DATENSCHUTZAKTUELL
APR 2026
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH

Themenheft:
Beschäftigtendatenschutz

BESCHÄFTIGTEN-DATENSCHUTZ: RECHTLICHE GRENZEN IM ARBEITSALLTAG

Schutz statt Datensammlung

Liebe Leserin, lieber Leser,

im Arbeitsverhältnis werden personenbezogene Daten nicht freiwillig, sondern aus Notwendigkeit preisgegeben. Genau dieses strukturelle Ungleichgewicht macht den Beschäftigtendatenschutz so wichtig. Personenbezogene Daten entstehen im Arbeitsalltag oft nebenbei – ohne formelle Erhebung, aber mit datenschutzrechtlicher Bedeutung.

Für Sie als Datenschutzbeauftragter zeigt dieses Themenheft anhand typischer Situationen aus dem Arbeitsalltag, wo datenschutzrechtliche Grenzen liegen – und wo sie häufig unbemerkt überschritten werden.

Viele Grüße

Dr. Anna-Kathrin Mauch,
Rechtsanwältin und Redakteurin

Ihre Expertin für Datenschutz
Dr. Anna-Kathrin Mauch ist Rechtsanwältin und Europajuristin mit Erfahrung im Vertrags- und Datenschutzrecht. Sie bringt Datenschutz verständlich und praxisnah auf den Punkt.

Inhalt

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

Expertensprechstunde:
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, Bonn

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

Produktmanagement: Franziska Rohrbach, Bonn

Autorin:
Dr. Anna-Kathrin Mauch, Rottweil

Design: Kreativ Konzept Agentur für Werbung, Bonn
Satz: Schmelzer Medien GmbH, Siegen
Druck: Warlich Druck Meckenheim GmbH,
Am Hambuch 5, 53340 Meckenheim
Bildnachweise: Titel: Adobe Stock | vegefox.com; Seite 1: Adobe Stock | deagreez

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.

Personenbezogene Daten müssen faktisch zwingend preisgegeben werden.

Freiwillig, aber nicht frei? Datenschutz im Ungleichgewicht

Datenschutz entfaltet seine Wirkung nicht nur in klassischen Vertragsverhältnissen, in denen sich die Beteiligten auf Augenhöhe begegnen – etwa beim Kaufvertrag zwischen gleichberechtigten Marktteilnehmern. Seine besondere Bedeutung zeigt sich vielmehr dort, wo ein strukturelles Ungleichgewicht besteht und personenbezogene Daten nicht freiwillig, sondern faktisch zwingend preisgegeben werden müssen.

Wo Datenschutz besonders schützt

Gerade in solchen Konstellationen übernimmt Datenschutz eine ausgeprägte Schutzfunktion. Er begrenzt nicht nur, welche Daten erhoben werden dürfen, sondern auch, zu welchen Zwecken sie verarbeitet und weiterverwendet werden können. Datenschutz wirkt hier als rechtliches Korrektiv, das Machtungleichgewichte ausgleicht und die informationelle Selbstbestimmung absichert. Maßgeblich ist dabei stets, ob die Datenverarbeitung erforderlich und verhältnismäßig ist. Typische Konstellationen, in denen Datenschutz eine ausgeprägte Schutzfunktion übernimmt, sind:

- **Arbeitnehmer und Arbeitgeber**
  Im Arbeitsverhältnis besteht regelmäßig ein deutliches Ungleichgewicht. Beschäftigte können sich der Verarbeitung ihrer personenbezogenen Daten kaum entziehen, da diese Voraussetzung für das Begründen, Durchführen und Beenden des Arbeitsverhältnisses ist. Wer arbeiten, vergütet werden und sozial abgesichert sein will, muss personenbezogene Daten offenlegen – häufig in erheblichem Umfang.
- **Patienten und medizinische Einrichtungen**
  Auch im Gesundheitswesen besteht keine Verhandlung auf Augenhöhe. Patienten müssen hochsensible Gesundheitsdaten offenlegen, um überhaupt behandelt zu werden. Die Datenverarbeitung ist zwingende Voraussetzung für die medizinische Versorgung und unterliegt daher besonders strengen datenschutzrechtlichen Anforderungen.
- **Leistungsbezieher und Sozialleistungsträger**
  Personen, die existenzsichernde Leistungen beantragen, sind darauf angewiesen, umfangreiche persönliche Informationen preiszugeben. Auch hier entsteht ein faktisches Abhängigkeitsverhältnis, das einen erhöhten Schutz personenbezogener Daten erforderlich macht.

