DATENSCHUTZAKTUELL Professional
AUG I 2025
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH

VERARBEITUNG SENSIBLER DATEN: DARAUF KOMMT ES AN

AWARENESS
Neues Bundeslagebild Cybercrime: Sensibilisieren Sie mit dem BKA-Bericht 1–2

DATENSCHUTZ ORGANISIEREN
Organisatorische Maßnahmen: Ist das in Ihrem Unternehmen umgesetzt? 3

Bleiben Sie nie sprachlos

Liebe Leserin, lieber Leser,

haben Sie das bereits erlebt? Sie sind in einer Besprechung und man haut Ihnen manche unpassende Aussage um die Ohren. Das mögliche Ziel: Man will den Datenschutz schlechtmachen und Sie diskreditieren. Auch wenn Sie erst einmal baff sind, dürfen Sie in einer solchen Situation nie sprachlos bleiben.

Am besten ist: Gewinnen Sie etwas Zeit zum Überlegen. Fragen Sie nach, wie das konkret gemeint ist und woran man das festmacht. Und gehen Sie dann zum Gegenangriff über. Stellen Sie infrage, inwieweit das Gesagte überhaupt ernst zu nehmen ist. Schließlich ist Datenschutz ein Muss, ohne Wenn und Aber.

Viele Grüße

Andreas Würtz,
Rechtsanwalt und Chefredakteur

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

Awareness
Neues Bundeslagebild Cybercrime: Sensibilisieren Sie mit dem BKA-Bericht
Seiten 1–2

Datenschutz organisieren
Organisatorische Maßnahmen: Ist das in Ihrem Unternehmen umgesetzt?
Seite 3

Know-how
Verarbeitung sensibler Daten: Darauf kommt es an
Seiten 4–5

Besser arbeiten
Ineffizienz ade: So holen Sie mehr aus Besprechungen und Terminen heraus
Seite 6

Fragen an die Redaktion
? *Teilnehmerdaten für den Trainer: Liegt eine Auftragsverarbeitung vor?*
? *Smartphone gestohlen: Besteht hier ein großes Risiko?*
Seite 7

Rechtsprechung
OLG Köln: Meta darf KI mit öffentlichen Daten trainieren
Seite 8

Zum neuen Onlinebereich!
www.privacyxperts.de/login

Expertensprechstunde:
https://t1p.de/andreas-wuertz

Bildnachweise:
Titel: Adobe Stock | Leo Rohmann
Seite 1: Adobe Stock | Deborah

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, Am Hambuch 5, 53340 Meckenheim

Erscheinungsweise: 26-mal pro Jahr

E-Mail: kundendienst@privacyxperts.de

Internet: www.privacyxperts.de

(bei Rückfragen bitte Kundennummer angeben)

Alle Angaben wurden mit äußerster Sorgfalt ermittelt und überprüft. Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen. Eine Gewähr kann deshalb nicht übernommen werden.

Im Interesse der Lesbarkeit verzichten wir in unseren Beiträgen auf geschlechtsbezogene Formulierungen. Selbstverständlich sind immer alle Geschlechterformen gemeint, auch wenn explizit nur eines der Geschlechter angesprochen wird.

Dieses Produkt besteht aus FSC®-zertifiziertem Papier.

© 2025 by VNR Verlag für die Deutsche Wirtschaft AG, Bonn, Berlin, Bukarest, Jacksonville, Manchester, Passau, Warschau

Rücken Sie den Cybercrime mal wieder in den Mittelpunkt.

Neues Bundeslagebild Cybercrime: Sensibilisieren Sie mit dem BKA-Bericht

Eines ist sicher: Auch Ihr Unternehmen dürfte auf einem Schatz sitzen. Die Rede ist von den Daten des Unternehmens. Egal ob personenbezogen oder nicht, Daten haben einen enormen Wert. Sie sind oftmals unersetzliche Grundlage der Geschäftstätigkeit. Doch leider wissen das auch Cyberkriminelle. Umso wichtiger ist, dass Sie regelmäßig die Hand heben und auf Risiken aufmerksam machen.

Nutzen Sie den Bericht geschickt

Manchmal ist es wie verhext. Sie reden sich den Mund fusselig, doch in Ihrem Unternehmen und gerade bei der Unternehmensleitung will niemand so recht die von Cyberkriminellen ausgehenden Risiken sehen. Da kann es hilfreich sein, wenn Sie geschickt sensibilisieren und hier auf offizielle Zahlen setzen. Diese Zahlen lesen Sie beispielsweise im aktuellen Bericht des Bundeskriminalamts (BKA) „Bundeslagebild Cybercrime". Die Veröffentlichung finden Sie auf der Webseite der Behörde unter https://t1p.de/t1p9k.

Diese Erkenntnisse sind für Unternehmen und für Sie als Datenschutzbeauftragter von besonderer Bedeutung:

- **Cybercrime nimmt weiter zu:** Auch 2024 ist die Zahl der Fälle in Deutschland weiter gestiegen. Es gab über 131.000 Fälle an im Inland begangenen Straftaten. Aus dem Ausland liegt die Fallzahl mit knapp 202.000 erheblich höher. Letztere lassen sich meist nur schwer aufklären. Im Übrigen dürfte die Dunkelziffer der Straftaten im Bereich Cybercrime erheblich mehr betragen. Schließlich werden wohl viele Straftaten nicht erkannt oder angezeigt.

- **Schaden steigt:** Der durch Cybercrime verursachte Schaden lag 2024 bei rund 180 Mrd. €. Damit liegt der Schaden 30 Mrd. € über dem Betrag von 2023.

- **Cyberkriminelle werden professioneller:** Künstliche Intelligenz (KI) wird zunehmend auch von Cyberkriminellen genutzt, etwa für bessere Phishing-Aktivitäten oder für die Entwicklung von Malware.

- **Kritische Branchen stehen im Fokus:** Cyberkriminelle greifen kritische Branchen gezielt an, etwa im Bereich Gesundheit, Energie, Verwaltung und Verkehr.

