DATENSCHUTZAKTUELL
OKT II
2026
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH



ALLES VERSCHLÜSSELT? MACHEN SIE DEN PRAXISCHECK

MUSTER & VORLAGEN
Minimieren Sie die Risiken beim KI-Einsatz im Unternehmen 1–2

RECHT & RICHTLINIE
ArbG: Vertrauliches im Gruppenchat kann teuer werden 8



Unterschätzen Sie nie den Faktor Zeit

Liebe Leserin, lieber Leser,

wenn etwas am Auto kaputt ist, ändert sich am Zustand in der Regel nichts, wenn man Zeit ins Land ziehen lässt. Im Gegenteil: Je mehr Zeit verstreicht, desto größer wird meist der Schaden und desto teurer wird die Reparatur.

Nicht viel anders ist es im Datenschutz: Läuft etwas nicht rund oder passt etwas nicht, wird es mit der Zeit nicht von selbst besser. Auch hier können die Schäden schnell zunehmen und das Reparieren kann teuer werden. Daher: Besteht Handlungsbedarf, sollten Sie nie zum Abwarten raten. Heben Sie sofort die Hand oder gehen Sie schnell auf die Verantwortlichen zu.

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 im Unternehmen pragmatisch umsetzen lässt.

Inhalt

Muster & Vorlagen
Minimieren Sie die Risiken beim KI-Einsatz im Unternehmen
Seiten 1–2

Know-how
So prüfen Sie die Weitergabe von Daten an den Betriebsrat
Seite 3

Muster & Vorlagen
Alles verschlüsselt? Machen Sie den Praxischeck
Seiten 4–5

Datenschutz kompakt
So reagieren Sie auf Unqualifiziertes zum Datenschutz
Seite 6

Fragen an die Redaktion
Muss ich bei einem konsolidierten Tätigkeitsbericht mitmachen?
Seite 7

Darf der Betriebsrat nur über die Personalabteilung mit mir reden?
Seite 7

Recht & Richtlinie
ArbG: Vertrauliches im Gruppenchat kann teuer werden
Seite 8

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

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

E-Mail-Beratung:
https://t1p.de/andreas-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 Chefredakteur:
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: KI-generiert; Seite 1: Adobe Stock | m.mphoto

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

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.

© 2026 by VNR Verlag für die Deutsche Wirtschaft AG, Bonn, Berlin, Bukarest, Jacksonville, Manchester, Passau, Warschau



Ohne Frage, KI im Arbeitsalltag ist praktisch. Helfen Sie, immer die Risiken im Blick zu behalten.

Minimieren Sie die Risiken beim KI-Einsatz im Unternehmen

Nutzt Ihr Unternehmen bereits künstliche Intelligenz (KI)? Das wäre nicht überraschend. Schließlich kann mit KI so manches vereinfacht, beschleunigt und produktiver gestaltet werden. Denken Sie etwa an die Erstellung von Präsentationsfolien oder das Übersetzen eines Textes. Doch auch wenn das noch so praktisch ist. Wie so oft gilt: Wo Licht ist, da ist auch Schatten, gerade unter Datenschutzaspekten.

Gehen Sie den Dingen auf den Grund

Im Zusammenhang mit KI herrscht in vielen Unternehmen Aufbruchstimmung. Doch einfach drauflosprompten und die KI auch mit personenbezogenen Daten füttern ist keine gute Idee. Schließlich handelt es sich dann auch um eine Verarbeitung personenbezogener Daten. Und für die gelten Regeln, insbesondere die der Datenschutz-Grundverordnung (DSGVO).

Doch nicht jedem ist das bewusst. Umso wichtiger ist, dass Sie als Datenschutzbeauftragter Ihrem Beratungs- und Kontrollauftrag aus Art. 39 Abs. 1 DSGVO nachkommen. Das gelingt Ihnen beispielsweise, indem Sie zunächst etwas Licht ins Dunkel bringen.

Sprechen Sie mit den zuständigen Kollegen und setzen Sie auf die folgende Checkliste. So stellen Sie nicht nur sicher, dass Sie keinen wichtigen Aspekt vergessen. Sie können zugleich auch für die nötige Sensibilität sorgen. Schließlich gilt es bei KI, nicht nur die spezifischen Regeln der KI-Verordnung zu beachten. Sind personenbezogene Daten im Spiel, greift voll und ganz die DSGVO. Beherzigen Sie insofern immer: Der Schwerpunkt Ihres Checks sollte auf dem Datenschutz liegen.

Checkliste: Wichtige Aspekte beim Einsatz von KI

Aspekt	Das ist wichtig	In Ordnung?
Datenschutzaspekte		
Besteht ein Überblick darüber, welche KI-Lösungen bereits im Einsatz sind?	› Es ist wahrscheinlich, dass KI auch dann zum Einsatz kommt, wenn sie noch nicht offiziell eingeführt wurde. Schließlich kann es nicht nur Schatten-IT geben, sondern auch Schatten-KI. Das sind KI-Tools, die ohne Freigabe und von Mitarbeitern eigenmächtig eingesetzt werden. › Eine kritische Bestandsaufnahme ist unerlässlich. Nehmen Sie keine Bereiche aus. Schließlich kann KI in allen Bereichen hilfreich sein, etwa auch im Facility Management oder bei der Planung des Speiseplans in der Kantine.	○ Ja ○ Nein
Inwieweit werden mit der KI personenbezogene Daten verarbeitet?	› Klären Sie, welche Daten verarbeitet werden. Entscheidend ist die Identifizierbarkeit einer natürlichen Person. › Bei KI wird schon der abgesendete Prompt zum Problem, wenn dieser personenbezogene Daten enthält. › Geben Sie die Faustregel aus, dass alles Personenbezogene entfernt sein muss, etwa Namen, E-Mail-Adressen, Kundennummern, Telefonnummern, Fotos und Individualisierendes in Bewerbungsunterlagen.	○ Ja ○ Nein

