einbringen von teilweise deidentifizierten bzw. zerlegten Daten aus zwei Plattformen in ein Training ist kein Zusammenführen. Es fehlt an der gezielten Verbindung von Daten derselben Person.

Kein Datenschutzverstoss ersichtlich

Ein Verstoss gegen die Rechtmässigkeit (Art. 5 Abs. 1 Buchst. a DSGVO) ist nicht zu erkennen. Die Verarbeitung kann Meta auf Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO stützen. Sie ist zur Wahrung berechtigter Interessen von Meta erforderlich. Diese Interessen überwiegen die Interessen der betroffenen Personen.

Das Interesse, eine von Meta entwickelte KI mit von Nutzern veröffentlichten Daten zu trainieren, ist als berechtigt anzuerkennen. Auch ist die Verarbeitung der Daten als erforderlich anzusehen. Die Verarbeitung ist zur Erreichung des Interesses geeignet und es gibt keine weniger in die Privatsphäre eingreifenden Möglichkeiten, um den Zweck zu erreichen. Gerade ein Datensammeln durch Web-Scraping wäre mit erheblicheren Eingriffen für die Betroffenen verbunden, etwa weil hier die von Meta umgesetzten Deidentifizierungs- und Abschwächungsmassnahmen nicht greifen würden.

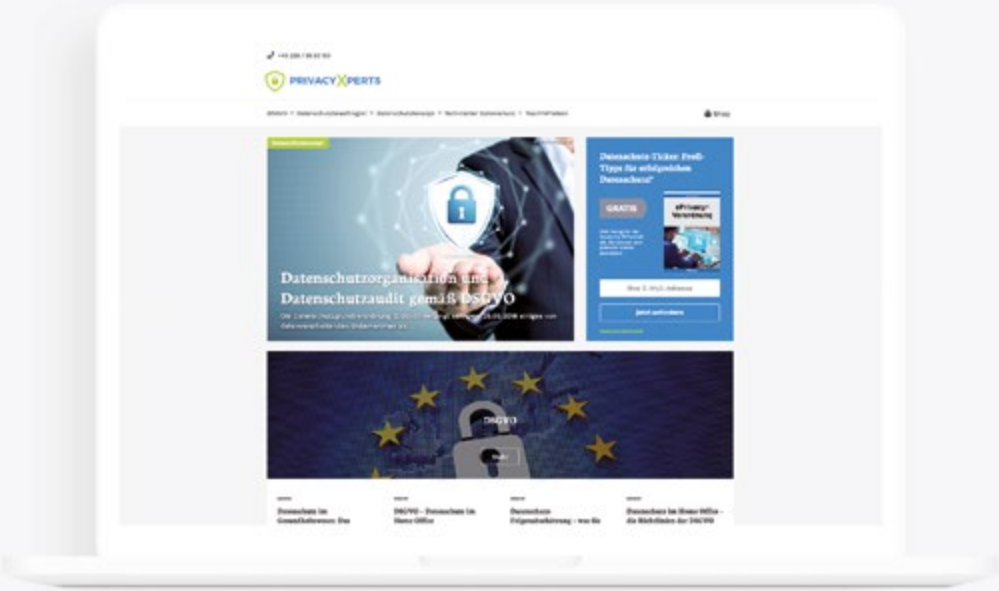
Interessen der Betroffenen überwiegen nicht

Aus Sicht des Gerichts mussten Betroffene bei der Erhebung der Daten vernünftigerweise mit einer entsprechenden Verarbeitung rechnen. Die Verarbeitung der Daten ist auf von Nutzern öffentlich gemachte Daten beschränkt. Zudem wurden seitens Meta Massnahmen umgesetzt, um den Eingriff in die Rechte der Betroffenen abzuschwächen. So werden im Rahmen der Deidentifizierung etwa Namen, Kontaktdaten, Kennungen und Kennzeichen entfernt und die Daten in unstrukturierter Form zusammengestellt.

Auch hat Meta geeignete Massnahmen ergriffen, um einen unbefugten Zugriff auf die Trainingsdaten auszuschliessen. Daneben haben Nutzer eine weitgehende Steuerungsmöglichkeit. Sie können Beiträgen den öffentlichen Status entziehen oder der Verarbeitung für Trainingszwecke widersprechen. Die Frist von sechs Wochen war angemessen.