- **Ransomware steht bei Cyberkriminellen hoch im Kurs:** Im Berichtszeitraum gab es 950 angezeigte Vorfälle, bei denen Daten durch Kriminelle verschlüsselt und Lösegeld erpresst wurde. Dabei richteten sich rund 80 % der Angriffe gegen kleine und mittlere Unternehmen.

- **Schwachstellen und Phishing machen Angriffe möglich:** Schwachstellen in Systemen und Software werden von Cyberkriminellen gezielt ausgenutzt, zunehmend auch unter KI-Einsatz. Phishing fungiert meist als Türöffner für weitere Aktivitäten der Cyberkriminellen. Häufig werden dazu falsche Nachrichten von Banken oder Versanddienstleistern genutzt, um die Empfänger zur Preisgabe sensibler Informationen zu bewegen.

Darum ist Ihr Aktivwerden so wichtig

Dass Cybercrime auch großes Risikopotenzial für Ihr Unternehmen hat, dürfte Sie als Datenschutzprofi nicht überraschen. Schließlich versuchen Cyberkriminelle, mittels Phishing-E-Mails oder unter Ausnutzung von Sicherheitslücken sich alles an Daten unter den Nagel zu reißen und im Anschluss zu Geld zu machen. Haben Cyberkrimielle mit einem Angriff Erfolg, hat

Ihr Unternehmen meist zugleich mehrere größere Probleme. So beispielsweise:

- Kommen Daten abhanden oder werden sie zwecks Lösegelderpressung verschlüsselt, kann Ihr Unternehmen ggf. nicht mehr weiterarbeiten. Das kann daran liegen, dass die entsprechenden Systeme oder Daten nicht mehr verfügbar sind. Oder eben daran, dass Ihr Unternehmen mit Schadensbegrenzung beschäftigt ist. Ist die Produktion betroffen, kann diese zum Erliegen kommen. Das führt nicht nur zu Lieferschwierigkeiten. Kann nicht geliefert werden, können Strafzahlungen an den Vertragspartner fällig werden.

- Jeder unbefugte Zugriff auf Daten oder jeder unrechtmäßige Datenabfluss führt zu einer Datenpanne. Da spielt es keine Rolle, ob Ihr Unternehmen hierfür etwas kann oder nicht. Auf jeden Fall kann gerade bei höheren Risiken die Pflicht bestehen, den Vorfall der zuständigen Datenschutzaufsichtsbehörde zu melden.

- Der Schaden ist garantiert immens: So können Kunden ausbleiben, wenn sich herumspricht, dass Ihr Unternehmen Probleme mit dem Datenschutz hat. Das ist so gut wie sicher, wenn etwa Kundendaten veröffentlicht oder im Darknet zum Verkauf angeboten und anschließend missbraucht werden. Auch ist es meist ziemlich teuer, Systeme zu säubern oder neu aufzusetzen. Gerade wenn es hierfür Spezialisten braucht, geht das richtig ins Geld. Außerdem: Bei einem Datenschutzverstoß, etwa weil keine angemessenen technischen oder organisatorischen Schutzmaßnahmen gegen Cyberkriminelle getroffen wurden (Art. 32 Datenschutz-Grundverordnung (DSGVO)), kann es zu einem hohen Bußgeld kommen. Und das lässt sich meist nicht aus der Portokasse bezahlen.

Sensibilisieren ist Ihr Ding

Was zu Ihren Aufgaben als Datenschutzbeauftragter zählt, ergibt sich aus Art. 39 Abs. 1 DSGVO. So erwähnt Art. 39 Abs. 1 Buchst. a DSGVO das Unterrichten und Beraten im Hinblick auf die Pflichten, die sich für Unternehmen und Beschäftigte aus der DSGVO ergeben. Dabei meint Unterrichten nicht „Lehren". Was gemeint ist, wird in der englischen Fassung der DSGVO deutlich. Das dort zu findende „inform" zeigt, dass das Informieren gemeint ist. Das bedeutet also auch, dass Sie sensibilisieren und aufmerksam machen, und zwar für Pflichten und Risiken im Zusammenhang mit der Verarbeitung personenbezogener Daten.

Setzen Sie auf eine kurze Information des Managements

Natürlich können Sie aus dem BKA-Bericht eine lange Abhandlung erstellen. Informationen und Zahlen gibt es zuhauf. Doch wichtiger ist meist, dass Sie dafür sorgen, das Thema Cybercrime einmal wieder in den Mittelpunkt zu rücken. Das geht beispielsweise auch mit einer kurzen E-Mail an das obere Management. Orientieren Sie sich doch einfach an dem folgenden Entwurf:

BEISPIEL: Information zum Cybercrime

Sehr geehrte Kolleginnen und Kollegen,

vor Kurzem hat das Bundeskriminalamt (BKA) in seinem Bericht „Bundeslagebild Cybercrime 2024" seine Ergebnisse rund um die Aktivitäten von Cyberkriminellen veröffentlicht. Die Entwicklung und die Zahlen sind alarmierend. Und sie sind auch für unser Unternehmen höchst relevant.

Cybercrime ist kein Randthema mehr

2024 gab es in Deutschland 201.877 Cybercrime-Fälle, die von außerhalb Deutschlands gestartet wurden – ein neuer Höchststand. Die Zahl der Inlandsfälle lag bei 131.391. Doch klar ist auch: Das sind nur die bekannten Fälle. Die Dunkelziffer dürfte noch weit höher liegen. Vielleicht ist es nur die Spitze des Eisbergs.