Aspekt	Das ist wichtig	In Ordnung?
Wurden Daten nach ihrer Schutzbedürftigkeit kategorisiert?	› Nicht alle Daten haben das gleiche Schutzbedürfnis. Auch das Potenzial eines Schadens ist unterschiedlich, etwa wenn Daten in falsche Hände geraten. › Die Schutzbedürftigkeit sollte regelmäßig überprüft werden. Mit der Zeit kann es zu erheblichen Veränderungen kommen, etwa wenn neue Datenarten verarbeitet werden.	○ Ja ○ Nein
Können für die auf KI basierende Verarbeitung personenbezogener Daten die Grundsätze nach Art. 5 Abs. 1 DSGVO eingehalten werden?	› Sollen personenbezogene Daten verarbeitet werden, müssen alle Grundsätze der Verarbeitung aus Art. 5 Abs. 1 DSGVO eingehalten werden. Die sind immer verpflichtend. › Gerade bei der Rechtsgrundlage heißt es Obacht. Je nach Verarbeitungszusammenhang können unterschiedliche Rechtsgrundlagen nötig sein. Das Übersetzen einer E-Mail kann ggf. auf ein überwiegendes berechtigtes Interesse gestützt werden. Für das Training eines KI-Modells bedarf es jedoch meist der Einwilligung des Betroffenen. › Haben Sie besonders ein Auge auf die Grundsätze der Datenminimierung und Vertraulichkeit. Die personenbezogenen Daten müssen auf das Erforderliche begrenzt sein. Zudem muss die Sicherheit der Verarbeitung gewährleistet sein. Insbesondere dürfen Daten nicht in falsche Hände geraten.	○ Ja ○ Nein
Wird mit der KI über Personen entschieden?	› Soll die KI automatisiert Entscheidungen über Personen treffen, die erhebliche Tragweite haben (z. B. Bewerberauswahl, Kreditvergabe), kann dies nach Art. 22 DSGVO unzulässig sein. › Lassen Sie sich das konkrete Vorgehen schildern und bewerten Sie dann die Relevanz.	○ Ja ○ Nein
Sind denkbare Risiken analysiert und bewertet?	› Gerade im Hinblick auf den Datenschutz müssen Gefahren und die daraus resultierenden Risiken bewertet werden. Auch Schutzmaßnahmen müssen risikoangemessen ausgewählt und umgesetzt werden. › Betrachten Sie die Sache nicht nur aus Unternehmenssicht. Im Fokus müssen auch der Betroffene und dessen Daten stehen. › Wagen Sie zudem den Blick über den Tellerrand. Es bestehen immer Risiken für schützenswerte Unternehmensdaten, etwa Produktionsverfahren, Quellcode, Marktanalysen oder Geschäftsgeheimnisse.	○ Ja ○ Nein
Wurden risikoangemessene Schutzmaßnahmen festgelegt und umgesetzt?	› Schutzmaßnahmen sind auch beim Einsatz von KI unerlässlich. So muss nicht nur gewährleistet sein, dass bei den Systemen die Vertraulichkeit gewährleistet ist. Das gilt auch für die Integrität und Verfügbarkeit der Systeme und Dienste für die Verarbeitung der Daten. › Schauen Sie, inwieweit die Maßnahmen tatsächlich dazu beitragen, Risiken angemessen zu reduzieren. Hohe Risiken sind ein Problem. Meist ist in diesem Zusammenhang auch eine Datenschutz-Folgenabschätzung erforderlich.	○ Ja ○ Nein
Sind Datenanbindungen bzw. Zugriffsrechte der KI eingeschränkt?	› Auch KI-Systeme bzw. Agenten können ein Eigenleben entwickeln oder etwas mit Informationen anstellen, was Ihrem Unternehmen nicht recht ist. Insofern sollten Anbindungen und Zugriffsrechte weitgehend eingeschränkt werden. Auch hier kann eine Risikoanalyse nötig sein. › Machen Sie stets klar: Geht etwas schief, ist Ihr Unternehmen dafür verantwortlich. Dass die KI gepatzt hat, ist für die Verantwortung und Haftung irrelevant.	○ Ja ○ Nein
Können Betroffenenrechte gewahrt werden?	› Lassen Sie sich konkret erläutern, wie man die nötige Transparenz gegenüber Betroffenen herstellt. Ggf. müssen die Datenschutzhinweise um Informationen zu einer KI-Verarbeitung ergänzt werden. › Werden mit fremdbetriebener KI personenbezogene Daten verarbeitet, muss sich eine Auskunft auch hierauf beziehen. › Auch das Löschen von personenbezogenen Daten im Zusammenhang mit KI-Systemen ist zu bedenken. Das muss umsetzbar sein.	○ Ja ○ Nein
Sind datenschutzrechtliche Rollen geklärt und ggf. erforderliche Vereinbarungen getroffen?	› Im Zusammenhang mit KI kann der Anbieter Auftragsverarbeiter sein. Dann ist eine entsprechende Vereinbarung obligatorisch. › Kommt es zum Datentransfer in Drittstaaten, muss das Datenschutzniveau abgesichert werden. Das Kapitel V der DSGVO ist umzusetzen.	○ Ja ○ Nein
Regelungen		
Gibt es eine verbindliche schriftliche Regelung zur KI-Nutzung im Unternehmen?	› Eine Arbeitsanweisung oder Richtlinie ist in der Regel unerlässlich. In dieser muss möglichst genau geregelt werden, was erlaubt und was verboten ist. › Achten Sie darauf, dass ein entsprechendes Regelwerk verständlich und aktuell ist. Gerade zulässige KI-Lösungen und erlaubte Einsatzszenarien müssen auf aktuellem Stand sein. › Neben einer Regelung für die Beschäftigten kann auch ein Betriebskonzept für die IT-Abteilung nötig sein. Das kann z. B. regeln, welche Funktionen nicht nutzbar sein sollen.	○ Ja ○ Nein
Ist die Nutzung privater KI-Lösungen und nicht freigegebener Werkzeuge untersagt?	› Private Accounts bergen für Ihr Unternehmen erhebliche Risiken. Oft ist nicht überschaubar, was mit personenbezogenen Daten des Unternehmens passiert. Dennoch bleibt das Unternehmen für seine Daten verantwortlich. › Gerade bei kostenlosen Accounts oder Einsteiger-Abos werden oft die Prompts und die der KI zur Verfügung gestellten Daten für Trainings- oder Analysezwecke verwendet. Das kann nicht im Interesse des Unternehmens sein.	○ Ja ○ Nein
Sind die Beschäftigten geschult und für Datenschutzaspekte sensibilisiert?	› Die mit KI arbeitenden Beschäftigten müssen über das nötige Know-how verfügen. Das fordert beispielsweise auch Art. 4 der KI-Verordnung. › Sehen Sie Awareness immer auch als organisatorische Schutzmaßnahme nach Art. 32 DSGVO.	○ Ja ○ Nein
Wurde der Betriebsrat eingebunden?	› KI-Systeme behalten vieles im „Gedächtnis". Das kann auch eine Leistungs- oder Verhaltenskontrolle der Arbeitnehmer ermöglichen. Dann hat der Betriebsrat mitzubestimmen (§ 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz). › Eine Betriebsvereinbarung darf die Datenschutzstandards der DSGVO nicht reduzieren. Das gilt auch bei KI-Lösungen.	○ Ja ○ Nein

So prüfen Sie die Weitergabe von Daten an den Betriebsrat

Gibt es in Ihrem Unternehmen einen Betriebsrat, wird dieser für seine Aufgaben auch viel mit personenbezogenen Daten zu tun haben. In diesem Zusammenhang ist es oft unerlässlich, dass der Betriebsrat vom Arbeitgeber Informationen über Arbeitnehmer erhält. Doch bei der Weitergabe von Daten an den Betriebsrat muss einiges beachtet werden. Hier sind Sie gefragt.