Diese Beispiele verdeutlichen für Sie als Datenschutzbeauftragten: Datenschutz erfüllt seine Schutzfunktion insbesondere dort, wo personenbezogene Daten nicht aus freier Entscheidung, sondern im Rahmen struktureller Abhängigkeiten verarbeitet werden. Das Arbeitsverhältnis ist hierfür eines der prägnantesten Beispiele. Entsprechend kommt der Einwilligung als Rechtgrundlage im Beschäftigungsverhältnis auch nur eine eingeschränkte Bedeutung zu. Ihre Freiwilligkeit ist im Einzelfall sorgfältig zu prüfen; zudem stellt sie aufgrund ihrer jederzeitigen Widerruflichkeit eine weniger stabile Rechtsgrundlage dar.

8 typische Beispiele des Beschäftigtendatenschutzes im Arbeitsalltag

Im Arbeitsverhältnis werden personenbezogene Daten an vielen Stellen und häufig über lange Zeiträume hinweg verarbeitet. Die Verarbeitung beschränkt sich nicht auf klassische Stammdaten, sondern umfasst vielmehr auch Leistungsinformationen, Nutzungsdaten sowie zunehmend automatisierte Auswertungen. Diese Vielzahl unterschiedlicher Verarbeitungsvorgänge macht den Beschäftigtendatenschutz in der Praxis besonders komplex und fehleranfällig.

Sie als Datenschutzbeauftragter nehmen hier eine zentrale Rolle ein, indem sie zwischen rechtlichen Vorgaben und betrieblicher Umsetzung vermitteln. Für die Praxis ist es daher entscheidend,

typische Risikosituationen zu erkennen, in denen datenschutzrechtliche Fehler gehäuft auftreten und in denen gezielte Sensibilisierung, klare Vorgaben und ggf. Kontrollen erforderlich sind.

Zu den typischen Situationen im Arbeitsverhältnis zählen etwa:

1. **Begründung des Arbeitsverhältnisses: Bewerbungs- und Auswahlverfahren, digitale Profile, Assessment-Tools**
   In der Praxis zeigt sich hier früh ein erhebliches Ungleichgewicht: Schon vor Vertragsabschluss werden Entscheidungen auf Basis von Daten getroffen, ohne dass Bewerber transparent nachvollziehen oder steuern können, welche Informationen tatsächlich herangezogen werden – und ob diese überhaupt zulässig erhoben wurden.
2. **Durchführung des Arbeitsverhältnisses: Personalakten, Arbeitszeit-, Leistungs- und Verhaltensdaten**
   Aus der Praxis weiß ich, wie selbstverständlich laufende Datenerfassung zum Arbeitsalltag gehört. Problematisch wird das vor allem dann, wenn diese Daten nicht nur dokumentiert, sondern stillschweigend zur Bewertung von Leistung, Zuverlässigkeit oder „Eignung" herangezogen werden.
3. **Technische Systeme: Zeiterfassung, Kommunikationstools, Videoüberwachung sowie Zutritts- und Zugangskontrollsysteme**
   In vielen Mandaten zeigt sich, dass Unternehmen selbst den Überblick verlieren, welche Daten ihre Systeme im Hintergrund erfassen. Mitarbeitende wissen häufig nicht, in welchem Umfang solche Daten entstehen.
4. **Leistungs- und Verhaltenskontrolle: Zielvereinbarungen, KPIs, Monitoring und Auswertungen**
   Gerade hier verlaufen die meisten Streitlinien. In Gesprächen mit Mandanten wird oft deutlich, wie schnell der Übergang von zulässiger Leistungsbewertung zu faktischer Dauerüberwachung vollzogen ist – oft ohne klare Grenze oder bewusste Entscheidung.
5. **Gesundheits- und Fürsorgekontext: Krankmeldungen, betriebliches Eingliederungsmanagement, betriebsärztliche Untersuchungen**
   Aus anwaltlicher Sicht sind dies regelmäßig die sensibelsten Fälle. Ich erlebe häufig, dass gut gemeinte Fürsorgemaßnahmen datenschutzrechtlich problematisch umgesetzt werden – mit erheblichem Vertrauensverlust aufseiten der Betroffenen.
6. **Homeoffice und mobile Arbeit: Überschneidung beruflicher und privater Sphären**
   Seit der Verlagerung von Arbeit in den privaten Raum stellen sich neue Fragen: Wer hat wann Zugriff? Was wird protokolliert? Wo endet die betriebliche Kontrolle? Klare Antworten fehlen hier oft – mit entsprechenden Risiken.
7. **Automatisierte Entscheidungen und KI-Systeme: Bewerbervorauswahl, Leistungsbewertung, Personalplanung**
   In der Praxis zeigt sich, dass viele Entscheidungen als „technisch" oder „neutral" wahrgenommen werden, obwohl die dahinterliegenden Kriterien kaum nachvollziehbar sind. Gerade bei Konflikten wird deutlich, wie schwierig es ist, diese Systeme rechtlich sauber einzuordnen.
8. **Beendigung des Arbeitsverhältnisses: Kündigungen, Aufhebungsverträge, Zeugnisse, Löschpflichten**
   Erfahrungsgemäß entstehen auch noch in dieser Phase viele Fehler. Unter Zeitdruck und emotionaler Belastung wird der Datenschutz oft nachrangig behandelt – was später nicht selten zu zusätzlichen rechtlichen Auseinandersetzungen führt.