Die finanziellen Schäden sind enorm

Das BKA zitiert den Branchenverband Bitkom e. V. und dessen Schätzung. So entstand 2024 durch Cyberangriffe ein Schaden von 178,6 Mrd. € – also 30,4 Mrd. € mehr als im Vorjahr. Ransomware-Angriffe, bei denen Daten verschlüsselt und Unternehmen erpresst werden, bleiben die zentrale Bedrohung. 950 solcher Angriffe wurden angezeigt, wobei in 80 % der Fälle kleine und mittlere Unternehmen Opfer wurden. Meist wird versucht, mehrfach zu kassieren, etwa einmal für das Entschlüsseln der gestohlenen Daten und noch mal für das Nichtveröffentlichen. Die Lösegeldzahlung betrug im Durchschnitt rund 240.000 €.

Cyberkriminelle agieren immer professioneller

Beim Phishing und Ausnutzen von IT-Schwachstellen gehen Cyberkriminelle immer professioneller vor. Auch der Einsatz künstlicher Intelligenz macht Angriffe raffinierter und schwerer abzuwehren. Gerade Phishing-E-Mails oder Phishing-Nachrichten werden immer ausgefeilter. Fehler und Unstimmigkeiten sind nicht mehr so leicht zu entdecken. Also gilt noch mehr: Holzauge sei wachsam! Lassen Sie sich und Ihre Mitarbeiter kein X für ein U vormachen.

Was bedeutet das für uns?

Die neuen Zahlen des BKA bestätigen: Kein Unternehmen ist zu klein oder zu unbedeutend, um nicht Ziel und ggf. auch Opfer zu werden. Deshalb ist es wichtig, dass wir gemeinsam alles daransetzen, Cyberkriminellen das Leben schwer zu machen und unser Unternehmen vor Schaden zu bewahren.

Ihr Beitrag zählt

Als Führungskraft können Sie viel dazu beisteuern, dass unser Unternehmen nicht zum Opfer von Cyberkriminellen wird. Setzen Sie immer auf risikoangemessene Schutzmaßnahmen, fördern Sie die Sensibilität Ihrer Mitarbeiter. Stellen Sie sicher, dass unser Unternehmen auf aktuelle Bedrohungen vorbereitet ist und neue Gefahren frühzeitig erkannt werden. Denn Cybercrime ist eine reale Gefahr – und wir alle sind gefordert, aktiv gegenzusteuern.

Sie wollen mehr zum aktuellen Lagebild des BKA erfahren? Den Bericht finden Sie hier: https://t1p.de/t1p9k. Übrigens: Bei Fragen zum Schutz von (personenbezogenen) Daten können Sie mich jederzeit ansprechen. Ich stehe Ihnen gerne mit Rat und Tat zur Seite.

Ihr Datenschutzbeauftragter

Organisatorische Maßnahmen: Ist das in Ihrem Unternehmen umgesetzt?

Verarbeitet Ihr Unternehmen personenbezogene Daten, ist eines ganz klar: Es muss sich an die Datenschutzvorschriften halten, beispielsweise die Datenschutz-Grundverordnung (DSGVO). Doch damit es mit dem Umsetzen klappt, sind beispielsweise auch organisatorische Maßnahmen nötig. Bei denen können Sie einmal etwas genauer hinschauen.

Organisatorische Maßnahmen sind unerlässlich

Wenn Sie von organisatorischen Maßnahmen lesen, denken Sie vielleicht gleich an Art. 32 DSGVO. Dieser Artikel macht zur Vorgabe, dass durch risikoangemessene technische und organisatorische Maßnahmen ein angemessenes Sicherheitsniveau für die verarbeiteten personenbezogenen Daten geschaffen werden muss. Doch Art. 32 DSGVO ist nicht gemeint. Die organisatorischen Maßnahmen sind viel grundlegendere Voraussetzungen, damit der Datenschutz funktioniert. Und sie stehen auch in Art. 24 DSGVO. So sieht Art. 24 Abs. 1 Satz 1 DSGVO vor, dass Ihr Unternehmen als Verantwortlicher geeignete technische und organisatorische Maßnahmen umsetzen muss. Mit diesen soll es sicherstellen und den Nachweis erbringen können, dass eine Verarbeitung im Einklang mit der DSGVO erfolgt.

Machen Sie den Check

Die folgende Checkliste enthält viele organisatorische Maßnahmen, mit denen Ihr Unternehmen und Sie sicherstellen können, dass es mit dem Datenschutz rundläuft.