Will einmal die Personalabteilung von Ihnen wissen, ob man die vom Betriebsrat geforderten Informationen bereitstellen muss, ist Ihre Beratung bzw. Bewertung unerlässlich. Beachten Sie dabei die folgenden Tipps:

Tipp Nr. 1: Fordern Sie mehr konkrete Informationen

Unter Umständen ist Ihnen nicht klar, worum es ganz genau gehen soll. Vielleicht gibt es nur eine allgemeine Anfrage des Betriebsrats, etwa nach einer detaillierten Überstundenliste. Damit Sie überhaupt eine Bewertung vornehmen können, müssen Sie den Sachverhalt so klären, dass keine Fragen mehr offen sind. Wichtig ist beispielsweise:

- Wer konkret will die Informationen haben? Häufig muss der Betriebsrat als Gremium aktiv werden. Einzelne Mitglieder haben an sich keinen Anspruch auf bestimmte Informationen. Insofern bedarf es meist eines Betriebsratsbeschlusses.
- Um welche Informationen geht es ganz genau? Es muss vollständig aufgeführt werden, welche Informationen beansprucht werden. Allgemeine Beschreibungen, etwa Anwesenheitszeiten, reichen nicht aus. Fordern Sie eine Liste der einzelnen Datenfelder an. Diese muss man Ihnen nennen können, denn darauf basieren Ihre Bewertungen.
- Für welchen Zweck bzw. für welche Aufgabe werden die Daten benötigt? Auch hier muss für Klarheit gesorgt werden. Etwa ein „Überwachen der Einhaltung von Gesetzen" ist zu allgemein. Hier muss der Betriebsrat konkreter werden.

Tipp Nr. 2: Bewerten Sie die Schutzwürdigkeit

Verlassen Sie sich hier nicht auf allgemeine Einschätzungen. Häufig liegt man nämlich daneben. Prüfen Sie einerseits die Personenbeziehbarkeit von Daten. Denn die wird ab und an verkannt, etwa bei Personalnummern. Schauen Sie andererseits danach, ob besondere Kategorien personenbezogener Daten betroffen sind. Daten im Sinne von Art. 9 Abs. 1 Datenschutz-Grundverordnung (DSGVO) unterliegen strengeren Anforderungen.

Tipp Nr. 3: Klären Sie die Erforderlichkeit für die Betriebsratsarbeit

Die Daten müssen für die Wahrnehmung der Aufgaben des Betriebsrats erforderlich sein, siehe § 80 Abs. 1 Betriebsverfassungsgesetz (BetrVG). Das bedeutet einerseits, es muss eine entsprechende Aufgabe bestehen, etwa die Kontrolle der Einhaltung des Arbeitszeitgesetzes. Daneben müssen für diese Aufgabe genau die geforderten Informationen zu den Arbeitnehmern erforderlich sein.

Tipp Nr. 4: Thematisieren Sie die Grundprinzipien

Bei jeder Verarbeitung, eben auch bei der Weitergabe von Daten an den Betriebsrat, müssen die Grundsätze aus Art. 5 Abs. 1 DSGVO eingehalten werden. Wichtig ist hier besonders:

- **Rechtmäßigkeit:** Sind die Informationen für die Aufgabenwahrnehmung des Betriebsrats erforderlich, lässt sich die Weitergabe meist auf Art. 6 Abs. 1 Satz 1 Buchst. c DSGVO in Verbindung mit § 80 Abs. 2 BetrVG stützen. Eine Betriebsvereinbarung taugt als Rechtsgrundlage nur, wenn die Anforderungen aus Art. 80 Abs. 2 DSGVO eingehalten sind und die von der DSGVO vorgegebenen Standards eingehalten werden. Bei Daten nach Art. 9 Abs. 1 DSGVO muss zusätzlich eine Erlaubnis nach Art. 9 Abs. 2 DSGVO gegeben sein.
- **Datenminimierung:** Die Verarbeitung muss auf das erforderliche Maß beschränkt sein. Das bedeutet auch, dass ggf. zunächst nur anonymisierte Daten bereitgestellt werden, wenn dies für die Aufgabenwahrnehmung ausreichend ist.

Tipp Nr. 5: Die Schutzmaßnahmen müssen beim Empfänger passen

Zwar kann der Betriebsrat bei sich den Datenschutz weitgehend eigenständig organisieren und beispielsweise in einem Datenschutzkonzept festhalten. Allerdings müssen die Schutzmaßnahmen im Sinne von Art. 32 DSGVO passen. Gibt es etwa keine risikoangemessenen Schutzmaßnahmen, kann der Arbeitgeber die Weitergabe der betreffenden Daten verweigern.

Tipp Nr. 6: Schlagen Sie Regeln für regelmäßige Weitergaben vor

Häufig kommen Anfragen wiederholt vor. Geht es etwa um gleiche Verarbeitungen, z. B. die Bereitstellung von Arbeitszeitlisten, können Standardprozesse etabliert werden. Das hat viele Vorteile. So kann das Vorgehen beschleunigt werden und der Betriebsrat erhält kurzfristig und damit rechtzeitig die nötigen Informationen. Die Personalabteilung kann die festgelegten Schritte zuverlässig abarbeiten. Und Sie als Datenschutzbeauftragter müssen nicht immer wieder das Gleiche neu prüfen.

Tipp Nr. 7: Dokumentieren Sie Ihre Einschätzung

Halten Sie Ihre Einschätzung schriftlich fest. Das umfasst nicht nur die Einschätzung und Ihre Empfehlung. Am besten dokumentieren Sie auch den Sachverhalt bzw. wer Ihnen was mitgeteilt hat. Das beugt gerade späteren Erinnerungslücken vor.

Alles verschlüsselt? Machen Sie den Praxischeck

Verschlüsselung ist wichtig – das weiß jeder Datenschutzbeauftragte. Doch bei Unternehmensleitung, IT-Abteilung und Beschäftigten ist das noch lange nicht so. Schließlich kann auch eine Verschlüsselung manches unpraktisch machen oder mit viel technischem wie finanziellem Aufwand verbunden sein. Und dennoch sollten Sie ein Auge auf zu verschlüsselnde Daten haben.

Schauen Sie in Art. 32 Datenschutz-Grundverordnung (DSGVO), erkennen Sie schnell: Ihr Unternehmen muss als Verantwortlicher oder Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen ergreifen, damit ein dem Risiko angemessenes Schutzniveau sichergestellt wird. Und genau in Art. 32 DSGVO wird das Verschlüsseln ausdrücklich als mögliche Schutzmaßnahme erwähnt.