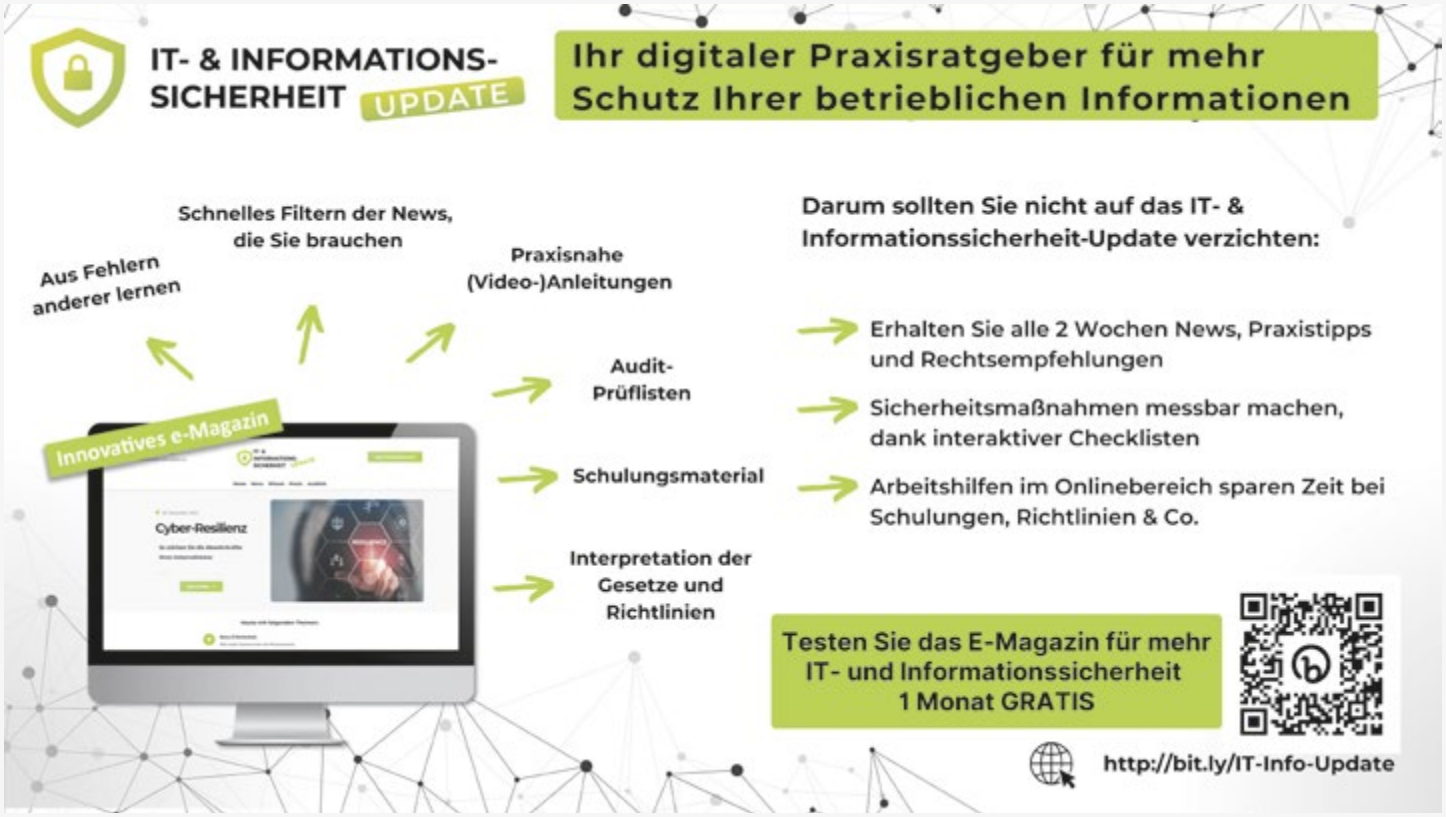
Diese Entscheidung liefert Ihnen Argumente
Erinnern Sie sich an die Entscheidung, wenn es um die Nutzung von Daten für KI-Trainingszwecke geht. Eine Einwilligung muss nicht immer sein. Bei Umsetzung entsprechender Massnahmen kann eine Bearbeitung auch auf das überwiegende berechtigte Interesse Ihres Unternehmens gestützt 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



Vorschau:

Das sind Ihre Möglichkeiten, wenn Mitarbeiter aus der Reihe tanzen
Immer gut vorbereitet sein: Checken Sie die Notfallpläne Ihres Unternehmens

PRIVACYXPERTS

Telefon: +49 2 28 95 50 150
Fax: +49 2 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
Deutschland