Wo ist der Beschäftigtendatenschutz geregelt?

Der Beschäftigtendatenschutz beruht aktuell auf einem Zusammenspiel aus der Datenschutz-Grundverordnung (DSGVO), § 26 Bundesdatenschutzgesetz (BDSG), kollektivrechtlichen Regelungen und der Rechtsprechung. § 26 BDSG erlaubt die Verarbeitung von Beschäftigtendaten, soweit sie für die Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses erforderlich ist. Tarifverträge sowie Betriebs- und Dienstvereinbarungen können ergänzend als Rechtsgrundlage dienen, sofern sie den Anforderungen des Art. 88 DSGVO entsprechen; bei technischen Einrichtungen mit Überwachungs- oder Kontrollpotenzial ist zudem das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz zu beachten.

Der Europäische Gerichtshof 30.3.2023, Rs. C-34/21) hat diese Rechtslage zuletzt präzisiert: Nationale Sonderregelungen zum Beschäftigtendatenschutz können nur angewendet werden, soweit sie den Vorgaben der DSGVO entsprechen. Vor diesem Hintergrund ist umstritten, in welchem Umfang § 26 BDSG noch als eigenständige Rechtsgrundlage herangezogen werden kann. Für die Praxis bedeutet das, dass Datenverarbeitungen im Arbeitsverhältnis **stets** an den Maßstäben der DSGVO auszurichten sind.

Drama ohne Ende: das Beschäftigtendatengesetz

Ein eigenständiges Beschäftigtendatengesetz war seit Jahren angekündigt, ist bislang jedoch nie Realität geworden. Zwar wurde im Oktober 2024 ein Gesetzentwurf vorgelegt, der unter anderem Regelungen zur Einwilligung, zu Löschfristen von Bewerberdaten, zur Beschäftigtenüberwachung und zur Mitbestimmung des Betriebsrats vorsah. Durch das vorzeitige Ende der Ampel-Koalition wurde das Gesetzgebungsvorhaben jedoch erneut gestoppt. Vor dem Hintergrund der aktuellen Parteiprogramme und des politischen Ziels des Bürokratieabbaus ist kurzfristig nicht mit einem neuen Anlauf zu rechnen. Für die Praxis bleibt es daher bei der Anwendung von DSGVO und § 26 BDSG.

Praktische Konsequenzen für Ihren Arbeitgeber

Aus dem strukturellen Ungleichgewicht im Arbeitsverhältnis folgt für Arbeitgeber eine besondere Verantwortung bei der Verarbeitung von Beschäftigtendaten, deren Wahrnehmung für Sie als Datenschutzbeauftragten regelmäßig Prüf- und Beratungsbedarf auslöst. Maßgeblich ist nicht, ob eine Datenverarbeitung technisch möglich oder betrieblich etabliert ist. Entscheidend ist vielmehr, ob sie rechtlich erforderlich und verhältnismäßig ist. Jede Verarbeitung von Beschäftigtendaten bedarf einer eigenständigen Prüfung darauf, ob sie tatsächlich der Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses dient oder ob weniger eingriffsintensive Alternativen zur Verfügung stehen. Dies gilt vor allem bei der Einführung neuer technischer Systeme, Kontrollinstrumente oder automatisierter Auswertungen. In diesen Fällen entstehen häufig zusätzliche, bislang nicht erhobene Beschäftigtendaten, was das Eingriffsgewicht erhöht und eine sorgfältige datenschutzrechtliche Prüfung erforderlich macht.