So überzeugen Sie Zweifler

Das Verschlüsseln von Daten oder Übertragungswegen ist mit Aufwand und Kosten verbunden. Kein Wunder, dass mancher lieber darauf verzichtet. Doch einer ablehnenden Haltung können Sie immer mit drei guten Argumenten entgegentreten:

- Verlust führt nicht automatisch zur Datenpanne: Wird beispielsweise das Notebook des Geschäftsführers gestohlen, kann das schnell zum großen Problem werden. Wurde nicht auf eine dem Stand der Technik entsprechende Verschlüsselung gesetzt, können personenbezogene Daten in die Hände Unbefugter gelangen. Schon die Möglichkeit kann die Meldepflicht nach Art. 33 DSGVO auslösen. Und die Meldung einer Datenpanne kann schnell zu weiteren Fragen der Behörde oder gar einer Kontrolle führen. Ist das Notebook verschlüsselt, wäre erst mal nur der Verlust des Geräts zu beklagen.
- Benachrichtigung Betroffener kann überflüssig werden: Datenpannen sind schlecht für das Image Ihres Unternehmens. Das gerade dann, wenn hohe Risiken für die Betroffenen bestehen und nach Art. 34 DSGVO auch die Betroffenen über die Verletzung des Schutzes personenbezogener Daten zu informieren sind. Doch das kann man sich sparen, wenn die Daten für Unbefugte unzugänglich gemacht waren, etwa durch Verschlüsselung (Art. 34 Abs. 3 Buchst. a DSGVO).
- Beute wird für Cyberkriminelle wertlos: Auch wenn Ihr Unternehmen viel in die Sicherheit seiner Systeme investiert, kann es dennoch passieren, dass Hacker oder Cyberkriminelle Erfolg haben. Und die reißen sich dann alles unter den Nagel, was sie finden können. Denn je mehr oder sensibler die erbeuteten Daten sind, desto eher und mehr lassen sich diese für Erpressungen nutzen. Nutz- und wertlos ist die Beute jedoch, wenn die Daten mit aktuellen Verfahren verschlüsselt sind.

Verschlüsselung: Übersehen Sie keine wichtigen Bereiche

Am besten ist, wenn Sie ins Gespräch mit der IT-Abteilung gehen. Mit den Kollegen können Sie einerseits diskutieren, ob in wichtigen Feldern Verschlüsselung zum Einsatz kommt. Nehmen Sie die folgende Checkliste als Gesprächsleitfaden. Hier können Sie auch eine wichtige Frage stellen: Entspricht die jeweils eingesetzte Verschlüsselung dem Stand der Technik? Dabei müssen Sie sich nicht in Fachbegriffe stürzen oder mit kryptografischen Schlüssellängen hantieren. Erst recht müssen Sie nicht entscheiden, was dem Stand der Technik entspricht. Das ist Sache der Kollegen. Es reicht, wenn Sie darum bitten, dass man beispielsweise die technische Richtlinie des Bundesamts für Sicherheit in der Informationstechnik „Kryptographische Algorithmen und Schlüssellängen" (BSI TR-02102-1 vom 23.1.2026) einhält.

Checkliste: Hier sollte Verschlüsselung zum Einsatz kommen

Bereich	Das ist besonders wichtig	Besprochen?
Internes WLAN am Standort	› Das WLAN endet nicht am Gebäude bzw. an der Grundstücksgrenze. Ohne Verschlüsselung können Unbefugte unbemerkt von außerhalb Zugriff nehmen. › Mindeststandard bei der WLAN-Verschlüsselung sollte WPA2-PSK oder WPA3 sein. Der Schlüssel darf nicht leicht zu erraten oder zu erschließen sein. Komplexität und eine Länge von mindestens 20 Zeichen sind hier ein Muss. › Ggf. kann auch eine Gerätefilterung sinnvoll sein, sodass sich nur registrierte und bekannte Geräte mit dem WLAN verbinden können. › Eventuell müssen Schlüssel geändert werden, wenn Beschäftigte das Unternehmen verlassen.	○ Ja ○ Nein
Bereich	**Das ist besonders wichtig**	**Besprochen und in Ordnung?**
Gäste-WLAN	› Besucher und Gäste sollten nie im allgemeinen WLAN des Unternehmens sein. Das reduziert an sich schon Zugriffsmöglichkeiten. › Neben der Verschlüsselung können Zugriffsrechte für Gäste auch zeitlich begrenzt werden. Verfallen Zugriffsrechte automatisch, muss sich niemand um den Entzug kümmern.	○ Ja ○ Nein
WLAN im Homeoffice	› Hierbei handelt es sich in erster Linie um ein Sensibilisierungsthema. Auch Beschäftigte müssen einen angemessenen Sicherheitsstandard umsetzen, wenn sie im Homeoffice das eigene WLAN nutzen. › Klären Sie, inwieweit es Checklisten gibt, die auch die Themen Verschlüsselung sowie Sicherheitsupdates des Routers abdecken.	○ Ja ○ Nein