CHECKLISTE: Organisatorische Maßnahmen zur Umsetzung des Datenschutzes

Organisatorische Maßnahme	Hintergrund	Umgesetzt?
Etablierung eines Datenschutz-Management-Systems	Hierbei handelt es sich um ein ganzheitliches Konzept zur Planung, Umsetzung, Kontrolle und Verbesserung aller zum Datenschutz erforderlichen Maßnahmen. Damit soll insbesondere dauerhaft, nachhaltig und wirksam die Umsetzung des Datenschutzes in allen Bereichen und auf allen Ebenen sichergestellt werden. Umfasst sind meist grundsätzliche Festlegungen, das Management von Risiken, die Umsetzung nötiger Maßnahmen, Kontrollmaßnahmen und Aktivitäten zur kontinuierlichen Verbesserung im Rahmen des Plan-Do-Check-Act-Prinzips.	☐ Ja ☐ Nein
Risikomanagement im Datenschutz	Es gibt zahlreiche Risiken mit Bezug zum Datenschutz bzw. im Hinblick auf Betroffene und deren Daten. Auch bezüglich der Umsetzung der gesetzlichen Anforderungen können Risiken bestehen. Risiken müssen identifiziert, bewertet und mit geeigneten Maßnahmen behandelt werden. Hohe Risiken sind in der Regel nicht akzeptabel und müssen reduziert werden.	☐ Ja ☐ Nein
Richtlinien, Anweisungen, Vorschriften und Regelungen	Damit klar ist, wie mit personenbezogenen Daten umzugehen ist, muss es klare Regeln und Anweisungen geben. Auch gut gestaltete Prozesse sind für einen funktionierenden Datenschutz von großer Bedeutung.	☐ Ja ☐ Nein
Verpflichtung der Beschäftigten	Den Beschäftigten sollte die ihnen zukommende Verantwortung für den Datenschutz verdeutlicht werden. Das kann grundlegend im Arbeitsvertrag passieren. Meist ist eine ergänzende schriftliche Verpflichtungserklärung sinnvoll. Damit lässt sich die Verantwortung für den Datenschutz greifbarer und umfassender darstellen.	☐ Ja ☐ Nein
Awareness und Trainings	Den Beschäftigten Know-how zu vermitteln ist unerlässlich. Hier braucht es nicht nur ein gutes Konzept, damit alle bedarfsgerecht mit Wissen versorgt werden. Auch die Inhalte müssen passen und aktuell sein.	☐ Ja ☐ Nein
Klare Zuweisung von Verantwortlichkeiten und Zuständigkeiten	Es darf keine Zweifel geben, wer im Datenschutz wofür verantwortlich ist. Das ist auch unerlässlich, wenn es um konkrete Verarbeitungen geht. Nur mit Verantwortung entsteht auch ein gewisser Handlungsdruck.	☐ Ja ☐ Nein
Audits und Kontrollen	Ob Gesetze und interne Regeln eingehalten werden, kann auf verschiedene Weise kontrolliert werden. Neben Selbstchecks in den einzelnen Abteilungen können Prüfungen durch die Revision oder durch Sie als Datenschutzbeauftragten erfolgen.	☐ Ja ☐ Nein
Vertrags- und Dienstleistungsmanagement	Einerseits sorgt dies für den nötigen Überblick. Andererseits wird so deutlich, worauf geachtet werden muss, wo spezifische Risiken bestehen, welche Maßnahmen nötig sind und wo Handlungs- oder Kontrollbedarf besteht.	☐ Ja ☐ Nein
Beobachtung relevanter Entwicklungen	Das ist auf verschiedenen Ebenen nötig. So kann eine sich verändernde Geschäftstätigkeit andere Verarbeitungen mit sich bringen, die zu anderen Herausforderungen bzw. Risiken im Datenschutz führen. Auch können Veränderungen bei der Rechtslage, bei technischen Entwicklungen oder bei der praktischen Umsetzung von Verarbeitungen Handlungsbedarf auslösen.	☐ Ja ☐ Nein

Verarbeitung sensibler Daten: Darauf kommt es an

In jedem Unternehmen wird hier und da mit sensiblen personenbezogenen Daten gearbeitet, sprich mit Daten im Sinne von Art. 9 Abs. 1 Datenschutz-Grundverordnung (DSGVO). Denken Sie beispielsweise an Gesundheitsdaten in der Personalabteilung. Dass bei Sensiblem besonderer Schutz nötig ist, liegt auf der Hand. Doch es gilt, noch einige weitere Aspekte zu beachten.

Daten sind schneller als sensibel einzuordnen, als viele denken

Sprechen Sie mit Kollegen, ob man mit sensiblen personenbezogenen Daten arbeitet, werden Sie häufig ziemlich schnell hören, dass dem nicht so sei. Und Sie ahnen es: Oft wird man mit dieser Einschätzung danebenliegen. Der Grund: Häufig ist nicht so wirklich bekannt, was mit sensiblen Daten, sprich den besonderen Kategorien personenbezogener Daten, gemeint ist. Schauen Sie mit den Kollegen ins Gesetz, wird deutlich, was alles umfasst ist. Und zwar sind das

- personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen,
- genetische Daten,
- biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,
- Gesundheitsdaten oder
- Daten zum Sexualleben oder zur sexuellen Orientierung einer natürlichen Person.

Und hier steckt oftmals der Teufel im Detail. So kann der Name im Zusammenhang mit der Mitgliedschaft in einem Verein für Betroffene einer Krankheit selbst zum personenbezogenen Datum im Sinne von Art. 9 Abs. 1 DSGVO werden. Auch die biometrische Zutrittskontrolle im Unternehmen muss an den besonderen Vorgaben gemessen werden, weil etwa der Fingerabdruck zur eindeutigen Identifizierung genutzt werden soll.

Sprechen Sie „einfach“
Juristisch sauber müssten Sie immer von „besonderen Kategorien personenbezogener Daten“ sprechen. Das ist aber ziemlich sperrig und für „Nicht-Datenschützer“ kaum im Gedächtnis zu behalten. Daher: Setzen Sie auf eine einfache Sprache. „Sensible personenbezogene Daten“ verdeutlicht sprachlich viel einfacher, worum es geht. Erklären Sie aber bei Bedarf, dass es sich um Daten im Sinne von Art. 9 Abs. 1 DSGVO handelt.

Verbot mit Erlaubnisvorbehalt

Einfach sensible personenbezogene Daten verarbeiten ist nicht drin. Das liegt am Verbot mit Erlaubnisvorbehalt. Nach Art. 9 Abs. 1 DSGVO ist das Verarbeiten solcher Daten grundsätzlich verboten. Es ist aber erlaubt, wenn beispielsweise nach Art. 9 Abs. 2 DSGVO ein Ausnahmetatbestand erfüllt ist. Das kann etwa die Einwilligung des Betroffenen sein. Außerdem ist wichtig: Ausnahmetatbestände kann es auch in anderen Gesetzen geben. Unter Datenschutzaspekten besonders relevant sind die Festlegungen des § 22 Bundesdatenschutzgesetz (BDSG). Danach gibt es hier in Deutschland spezifische für öffentliche und nicht öffentliche Stellen (z. B. Unternehmen, Vereine) geltende Ausnahmen.

Auch bei Beschäftigten gelten besondere Rahmenbedingungen

Sollen etwa sensible Daten zu Beschäftigten verarbeitet werden, z. B. für eine biometrische Zutrittskontrolle, ist es unerlässlich, dass Sie ein Auge auf die deutschen Festlegungen zum Beschäftigtendatenschutz haben. So finden Sie in § 26 Abs. 3 und 4 BDSG die Bedingungen, unter denen eine Verarbeitung sensibler Daten von Beschäftigten zulässig sein kann. So kann sich die Erlaubnis z. B. auch aus einer Betriebsvereinbarung ergeben.