Weltfrauentag: besondere Schutzbedürftigkeit

Der Weltfrauentag erinnert daran, dass rechtlicher Schutz dort besonders wichtig ist, wo strukturelle Benachteiligung besteht. Im Arbeitsverhältnis betrifft dies Frauen in besonderer Weise – nicht aufgrund individueller Eigenschaften, sondern wegen typischer „Rollenbilder", Zuschreibungen und Erwartungshaltungen. Viele datenschutzrechtlich relevante Situationen entstehen dabei nicht durch formale Abfragen, sondern durch beiläufige Informationen, informelle Bewertungen und vermeintlich „bekanntes" Wissen.

Frauen im Arbeitsalltag: kritische Datensituationen

Die folgenden Beispiele zeigen Konstellationen, die im Arbeitsalltag häufig informell auftreten und datenschutzrechtlich besonders sensibel sind. Für Sie als Datenschutzbeauftragten sind sie vor allem deshalb relevant, weil hier schnell Bewertungen, Annahmen oder Dokumentationen entstehen, die keine tragfähige Rechtsgrundlage haben. Ihre Aufgabe besteht darin, diese Situationen zu erkennen, einzuordnen und durch klare Vorgaben sowie Sensibilisierung insbesondere der Personalabteilung gegenzusteuern.

Beispiel	Warum problematisch?	So geht's richtig
Schwangerschaft und Familienplanung: „Sie ist schwanger", „Sie will bald wieder in Teilzeit"	Diese Informationen betreffen sensible Lebens- und Gesundheitsumstände und bergen ein hohes Diskriminierungsrisiko. Sie ermöglichen Rückschlüsse auf künftige Verfügbarkeit oder Belastbarkeit und sind für Personalentscheidungen regelmäßig nicht erforderlich (§ 26 Bundesdatenschutzgesetz).	Nur solche Informationen verarbeiten, die für Arbeitsschutz oder konkrete organisatorische Maßnahmen erforderlich sind. Keine Weitergabe über den notwendigen Personenkreis hinaus und keine Berücksichtigung bei Leistungs-, Entwicklungs- oder Beförderungsentscheidungen.
Fehlzeiten und Care-Arbeit: „Sie fällt öfter aus", „wegen der Kinder eingeschränkt verfügbar"	Fehlzeiten erlauben mittelbare Rückschlüsse auf Gesundheit oder familiäre Situation und führen schnell zu pauschalen Zuschreibungen. Solche Bewertungen sind datenschutzrechtlich unzulässig und verstärken strukturelle Benachteiligung.	Fehlzeiten sind ausschließlich organisatorisch zu behandeln (z. B. Vertretung, Planung). Eine Bewertung von Ursachen oder eine Verknüpfung mit Leistungs- oder Zuverlässigkeitsannahmen im Rahmen von Personalentscheidungen ist unzulässig.
Teilzeit, Rückkehr, Homeoffice: „nicht voll da", „arbeitet viel von zu Hause"	Arbeitsmodelle werden informell mit Engagement oder Leistung gleichgesetzt. Sichtbarkeit tritt an die Stelle sachlicher Kriterien, ohne dass hierfür eine datenschutzrechtliche Grundlage besteht.	Leistung ausschließlich anhand arbeitsbezogener Ergebnisse bewerten. Teilzeit, Homeoffice oder Rückkehrphasen dürfen weder als Negativkriterium herangezogen noch dokumentiert werden.
Gesundheitliche Themen: Zyklusbeschwerden, Fertilität, psychische Belastungen	Es handelt sich um besondere Kategorien personenbezogener Daten (Art. 9 Datenschutz-Grundverordnung). Auch freiwillig geteilte Informationen bleiben besonders schutzbedürftig.	Keine Speicherung, keine Weitergabe und keine Nutzung für Einsatz-, Leistungs- oder Eignungsentscheidungen. Eine freiwillige Offenlegung hebt den datenschutzrechtlichen Schutz nicht auf.
Projektvergabe und „Verfügbarkeit": „für das Projekt aktuell nicht geeignet", „familiär wohl zu stark gebunden"	Projektentscheidungen beruhen auf vermuteten privaten Umständen, die weder relevant noch zulässig erhoben sind. Ziehen Arbeitgeber solche Annahmen heran, fehlt regelmäßig die Rechtsgrundlage.	Projektvergabe ausschließlich an objektive, arbeitsbezogene Kriterien knüpfen (Qualifikation, Kapazität, vertraglicher Umfang). Private Lebensumstände dürfen weder abgefragt noch stillschweigend berücksichtigt werden.