Bereich	Das ist besonders wichtig	Besprochen und in Ordnung?
VPN-Datenübertragung	› Eine Einwahl ins Firmennetzwerk darf nur möglich sein, wenn hierfür eine aktuelle VPN-Lösung eingesetzt wird. › Die Nutzung sollte technisch erzwungen werden, damit Beschäftigte diese Sicherheitsmaßnahme nicht aus Bequemlichkeit unterlassen.	○ Ja ○ Nein
Computer & Co.	› Denken Sie nicht nur an Notebooks. Auch Desktop-Computer sollten beim Thema Verschlüsselung nicht ausgenommen werden. Schließlich können auch diese gestohlen werden. Eine Datenpanne ist in einem solchen Fall vorprogrammiert. › Achten Sie darauf, dass zumindest die bordeigenen Lösungen der Betriebssysteme zum Einsatz kommen, z. B. BitLocker bei Windows oder FileVault bei MacOS. › Auch Funkgeräte wie Maus oder Tastatur sollten Verschlüsselung beherrschen.	○ Ja ○ Nein
Mobile Datenträger	› Am besten sind mobile Datenträger voll verschlüsselt. Dann kann nichts aus Versehen unverschlüsselt gespeichert werden. Gut funktionieren auch bordeigene Verschlüsselungen der Betriebssysteme. › Je nach Situation und Nutzer können auch hardwareverschlüsselte Datenträger infrage kommen. Die sind jedoch oft sehr teuer. Außerdem muss auch hier darauf geachtet werden, dass die Verschlüsselung dem Stand der Technik entspricht.	○ Ja ○ Nein
Smartphones und Tablets	› Verschlüsselung der Geräte ist ein Muss und nicht nur eine Option. › Idealerweise sind solche Endgeräte durch die IT-Abteilung gemanagt. Dann können auch Sicherheitsrichtlinien implementiert werden, etwa zur Verschlüsselung und zur Anmeldung bzw. zu Entsperrcodes. › Bei nicht gemanagten Geräten sollte es Regeln und Anweisungen für die Nutzer geben. Mit entsprechender Sensibilisierung steigt die Wahrscheinlichkeit, dass die vorgegebenen Schutzmaßnahmen auch tatsächlich umgesetzt werden.	○ Ja ○ Nein
Multifunktionsgeräte, Fax & Co.	› Moderne Geräte verfügen über Datenspeicher und Festplatten. Idealerweise sind die enthaltenen Daten verschlüsselt, sodass bei Rückgabe oder im Wartungsfall kein Risiko für einen unbefugten Zugriff besteht. › Standardpasswörter und Verschlüsselungskennwörter müssen geändert sein.	○ Ja ○ Nein
Videokonferenzen, Chat- und Messengerdienste	› Fehlt es hier an Verschlüsselung können Unbefugte mithören, mitlesen oder zuschauen. Auch hier kann es schnell zu einem Datenabfluss kommen, der für Ihr Unternehmen zum Problem wird. › Schauen Sie in die Produktspezifikationen des Anbieters und klären Sie mit der IT-Abteilung, ob der Stand der Technik eingehalten wird.	○ Ja ○ Nein
Dateiablagen und Datenbanken	› Je sensibler Daten sind, desto mehr muss auch hier auf Verschlüsselung gesetzt werden. › Verschlüsselung ist hier eine wichtige Maßnahme, um eine Chance gegen Cyberkriminelle zu haben, wenn deren Angriff erfolgreich ist.	○ Ja ○ Nein
Datencontainer	› Müssen mehrere Dateien ausgetauscht werden, bieten sich Datencontainer an, etwa ZIP-Dateien. Hier ist wichtig, dass ein sicheres Verschlüsselungsverfahren verwendet wird, etwa AES 256. › Am besten wird die komplette ZIP-Datei verschlüsselt, sodass beim Anklicken direkt die Passwortabfrage kommt und die Inhalte der ZIP-Datei nicht angezeigt werden. Auch Dateinamen können viel verraten. › Verschlüsselte Datencontainer können eine gute Lösung sein, wenn große Datenmengen sicher transportiert werden müssen.	○ Ja ○ Nein
Datensicherungen	› Auch Back-ups sind für Angreifer ein interessantes und attraktives Ziel. Am besten ist es, wenn die Back-ups verschlüsselt sind und die Entschlüsselungspasswörter anderswo sicher aufbewahrt werden. › Sprechen Sie auch immer das Thema Wiederherstellbarkeit an. Die muss funktionieren, was auch geprobt werden sollte.	○ Ja ○ Nein
Daten auf dem Weg in die Cloud und in der Cloud	› Für den Transport ist eine TLS-Verschlüsselung geboten, die am besten TLS1.3 entspricht. Auch bei der Speicherung sollte Verschlüsselung zum Einsatz kommen. › Eine moderne Verschlüsselung ist eine Sache. Eine andere Sache ist, wer die Hoheit über den Schlüssel hat. Liegt dieser beim Cloud-Anbieter, hat dieser Zugriff. Auch kann er beim Anbieter abhandenkommen oder gestohlen werden. Besser ist es, wenn Ihr Unternehmen den Schlüssel selbst verwaltet.	○ Ja ○ Nein
E-Mail-Austausch zwischen Servern	› Der Austausch von E-Mails sollte immer TLS-verschlüsselt sein, sodass der Transport zwischen E-Mail-Servern sicher ist. › Die Verschlüsselung muss obligatorisch sein, damit das Risiko für einen unbefugten Zugriff beim Transport ausgeschlossen ist.	○ Ja ○ Nein
Ende-zu-Ende-Verschlüsselung bei E-Mails	› Werden hoch sensible oder besonders schützenswerte Daten ausgetauscht, sollte eine Ende-zu-Ende-Verschlüsselung zum Einsatz kommen. › Bringen Sie in diesem Zusammenhang auch das Thema Signatur zur Sprache. Werden Inhalte signiert, werden Manipulationen leichter erkennbar.	○ Ja ○ Nein
Dateiaustausch mit Externen	› Für den Austausch sollten Mittel und Wege bereitstehen, damit sensible Informationen nicht in falsche Hände geraten können. › Klären Sie, welche Austauschportale genutzt werden und wie es hier um das Thema Verschlüsselung bei der Übertragung und bei der Speicherung steht.	○ Ja ○ Nein
Passwortaufbewahrung	› Vielleicht nutzen die Beschäftigten Ihres Unternehmens Passwortmanager zur sicheren Aufbewahrung komplexer Passwörter. Auch hier muss die Verschlüsselung der Passwortdatei dem Stand der Technik entsprechen. › Eine gute Verschlüsselung ist jedoch kaum etwas wert, wenn auf ein schwaches Master-Passwort gesetzt wird. Ist das Master-Passwort stark?	○ Ja ○ Nein
Passwortspeicherung in eigenen Systemen	› Passwörter sollten nie im Klartext gespeichert werden. Vielmehr sind Hash-Werte das Mittel der Wahl. Aus diesen kann nämlich nicht auf das Passwort geschlossen werden. › Achten Sie darauf, dass eine verschlüsselte Speicherung der Anmeldeinformationen erfolgt.	○ Ja ○ Nein
Webseite, Onlineshop und Kontaktformulare	› Gibt es die Möglichkeit zur Dateneingabe (beispielsweise Shop oder Kontaktformular) oder zu einem Upload (etwa Bewerbungsunterlagen), ist eine aktuelle Verschlüsselung obligatorisch. › Prüfen Sie zudem Folgeprozesse. Auch beim Weiterversand von auf der Webseite eingegeben Informationen (z. B. an ein internes Postfach) muss auf Verschlüsselung gesetzt werden.	○ Ja ○ Nein

So reagieren Sie auf Unqualifiziertes zum Datenschutz

Früher oder später macht jeder Datenschützer Bekanntschaft damit. Die Rede ist von unqualifizierten oder populistischen Aussagen gegen den Datenschutz. Weil Sie im Unternehmen für viele der personifizierte Datenschutz sind, ist es kein Wunder, dass man Ihnen diese an den Kopf wirft. Die Vorwürfe brauchen Sie jedoch nicht schlucken. Drehen Sie einfach den Spieß um.