Betrachten Sie nicht nur die sensiblen Daten
Meist ist es nicht so, dass nur sensible Daten verarbeitet werden. Vielmehr geht es in erster Linie um „normale“ personenbezogene Daten. Für die „normalen“ Daten bedarf es ebenfalls einer Rechtsgrundlage, die sich z. B. aus Art. 6 Abs. 1 Satz 1 DSGVO ergeben kann. Im Hinblick auf die sensiblen Daten bedarf es dann ggf. eines weiteren Erlaubnistatbestands, etwa nach Art. 9 Abs. 2 DSGVO oder § 22 BDSG.

Besonderer Schutz ist unerlässlich

Sensible personenbezogene Daten sind schon allein deswegen besonders zu schützen, weil hier meist ein erheblich höheres Missbrauchs-, Rufschädigungs- oder Schadensrisiko für Betroffene besteht, wenn sie in falsche Hände geraten. Dies muss bei der Auswahl der technischen und organisatorischen Maßnahmen unbedingt berücksichtigt werden.

Zudem: Auch die spezifischen deutschen Regelungen dürfen Sie nicht übersehen. Stützt man eine Verarbeitung auf die Ausnahmetatbestände des § 22 Abs. 1 BDSG, müssen spezifischere Schutzmaßnahmen umgesetzt werden (§ 22 Abs. 2 BDSG). Neben den sich aus Art. 32 DSGVO ergebenden risikoangemessenen Schutzmaßnahmen muss beispielsweise eine Protokollierung vorgenommen werden. Auch sind die an der Verarbeitung Beteiligten zu sensibilisieren. Ferner müssen die gewählten Schutzmaßnahmen regelmäßig überprüft werden.

Übrigens: Auf die besonderen Vorgaben zum Schutz der sensiblen Daten verweist auch § 26 Abs. 3 Satz 3 BDSG. Insofern sind entsprechende Schutzmaßnahmen auch bei der Verarbeitung sensibler Daten im Beschäftigungsverhältnis vorzusehen. Zwar kann mit einer Betriebsvereinbarung die nötige Rechtsgrundlage geschaffen werden. Dadurch darf das Schutzniveau der DSGVO nicht unterschritten werden.

CHECKLISTE: Wichtige Aspekte bei der Verarbeitung sensibler Daten

Aspekt	Hintergrund	Geprüft und in Ordnung?
Welche personenbezogenen Daten sollen verarbeitet werden?	› Am besten lassen Sie sich alle Daten möglichst konkret nennen. Zu allgemeine Beschreibungen wie z. B. „Kundendaten" helfen hier meist nicht weiter. › Fordern Sie im Bedarfsfall eine Auflistung mit Beispielen.	☐ Ja ☐ Nein
Inwieweit handelt es sich um Daten im Sinne von Art. 9 Abs. 1 DSGVO?	› Bewerten Sie gemeinsam mit den Kollegen, inwieweit einzelne Daten als besondere Kategorien personenbezogener Daten einzustufen sind. › Prüfen Sie auch, ob in Zusammenhang stehende Daten dazu führen, dass zunächst unproblematische Daten(sätze) zu sensiblen Informationen werden.	☐ Ja ☐ Nein
In welcher Beziehung stehen die Betroffenen zum Verantwortlichen?	› Lassen Sie sich erläutern, in welcher Beziehung Ihr Unternehmen zum Betroffenen steht. › Hinterfragen Sie, inwieweit es sich bei den Betroffenen um Beschäftigte handelt. Dabei ist wichtig: Der Begriff des Beschäftigten ist weiter, als es zunächst erscheint. Prüfen Sie gemeinsam § 26 Abs. 8 BDSG.	☐ Ja ☐ Nein
Auf welche Rechtsgrundlage soll die Verarbeitung der personenbezogenen Daten an sich bzw. der sensiblen personenbezogenen Daten im Speziellen gestützt werden?	› Geht es um die Verarbeitung „normaler" persönlicher Informationen, sollte Ihr Blick in Richtung Art. 6 Abs. 1 Satz 1 DSGVO gehen. Bei sensiblen Daten muss eine Ausnahme vom Verarbeitungsverbot (Art. 9 Abs. 1 DSGVO) greifen, etwa nach Art. 9 Abs. 2 DSGVO bzw. § 22 Abs. 2 BDSG. › Bei sensiblen Beschäftigtendaten sollten Sie insbesondere ein Auge auf die Voraussetzungen des § 26 Abs. 3 und 4 BDSG haben.	☐ Ja ☐ Nein
Wie werden die Grundsätze der Verarbeitung personenbezogener Daten umgesetzt?	› Alle Grundsätze sind auch bei der Verarbeitung sensibler Daten von großer Bedeutung. Schauen Sie jedoch insbesondere auf die Aspekte Rechtmäßigkeit, Zweckbindung, Datenminimierung und Vertraulichkeit. › Klären Sie auch, wie man nachweist, dass die Grundsätze eingehalten und umgesetzt sind. Diese Rechenschaftspflicht ergibt sich aus Art. 5 Abs. 2 DSGVO.	☐ Ja ☐ Nein
Welche risikoangemessenen Schutzmaßnahmen sind vorgesehen und umgesetzt?	› Um die passenden technischen bzw. organisatorischen Maßnahmen auszuwählen, müssen zunächst die Risiken ausgemacht und bewertet sein. Lassen Sie sich die Risikoanalyse erklären. › Die Maßnahmen nach Art. 32 DSGVO müssen risikoangemessen sein. Bei sensiblen Daten kommen weitere Anforderungen hinzu. Denken Sie hier an die Vorgaben die etwa § 22 Abs. 2 BDSG für bestimmte Fälle macht. Diese Vorgaben gelten auch bei sensiblen Daten im Beschäftigungskontext (§ 26 Abs. 3 Satz 3 DSGVO).	☐ Ja ☐ Nein
Inwieweit ist eine Datenschutz-Folgenabschätzung (DSFA) erforderlich?	› Klären Sie die Erforderlichkeit aufgrund Art. 35 DSGVO bzw. auf Basis der Vorgaben der deutschen Aufsichtsbehörden im Rahmen der sogenannten DSFA-Muss-Liste. › Wurde eine Folgenabschätzung durchgeführt, prüfen Sie, inwieweit Sie eingebunden waren. Das ist Pflicht (Art. 35 Abs. 2 DSGVO). › Prüfen Sie, ob die DSFA den Mindestanforderungen nach Art. 35 Abs. 7 entspricht.	☐ Ja ☐ Nein
Wie werden die Betroffenenrechte umgesetzt?	› Schauen Sie sich mit den Kollegen die Art. 12 ff. DSGVO an. Sprechen Sie durch, wie beispielsweise die Transparenz oder das Recht auf Auskunft oder Löschung umgesetzt werden. › Hinterfragen Sie die Prozesse. Aufgrund der Sensibilität der Daten muss etwa bei der Klärung der Identität eines Betroffenen im Rahmen einer Auskunft sorgfältiger vorgegangen werden.	☐ Ja ☐ Nein
Welche Regelungen und Arbeitsanweisungen sind festgelegt, kommuniziert und in Kraft?	› Sehen Sie sich die Festlegungen an. Prüfen Sie diese auf Vollständigkeit und Aktualität. › Nur wenn Regelungen bekannt sind, können Sie auch beachtet werden. Klären Sie, wo die Regelungen zu finden sind.	☐ Ja ☐ Nein
Wie werden die zuständigen Beschäftigten sensibilisiert und trainiert?	› Das ist unerlässlich, damit keine Fehler passieren. Die wären gerade bei sensiblen Daten besonders kritisch. › Lassen Sie sich z. B. Schulungsmaterial vorlegen. Prüfen Sie, inwieweit das der Sache und der Schutzwürdigkeit der Daten gerecht wird.	☐ Ja ☐ Nein
Welche Eintragungen wurden im Verzeichnis von Verarbeitungstätigkeiten vorgenommen?	› Das Verzeichnis nach Art. 30 Abs. 1 DSGVO muss vollständig und aktuell sein. Werfen Sie einen Blick in die Eintragungen. › Passt etwas nicht, adressieren Sie die entsprechende Aufgabe an die zuständigen Kollegen.	☐ Ja ☐ Nein
Wie wird die Verarbeitung fortlaufend auf Vereinbarkeit mit dem Datenschutz kontrolliert?	› Gerade Risiken können sich im Laufe der Zeit ändern, sodass die Schutzmaßnahmen angepasst werden müssen. Lassen Sie sich erläutern, was man in diesem Zusammenhang unternimmt. › Legen Sie großen Wert auf die Dokumentation der Prüfung. Auch das ist Teil der Rechenschaftspflicht.	☐ Ja ☐ Nein