Diese Angaben sind nicht für den Arbeitgeber

Frauen sind im Arbeitsverhältnis nicht verpflichtet, Angaben zu Schwangerschaft, Familienplanung, gesundheitlichen Themen oder Care-Verpflichtungen zu machen. Ein Nachteil darf ihnen weder aus dem Schweigen noch aus einer wahrheitsgemäßen Verweigerung solcher Angaben entstehen. Entsprechende Fragen können unzulässig sein, wenn sie keinen Bezug zur Tätigkeit haben oder gegen das Benachteiligungsverbot verstoßen. Auch freiwillig mitgeteilte Informationen unterliegen dem Datenschutz und dürfen nicht für Leistungsbewertungen, Einsatzentscheidungen oder Beförderungen verwendet werden.

Fehlzeiten dürfen nicht pauschal mit Belastbarkeit, Zuverlässigkeit oder Engagement verknüpft werden. Eine solche Gleichsetzung ist rechtlich unzulässig und kann eine mittelbare Diskriminierung darstellen. Gesundheitsdaten unterliegen darüber hinaus einem besonderen Schutz und dürfen nur verarbeitet werden, soweit dies für klar definierte arbeitsrechtliche Zwecke zwingend erforderlich ist (z. B. gesetzliche Fürsorgepflicht).

Datenschutz im Bewerbungsprozess

Das Bewerbungsverfahren ist heute überwiegend digital, schneller und deutlich datengetriebener als früher. Unverändert geblieben ist jedoch eines: Bereits der Weg in ein Beschäftigungsverhältnis ist datenschutzrechtlich heikel. Arbeitgeber haben ein berechtigtes Interesse an aussagekräftigen Informationen, Bewerber dürfen aber nicht zum „gläsernen Menschen" werden. In meiner anwaltlichen Beratung berichten Mandanten immer wieder von Bewerbungsprozessen, bei denen Umfang und Tiefe der abgefragten Daten datenschutzrechtlich problematisch sind.

Informationsinteresse des Arbeitgebers – aber nicht grenzenlos

Arbeitgeber möchten verständlicherweise Informationen über fachliche Qualifikation, beruflichen Werdegang und Eignung künftiger Beschäftigter erhalten. Datenschutzrechtlich gilt jedoch ein klarer Grundsatz: Nicht alles, was aus Arbeitgebersicht interessant erscheint, darf auch erfragt werden. Denn es gilt das Erforderlichkeitsprinzip aus § 26 Bundesdatenschutzgesetz: Danach dürfen nur solche personenbezogenen Daten erhoben werden, die in einem unmittelbaren Bezug zum konkreten Stellenprofil stehen.

Arbeitsrechtlich wird der Bewerber zusätzlich durch das Fragerecht des Arbeitgebers und dessen Grenzen geschützt. Unzulässige Fragen betreffen den geschützten Persönlichkeitsbereich und müssen nicht wahrheitsgemäß beantwortet werden.

Für Sie als Datenschutzbeauftragten ergibt sich hier die Aufgabe, unzulässige oder zu weit gefasste Fragen frühzeitig zu erkennen und entsprechende Hinweise an Personalabteilung und Führungskräfte zu geben. Wer Informationen ohne klar definiertes Anforderungsprofil „auf Vorrat" erhebt, setzt sich nicht nur datenschutzrechtlichen Risiken aus, sondern läuft auch Gefahr, unzulässige Abfragen und Diskriminierungsindizien zu schaffen.

Zu viel gefragt! Unzulässige Fragen im Bewerbungsprozess

In meiner anwaltlichen Praxis erreichen mich regelmäßig Fälle, in denen Bewerber mit unzulässigen Fragen im Bewerbungsverfahren konfrontiert werden. Der erforderliche Bezug zur konkret ausgeschriebenen Stelle fehlt dabei häufig. Nicht selten werden mir Bewerber- und Personalbögen zur Prüfung vorgelegt, die darauf abzielen, möglichst viele Informationen abzufragen. Maßgeblich ist jedoch ein klarer Grundsatz: je geringer der Zusammenhang mit der Tätigkeit, desto größer das Risiko der Unzulässigkeit.