So reagieren Sie kompetent

Idealerweise beschäftigen Sie sich frühzeitig mit unqualifizierten Aussagen. Dann sind Sie nicht baff, wenn man Ihnen tatsächlich einmal etwas Unqualifiziertes um die Ohren haut. Überlegen Sie, wie Sie darauf reagieren und wie Sie die Aussagen entkräften können. Denn bei genauerem Überlegen lassen sich die Aussagen ganz schnell entkräften. Das zeigen Ihnen auch die folgenden Beispiele:

Die Aussage: „Der Datenschutz bremst uns nur aus"

So gehen Sie damit um: Machen Sie klar: Meist trifft das nicht zu. Es handelt sich um gesetzliche Vorgaben, die schon frühzeitig in die Planung einzubeziehen sind. Verzögerungen werden nur als „Bremsen" empfunden, weil nachträglich Prüfungen, Bewertungen oder Anpassungen vorgenommen werden müssen. Manchmal müssen auch zunächst nicht bedachte Risiken behandelt oder Vereinbarungen mit Anbietern oder Dienstleister geschlossen werden. Das alles geht nicht von jetzt auf gleich.

Die Aussage: „Das machen doch alle so"

So gehen Sie damit um: Lassen Sie dieses Statement einfach so stehen. Denn meist stimmt nichts an der Aussage. Fragen Sie konkret nach, wer denn „alle" sein sollen. Fordern Sie Namen von anderen Unternehmen. Zudem sind die Fälle meist nicht identisch, sodass sich ganz andere Konstellationen im Datenschutz ergeben können.

Die Aussage: „Der Anbieter sagt, alles sei datenschutzkonform"

So gehen Sie damit um: Werten Sie das als ein positives Zeichen, dass der Anbieter sich anscheinend um den Datenschutz bemüht. Hinterfragen Sie jedoch, was konkret mit der Aussage gemeint ist, etwa die Ausgestaltung eines Services, die Festlegungen in einer Vereinbarung oder die Umsetzung im konkreten Fall Ihres Unternehmens. Im Übrigen können Sie feststellen: Unter Umständen handelt es sich nur um eine etwas überzeichnete Marketingaussage. Die hilft Ihrem Unternehmen nicht viel. Schließlich ist und bleibt es für die Verarbeitung personenbezogener Daten verantwortlich.

Die Aussage: „Können Sie das nicht einfach freigeben?"

So gehen Sie damit um: Stellen Sie klar, welche Rolle und Funktion Sie haben. Sie sind der unabhängige Berater in Datenschutzfragen. Sie geben Empfehlungen, sie segnen nichts ab und geben nichts frei. Die Umsetzungsverantwortung und damit auch die unternehmerischen Entscheidungen im Zusammenhang mit einer Verarbeitung liegen beim Verantwortlichen, sprich der Unternehmensleitung.

Die Aussage: „Wir haben schon so viel Geld investiert. Wir können das nicht mehr ändern"

So gehen Sie damit um: Verdeutlichen Sie: Kam es zu Fehlentscheidungen oder vorschnellen Investitionen, ist das noch lange keine Rechtfertigung, um die geltenden gesetzlichen Anforderungen zu ignorieren. Empfehlen Sie, dass man Sie zukünftig frühzeitig einbindet, damit kostenträchtige Fehlentscheidungen vermieden werden.

Die Aussage: „Sie hätten schon viel früher sagen müssen, dass das so nicht umsetzbar ist"

So gehen Sie damit um: Gerade wenn schon viel Zeit und Geld in eine Verarbeitung investiert wurden, kann es ärgerlich sein, wenn sich erst spät herausstellt, dass die Sache nicht machbar ist. Verdeutlichen Sie hier, dass Ihre Einschätzung nicht auf bösem Wissen basiert. Vielmehr liegt es meist an der Komplexität der Materie bzw. an sich erst spät herausstellenden wichtigen Einflussfaktoren. Soweit möglich: Machen Sie Vorschläge, wie man dem Ziel möglichst nahekommen kann, ohne mit dem Datenschutz in Konflikt zu geraten.

Die Aussage: „Wir brauchen heute noch grünes Licht. Ansonsten müssen wir alles stoppen"

So gehen Sie damit um: Stellen Sie klar, dass eine qualifizierte und fundierte Einschätzung ihre Zeit braucht. Mit einer vorschnellen oder oberflächlichen Prüfung Ihrerseits ist niemandem gedient. Ob etwa ein Roll-out gestoppt wird, weil Ihre Einschätzung noch nicht vorliegt, entscheiden nicht Sie. Das ist eine unternehmerische Entscheidung. Bitten Sie darum, dass man Sie zukünftig rechtzeitig einbindet, damit ein Startdatum nicht gefährdet ist.

Die Aussage: „Wir machen das jetzt. Um den Datenschutzkram kümmern wir uns später"

So gehen Sie damit um: Zeigen Sie auf, dass ein solches Vorgehen geradezu fahrlässig ist. Vor Beginn einer Verarbeitung muss alles Erforderliche umgesetzt sein. Zum Start einer Verarbeitung muss alles passen. Ein gestuftes Vorgehen nach dem Motto „Wir starten und ziehen dann das Nötige nach" kennen weder die Datenschutz-Grundverordnung noch das Bundesdatenschutzgesetz. Datenschutzverstöße müssen von Anfang an vermieden werden.

Die Aussage: „Sie sorgen dafür, dass im Datenschutz alles passt"

So gehen Sie damit um: Stellen Sie klar, dass Sie gerade nicht der Umsetzer sind. Sie beraten und kontrollieren. Auch geben Sie gerne Hilfestellung. Das Umsetzen ist jedoch allein Sache des Unternehmens.

Muss ich bei einem konsolidierten Tätigkeitsbericht mitmachen?

FRAGE: Bei unserem Unternehmen gibt es regelmäßige Tätigkeitsberichte, etwa der Beauftragten für Compliance und Arbeitssicherheit. Auch ich als Datenschutzbeauftragter habe bislang einen eigenen Tätigkeitsbericht zum Ende des Jahres erstellt. Die Geschäftsführung fordert nun erstmalig einen konsolidierten Bericht, in dem alle Tätigkeitsberichte einheitlich dargestellt werden. Auch sollen Schlüsselthemen vorgegeben sein, die jeder Beauftragte auf das Jahr bezogen darstellen soll. Muss ich als Datenschutzbeauftragter bei einem konsolidierten Bericht mitmachen und mich mit den Kollegen abstimmen?