Ineffizienz ade: So holen Sie mehr aus Besprechungen und Terminen heraus

Wie bei den meisten Datenschutzbeauftragten kommt wahrscheinlich auch bei Ihnen keine Langeweile auf, eher im Gegenteil! Sie haben viel um die Ohren und wissen manchmal nicht, was Sie zuerst in Angriff nehmen sollen. Dieses Problem kann sich noch verstärken, wenn Sie viel in Terminen oder Besprechungen sind. Umso wichtiger ist, dass Sie hier das meiste herausholen.

Ineffizienz killt alles

Termine sind unerlässlich, etwa wenn Sie als Datenschutzbeauftragter zum richtigen Umgang mit personenbezogenen Daten beraten wollen. Schließlich sind häufig Rahmenbedingungen oder Vorgehensweisen zu klären und Lösungsmöglichkeiten zu besprechen. Doch nur weil es einen Termin gibt, heißt das noch lange nicht, dass dieser effizient ist. Er kann Ihnen auch den letzten Nerv rauben. Bekommen Sie also zukünftig eine Terminanfrage, sagen Sie nicht einfach direkt zu. Nutzen Sie die folgende Checkliste, um von Anfang an die Sache effizienter zu gestalten.

CHECKLISTE: Vorbereitung von effizienten Terminen

Das sollten Sie klären	Hintergrund	Erledigt?
Worum geht es im Termin?	Geht das nicht aus der Einladung zum Termin hervor oder ist der Grund Ihnen bereits bekannt, sollten Sie nachfragen. Das kann per E-Mail erfolgen. Per Telefon ist es jedoch meist besser, weil Sie hier unkompliziert weitere Informationen erfragen können, die für Sie von Bedeutung sind.	☐ Ja ☐ Nein
Worauf zielt die Besprechung ab?	Klären Sie, was das Ergebnis der Besprechung sein soll. Es macht einen großen Unterschied, ob es um einen Austausch, erste Informationen, Entscheidungen oder um eine konkrete Beratung Ihrerseits geht.	☐ Ja ☐ Nein
Ist eine Besprechung überhaupt sinnvoll bzw. erforderlich?	Nur weil man Ihnen einen Termin in den Kalender setzt, hat dieser noch nicht automatisch seine Berechtigung. Können Sie die Sache auch einfach mit einer kurzen E-Mail erledigen, hat sich ein Termin ggf. erübrigt.	☐ Ja ☐ Nein
Inwieweit ist der Zeitrahmen des Termins realistisch?	Das, was im Termin bewerkstelligt werden soll, muss auch realistisch machbar sein. Eine umfassende Beratung mit Diskussion von Lösungsmöglichkeiten lässt sich nicht in 20 Minuten unterbringen. Verschieben Sie ggf. den Termin bzw. bitten Sie um einen längeren Termin.	☐ Ja ☐ Nein
Haben Sie überhaupt die nötige Zeit für den Termin?	Bewerten Sie, inwieweit der Termin wichtig und dringlich ist, wenn Sie ohnehin schon einen übervollen Terminkalender haben. Ist das nicht der Fall, sollten Sie um einen späteren Termin bitten.	☐ Ja ☐ Nein
Ist Ihre Teilnahme vor Ort unerlässlich?	Nicht an jedem Termin müssen Sie selbst vor Ort teilnehmen. Ggf. können Sie sich auch virtuell zuschalten. Das kann Ihnen viel Zeit drumherum sparen.	☐ Ja ☐ Nein
Warum ist Ihre Teilnahme erforderlich bzw. wichtig?	Bewerten Sie Ihre Bedeutung für den Erfolg des Termins. Spielen Sie eine tragende Rolle, sollten Sie den Termin ermöglichen. Weil Sie im Mittelpunkt stehen, sollten Sie auch entsprechend Zeit und Aufwand in Ihre Vorbereitung investieren.	☐ Ja ☐ Nein
Welche anderen Teilnehmer gibt es?	Schauen Sie sich an, wer teilnimmt. Das hilft Ihnen, die Bedeutung und Ihre Position innerhalb der Teilnehmer einzuordnen. Ist etwa der Geschäftsführer dabei, sollten Sie schon allein wegen des Aspekts „Außenwirkung als Datenschutzbeauftragter" daran teilnehmen.	☐ Ja ☐ Nein
Welche Rollen nehmen die anderen Teilnehmer wahr?	Klären Sie, in welcher Rolle die anderen Teilnehmer agieren. Sind im Termin Entscheidungen zu treffen, sollten die Teilnehmer auch über die entsprechende Kompetenz verfügen. Fehlen aus Ihrer Sicht relevante Teilnehmer, sollten Sie deren Einladung anregen.	☐ Ja ☐ Nein