ANTWORT: Für betriebliche Datenschutzbeauftragte gibt es keine gesetzliche Pflicht zur Erstellung eines Tätigkeitsberichts. Dass Ihre Geschäftsführung einen Bericht einfordert, kann insbesondere folgende Gründe haben:

- **Risikomanagement:** Ihr Unternehmen muss Risikovorsorge treffen und bestehende Risiken aktiv managen, etwa zum Schutz von personenbezogenen Daten. Unter Umständen ist ein Tätigkeitsbericht eine wichtige Säule, um darauf basierend die Risiken effektiv zu steuern.
- **Informationsinteresse:** Auch wenn Sie Datenschutzbeauftragter sind, sind Sie zugleich Arbeitnehmer. Ein Arbeitgeber kann von einem Arbeitnehmer fordern, dass er einen Überblick darüber gibt, was er in seiner Arbeitszeit macht. Eine entsprechende Weisung im Sinne von § 106 Gewerbeordnung wird meist kaum zu beanstanden sein. Das vor allem dann, wenn Sie keine Dinge offenbaren, die Ihrer Pflicht zur Vertraulichkeit unterliegen.

Konsolidierter Bericht grundsätzlich kein Problem

Dem Wunsch der Geschäftsführung nach einem konsolidierten und einheitlichen Bericht sollten Sie sich nicht verweigern. Das kann der Unternehmensleitung helfen, ein Gesamtbild zu erhalten. Schließlich ist der Datenschutz nur ein Compliance-Thema unter vielen. Achten Sie bei der Abstimmung mit den Kollegen darauf, dass Ihre Vorstellungen von einem Bericht ausreichend berücksichtigt werden.

Klappt das nicht oder haben Sie vielleicht nicht genügend Platz, um alles Wichtige zu vermitteln, können Sie Folgendes machen: Sie nutzen den konsolidierten Bericht als Basis und geben eine Management Summary zum Stand der Dinge im Datenschutz. Im Bericht können Sie jedoch auf ausführliche Informationen in einem ergänzenden Bericht verweisen. Reicht Ihnen der Verweis nicht aus, können Sie den Entscheidungsträgern einen ergänzenden Bericht auch per E-Mail zukommen lassen.

Darf der Betriebsrat nur über die Personalabteilung mit mir reden?

FRAGE: Der neue Geschäftsführer hat mich und den Betriebsratsvorsitzenden angesprochen. Er will, dass der Betriebsrat zukünftig nicht mehr mit mir direkt spricht. Das soll über die Personalabteilung laufen, weil die Ansprechpartner des Betriebsrats ist. Der Betriebsratsvorsitzende und ich sind nun etwas verwirrt. Ist eine entsprechende Weisung wirklich möglich, sowohl gegenüber dem Betriebsrat als auch gegenüber mir als Datenschutzbeauftragtem?

ANTWORT: Es lässt sich darüber streiten, ob es sich um eine Weisung oder eher um einen Wunsch handelt. Wie dem auch sei – weder der Betriebsrat noch Sie müssen dem generell nachkommen. Wie so oft kommt es auf die konkrete Situation an.

Geht es etwa um Betriebsverfassungsrechtliches, etwa die Ausgestaltung einer Betriebsvereinbarung, lässt sich vertreten, dass tatsächlich die Personalabteilung Ansprechpartner für den Betriebsrat ist. Meist führt das jedoch nur zu einer zeitlichen Verzögerung. Relevante Fragen wird auch die Personalabteilung an Sie durchreichen müssen, damit Sie als Datenschutzbeauftragter Stellung nehmen. Weil Sie unabhängig und weisungsfrei sind, kann man sich diesen Umweg über die Personalabteilung ggf. auch sparen.

Geht es jedoch um Fragen des Datenschutzes beim Betriebsrat, etwa zum Umgang mit personenbezogenen Daten, Schutzmaßnahmen oder Awareness, kann sich dieser direkt an Sie wenden. Schließlich beraten Sie als Datenschutzbeauftragter alle Bereiche im Unternehmen. Da ist der Betriebsrat keine Ausnahme. Auch wenn er weitgehend autonom agieren darf, ist er Teil des Unternehmens. Doch diese Zugehörigkeit beeinträchtigt nicht seine Unabhängigkeit gegenüber dem Arbeitgeber.

ArbG: Vertrauliches im Gruppenchat kann teuer werden

Gruppenchats bei Messengern wie WhatsApp, Threema oder Signal sind beliebt, oft auch unter Kollegen im Unternehmen. Sie sind eine praktische Sache, wenn es etwa um den Austausch von Informationen geht. Und bei „privaten" Chats spielt die Datenschutz-Grundverordnung (DSGVO) keine Rolle. Ein Irrtum, wie ein Urteil des Arbeitsgerichts (ArbG) Siegburg vom 22.5.2026 (Az. 1 Ca 1741/25) zeigt.

Der Sachverhalt

Der Kläger und die spätere Beklagte waren angestellte Ärzte in einem Krankenhaus und in der Abteilung Allgemeinchirurgie tätig. Es existierte eine WhatsApp-Chatgruppe mit insgesamt neun Mitgliedern aus dieser Abteilung, darunter auch der Kläger und die Beklagte. Die Chatgruppe zielte darauf ab, Krankmeldungen, Dienstübernahmen, Urlaub, gemeinsame Feiern oder Geschenke untereinander zu organisieren.

Kläger wird krank

Weil er sich nicht wohlfühlte, suchte der Kläger am 29.5.2025 die Notaufnahme des Krankenhauses auf. Dort wurden Untersuchungen gemacht, darunter auch Laboranalysen. Zudem wurde eine Arbeitsunfähigkeitsbescheinigung bis zum 2.6.2025 ausgestellt. Der Kläger informierte die anderen Kollegen im Gruppenchat, dass er krankheitsbedingt ausfalle. Zugleich bat er die Kollegen um Vertretung.

Beklagte postet Krankheitsdetails

Am 31.5.2025 schrieb die Ärztin im Gruppenchat, dass der Erkrankte kurz vor der Krankmeldung drei Wochen in Urlaub gewesen wäre. Sie hätte alle Vertretungsdienste übernehmen und auch einen nicht angetretenen Wochenendurlaub bezahlen müssen. Die Laboruntersuchung hätte nichts ergeben. Bis auf eine Fettleber und Adipositas wäre nichts auffällig. Erst nachdem sie eine Krankmeldung gefordert hätte, wäre der Kläger in die Klinik gefahren. Auch am fraglichen Durchfall wäre nichts dran. Vielleicht säße ein Pups quer.

Der Kläger ließ das nicht auf sich sitzen. Er forderte am 25.7.2025 die Beklagte zur Abgabe einer Unterlassungserklärung auf. Im Oktober 2025 kündigte der Kläger seinen Job. Das führte er auch auf Belastungen im Team und die Verächtlichmachung im Chat zurück. Als die Ärztin keine Unterlassungserklärung abgab, kam es zur Klage vor dem ArbG.

Mann fordert Unterlassung und Entschädigung

Aus Sicht des Klägers stehe ihm zu, dass die Klägerin es unterlässt, seine personenbezogenen Gesundheitsdaten weiterzugeben. Zudem hätte er einen immateriellen Schaden erlitten, weshalb ihm nach Art. 82 Datenschutz-Grundverordnung (DSGVO) eine Zahlung von 2.000 € zu leisten wäre. Die Ärztin war sich keiner Schuld bewusst. Sie hätte sich nichts vorzuwerfen. Doch das ArbG schloss sich ihrer Sichtweise nicht an.

So entschied das ArbG

Dem Kläger steht einerseits ein Unterlassungsanspruch aus §§ 1004 Abs. 1, 823 Abs. 2 Satz 1 Bürgerliches Gesetzbuch (BGB) i. V. m. Art. 9 DSGVO zu. Andererseits besteht ein Anspruch auf Ersatz des immateriellen Schadens nach Art. 82 Abs. 1 DSGVO, jedoch nur in der Höhe von 1.000 €.

Verletzt jemand ein Gesetz, das einen anderen schützen soll, kann der Verletzte nach § 1004 BGB Unterlassung fordern. Die Beklagte hat gegen Art. 9 DSGVO verstoßen und somit gegen ein Schutzgesetz im Sinne von § 823 BGB. Die DSGVO zielt auf den Schutz natürlicher Personen bei der Verarbeitung ihrer Daten ab.

„Private Verarbeitung" unterfällt DSGVO

Die Beklagte kann sich nicht auf die Anwendungsausnahme nach Art. 2 Abs. 2 Buchst. c DSGVO berufen. Diese gilt nur für ausschließlich persönliche und familiäre Tätigkeiten. Es darf in diesem Zusammenhang keinen Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit geben. Das war jedoch im konkreten Fall gegeben. Im Chat wurden arbeitsbezogene Inhalte ausgetauscht. Es fehlt am ausschließlich persönlichen Zweck.

Ärztin ist Verantwortliche

Sie ist für die betreffende Datenübermittlung an die Chatteilnehmer datenschutzrechtlich Verantwortliche. Die Verantwortung kann nicht dem Arbeitgeber zugewiesen werden, weil die Ärztin nicht im Rahmen der ihr zugewiesenen Aufgaben handelte. Es handelt sich um einen Mitarbeiterexzess, bei dem der Mitarbeiter zum Verantwortlichen wird. Eine Berechtigung zur Verarbeitung der betreffenden Daten nach Art. 9 Abs. 2 DSGVO lag nicht vor.

Die Weitergabe der Daten führte zu einem Kontrollverlust des Klägers über seine Daten. Von einem Schaden ist auszugehen. Allerdings war nach Ansicht des Gerichts die Höhe des Schadensersatzes auf 1.000 € zu begrenzen. Zwar handelte es sich um besonders sensible Daten. Jedoch wurden keine Dokumente der Krankenakte weitergeleitet. Zudem war der Kreis der Empfänger überschaubar.

Das können Sie folgern

Sensibles im Chat unter Kollegen teilen kann nach hinten losgehen. Die Haushaltsausnahme greift seltener, als mancher denkt. Besteht ein Bezug zur Arbeit, kann man schnell zum Verantwortlichen werden und die DSGVO auch im anscheinend privaten Umfeld einhalten müssen.

PRIVACYXPERTS

IT- & INFORMATIONS-SICHERHEIT UPDATE

SICHER. AKTUELL. PRAXISNAH.

NAVIGIEREN SIE SOUVERÄN DURCH DEN DSCHUNGEL AUS IT-RECHT, CYBERSICHERHEIT UND COMPLIANCE.



CYBER COMPLIANCE-KOMPASS
24 ARBEITSHILFEN FÜR MEHR COMPLIANCE

IHR WEGWEISER FÜR COMPLIANCE, SICHERHEIT UND BUSINESS-KONTINUITÄT

Mit dem 24-teiligen Cyber-Compliance-Kompass und dem E-Magazin „IT- & Informationssicherheit Update" haben Sie das Wissen und die Werkzeuge,die Sie jetzt brauchen.

IHRE VORTEILE

Immer aktuell
Wichtige Entwicklungen und neue Richtlinien verständlich aufbereitet.

Praxisnah umsetzen
Checklisten, Vorlagen und Anleitungen direkt für Ihren Arbeitsalltag.

Über 100 Arbeitshilfen
Exklusive Inhalte im Premiumbereich – für nachhaltige Umsetzung.

Digital & mobil
Mobiloptimiert, durchsuchbar und überall verfugbar.

Webinare & Experten
Regelmäßige Live-Webinare und Aufzeichnungen mit Experten.

Mehr Sicherheit
Stärken Sie Ihre Cyber-Resilienz und erfüllen Sie alle Anforderungen.

HIGHLIGHTS AUS DEM CYBER-COMPLIANCE-KOMPASS

- E-Book: Navigieren im Dschungel des IT-Rechts
- Protokollierungskonzept IT-Systeme & Anwendungen (Excel)
- Soll-Ist Abgleich nach ISO 27001
- Checkliste: Bausteine der KRITIS Verordnung umsetzen
- Entscheidungsbaum: Ist es ein Security Incident?
- Checkliste: Uberprüfung IT-Dienstleister
- 12 Best Practices für Endpoint-Security
- Sicherheitsmaßnahmen für Outlook & Excel
- Anforderungen der Informationssicherheit an das Notfallmanagement
- Cyberversicherung-Fragenkatalog
- Mobile Device Management nach BS
- Muster-Richtlinie: Umgang mit Daten je Vertraulichkeitsklasse
- Richtlinien der Informationssicherheit (Übersicht)
- Checkliste: Cyber-Resilienz
- Checkliste: Backup-Konzept
- und viele weitere Arbeitshilfen, Vorlagen und Anleitungen ...

JETZT GRATIS TESTEN

Testen Sie das E-Magazin 30 Tage kostenlos. Inklusive Cyber-Compliance-Kompass und zahlreicher Arbeitshilfen.

https://t1p.de/it-kompass

DAS EXPERTEN TEAM AN IHRER SEITE



ANDREAS HESSEL
Chief Information Security Officer
Langjähriger Leiter Informationssicherheit Risikomanagement einer Bank. Externer Datenschutzbeauftragter und Berater für Cybersicherheit. Fachautor.



MICHAEL ROHRLICH
Rechtsanwalt
Fachautor, Dozent und Video-Trainer für IT-Recht, Datenschutz und e-Commerce. Autor fur diverse Print- und Online-Publikationen.



MARC OLIVER THOMA
IT-Sicherheitstrainer & Berater
Experte für IT-Sicherheit, Datenschutz und Kommunikation. Linkedin-Learning-Trainer und externer Datenschutzbeauftragter für KMU.

GUT INFORMIERT. PRAXISNAH. SOFORT UMSETZBAR. **www.privacyxperts.de**

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

Vorschau:

Budgetplanung 2027: Daran sollten Sie denken

5 Tipps zum Datenschutz in der Vorweihnachtszeit