Liegt bereits eine Agenda für die Besprechung vor?	Eine Agenda verrät Ihnen viel, was im Termin passieren soll. Dementsprechend können Sie sich darauf vorbereiten.	☐ Ja ☐ Nein
Stehen nötige Informationen zur Vorbereitung bereits vorab zur Verfügung?	Um den Termin inhaltlich effizient zu gestalten, ist eine gute Vorbereitung unabdingbar. Lassen Sie sich relevante Informationen oder Unterlagen vorab zur Verfügung stellen.	☐ Ja ☐ Nein
Müssen andere Teilnehmer etwas vorbereiten?	Eventuell muss aus Ihrer Sicht von den Teilnehmern bis zum Termin für diesen etwas vorbereitet werden. Auch Kleinigkeiten können hier viel bringen: Schon ein Datenflussdiagramm kann Ihnen das Überblicken der Gesamtsituation erleichtern.	☐ Ja ☐ Nein
Wird es ein Protokoll zum Termin geben?	Gerade wenn Sie am Termin nicht teilnehmen können oder früher rausmüssen, kann ein Protokoll Aufschluss geben, was noch passiert ist. Prüfen Sie ein Protokoll immer zeitnah, damit Sie falsche Darstellungen direkt korrigieren lassen können.	☐ Ja ☐ Nein

Teilnehmerdaten für den Trainer: Liegt eine Auftragsverarbeitung vor?

FRAGE: Unser Unternehmen holt sich beispielsweise für Verkaufstrainings oder für andere Schulungen externe Trainer ins Haus. Das ist nötig, da wir vom Spezialwissen und von den Branchenkenntnissen der Trainer profitieren wollen. Die Schulungen und der Kontakt zu den Trainern werden von unserer Personalentwicklung organisiert. Hier kam nun auch das folgende Thema hoch: Wenn beispielsweise Teilnehmerinformationen im Vorfeld zu einer Schulung an den Trainer weitergegeben werden, stellen wir dem Trainer zahlreiche Daten zur Verfügung. So z. B. Name, Abteilung, Zuständigkeitsbereich, dienstliche E-Mail-Adresse und Telefonnummer. Liegt hier ein Fall der Auftragsverarbeitung vor? Muss mit dem Trainer eine entsprechende Vereinbarung geschlossen werden bzw. müssen wir Vorgaben zum technisch-organisatorischen Datenschutz machen?

ANTWORT: Ob ein Fall der Auftragsverarbeitung vorliegt, hängt in der Regel von der Ausgestaltung der jeweiligen Zusammenarbeit ab. Kennzeichnend für eine Auftragsverarbeitung im Sinne von Art. 28 Datenschutz-Grundverordnung (DSGVO) ist das weisungsgebundene Verarbeiten personenbezogener Daten. Dabei steht das tatsächliche Verarbeiten im Vordergrund. Der Verantwortliche entscheidet zudem allein über Ob und Wie der Verarbeitung personenbezogener Daten. Er legt fest, welche personenbezogenen Daten zu welchem Zweck verarbeitet werden. Das umfasst beispielsweise auch den Personenkreis, den Verarbeitungszusammenhang oder die Gestaltung der Erhebung der Daten.

Bei externen Trainern ist jedoch meist keine solche Konstellation gegeben. Der Trainer erhält die Daten, um eigenständig seine Schulung zu organisieren. Insofern legt er auch fest, welche personenbezogenen Daten im Vorfeld erforderlich sind, damit er die Schulung inhaltlich gestalten kann. Je nach Schulung kann also auch der Umfang der Datenverarbeitung völlig unterschiedlich ausfallen. So kann es bei der einen Schulung ausreichen, eine Namensliste zu erhalten, um etwa die Anwesenheit kontrollieren zu können. Bei einer anderen Schulung sind ggf. weitergehende und auch persönlichere Informationen nötig, um die Inhalte auf die Vorkenntnisse der Teilnehmer zuzuschneiden. Den Umfang der Datenverarbeitung legt hier grundsätzlich der Trainer fest. Weil er selbst über Zweck und Mittel der Verarbeitung entscheidet, ist er selbst Verantwortlicher im Sinne von Art. 4 Nr. 7 Datenschutz-Grundverordnung (DSGVO).

Denken Sie an die Rechtsgrundlage

Da es sich beim Trainer um einen eigenen Verantwortlichen handelt, liegt zwar kein Fall der Auftragsverarbeitung vor. Insofern muss auch keine Vereinbarung zur Auftragsverarbeitung geschlossen werden. Allerdings dürfen personenbezogene Daten zu den Beschäftigten nicht einfach nach Wunsch und Belieben an den Trainer weitergegeben werden. Insofern bedarf es einer Rechtsgrundlage. Diese kann sich aus Art. 6 Abs. 1 Satz 1 DSGVO bzw. auch aus § 26 Abs. 1 Satz 1 Bundesdatenschutzgesetz ergeben. Beim Thema Rechtsgrundlage ist jedoch entscheidend: Die Verarbeitung muss für den verfolgten Zweck erforderlich sein. Auch müssen die Grundsätze der Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 DSGVO) beachtet werden. Hier ist insbesondere der Grundsatz der Datenminimierung von Relevanz. Danach müssen sie dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

Vertragliche Festlegungen können sinnvoll sein

Auch wenn kein Fall der Auftragsverarbeitung vorliegt, kann es Ihrem Unternehmen ein Anliegen sein, für umfassenden Datenschutz für die Beschäftigtendaten zu sorgen. Das lässt sich in den Vertrag mit dem Trainer aufnehmen. So z. B. dass dieser Daten durch risikoangemessene Maßnahmen zu schützen hat, was insbesondere die verschlüsselte Speicherung der Daten und die Löschung nach Abschluss der Schulungsmaßnahmen umfassen kann.

Smartphone gestohlen: Besteht hier ein großes Risiko?

FRAGE: Dem Geschäftsführer wurde sein Smartphone gestohlen. Um dieses zu entsperren, muss man einen alphanumerischen Code eingeben bzw. eine biometrische Erkennungsmethode nutzen. Er hat nun doch Sorge um die Daten auf dem Gerät. Was meinen Sie: Besteht hier ein großes Risiko? Müssen wir etwas veranlassen?

ANTWORT: Wenn die bordeigenen Schutzmechanismen aktiviert waren, etwa die Datenverschlüsselung, dürften die Daten auf dem Smartphone sicher sein. Allerdings ist nicht völlig auszuschließen, dass ein schwacher Code durch Erraten oder Ausprobieren „geknackt" wird und so ein Zugriff auf Daten möglich ist. Wie hoch das entsprechende Risiko ist, lässt sich kaum einschätzen. Doch die meisten Diebe haben eher kein Interesse an den Daten, sondern vielmehr am Gerät an sich, das sich leicht zu Geld machen lässt. Wird das Gerät dann neu eingerichtet, werden regelmäßig die Altdaten gelöscht, sodass kein Zugriff mehr möglich ist.

Empfehlen Sie, den Verlust schnellstens der IT-Abteilung zu melden. Vielleicht ist eine Fernlöschung möglich.

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 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 Datenverarbeitung. 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 entschieden die Richter

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

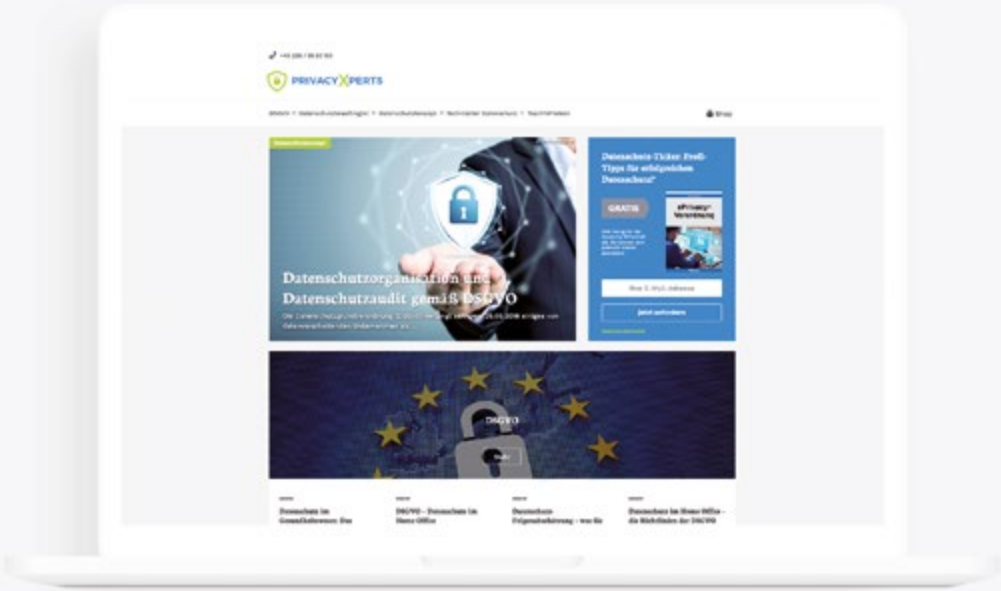
Aus Sicht des Gerichts mussten Betroffene bei der Erhebung der Daten vernünftigerweise mit einer entsprechenden Verarbeitung rechnen. Die Verarbeitung der Daten ist auf von Nutzern öffentlich gemachte Daten beschränkt. Zudem wurden seitens Meta Maßnahmen umgesetzt, um den Eingriff in die Rechte der Betroffenen 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.

Das können Sie aus der Entscheidung folgern

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 Verarbeitung 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

Schnell und effektiv Mitarbeiter schulen!

Jetzt Mitarbeiterinformation bestellen

https://t1p.de/gmxhs

Vorschau:

Ab in die Cloud: Diese Punkte sollten Sie ansprechen
Kontinuierlich besser werden: So gehen Sie es an

PRIVACYXPERTS

Telefon: 02 28 95 50 150
Fax: 02 28 36 96 480
E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de

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