Typische Stolperfallen im Bewerbungsprozess sind:

- **Familienverhältnisse**
  Fragen nach Familienstand, Alleinerziehendenstatus oder Anzahl und Namen der Kinder sind grundsätzlich unzulässig. Nur in eng begrenzten Ausnahmefällen kann ein konkreter Tätigkeitsbezug bestehen, etwa bei unvorhersehbaren Einsätzen zu atypischen Zeiten, die objektiv eine besondere Verfügbarkeit erfordern. Auch dann ist größte Zurückhaltung geboten.
- **„Stammdaten", die in Wahrheit diskriminierungsrelevant sind**
  Kontaktdaten sind erforderlich, um Bewerber zu erreichen. Angaben wie Geburtsort, Geburtsname, Alter oder Nationalität sind dagegen regelmäßig nicht notwendig und können schnell den Verdacht einer unzulässigen Selektion oder Diskriminierung begründen. Zur Identifizierung genügt im Zweifel die Vorlage eines Ausweisdokuments – eine Kopie ist damit jedoch nicht automatisch zulässig.
- **Fahrerlaubnis**
  Die Frage nach einer Fahrerlaubnis ist nur zulässig, wenn diese für die konkrete Tätigkeit erforderlich ist, etwa bei Berufskraftfahrern oder im Außendienst. Ein pauschales Abfragen „für alle Fälle" ist unzulässig.
- **Vorstrafen und Ermittlungsverfahren**
  Es gibt keinen allgemeinen Auskunftsanspruch. Zulässig sind – wenn überhaupt – nur eng arbeitsplatzbezogene Fragen nach einschlägigen Delikten. Ein Busfahrer muss keine Auskunft über Vermögensdelikte geben, ein Bankkassierer nicht über Verkehrsdelikte. Zudem gilt: Was rechtlich nicht offenbart werden muss (z. B. tilgungsreife oder getilgte Verurteilungen), darf auch nicht mittelbar erzwungen werden.
- **Pfändungen und Lohnabtretungen**
  Fragen hierzu kommen allenfalls bei echten Vertrauenspositionen mit erheblicher Vermögensverantwortung in Betracht. Für die überwiegende Zahl „normaler" Tätigkeiten sind solche Fragen überschießend und unzulässig.
- **Gesundheitsdaten**
  Hier ist besondere Zurückhaltung geboten. Zulässig sind allenfalls Fragen, die unmittelbar die Eignung für die konkrete Tätigkeit betreffen, etwa dauerhafte oder regelmäßig wiederkehrende Einschränkungen, ansteckende Erkrankungen mit Gefährdung Dritter oder eine absehbare längere Arbeitsunfähigkeit (z. B. durch geplante Operationen). Allgemeine Gesundheitsfragen greifen unverhältnismäßig in die Intimsphäre ein.
- **Religion**
  Fragen nach der Religionszugehörigkeit sind grundsätzlich unzulässig. Eine Ausnahme kann nur bei kirchlichen oder weltanschaulich geprägten Arbeitgebern in Betracht kommen, soweit die Religionszugehörigkeit eine wesentliche und gerechtfertigte berufliche Anforderung darstellt.
- **Fehlzeiten**
  Pauschale Fragen nach früheren Krankheitszeiten oder Fehlzeiten sind unzulässig. Sie erlauben regelmäßig Rückschlüsse

auf den Gesundheitszustand und sind für die Einstellungsentscheidung nicht erforderlich. Zulässig können allenfalls tätigkeitsbezogene Fragen sein, etwa bei sicherheitsrelevanten Positionen mit besonderen Belastungsanforderungen.

- **Vermögensverhältnisse**
  Fragen nach Eigentum, Schulden oder privaten Investitionen sind in der Regel unzulässig. Nur bei besonderen Vertrauensstellungen mit erheblicher Vermögensverantwortung kann ausnahmsweise ein enger Tätigkeitsbezug bestehen. Für gewöhnliche Beschäftigungsverhältnisse sind solche Fragen überschießend.
- **Soziale Netzwerke**
  Ein pauschales Durchforsten privater Social-Media-Profile ist unzulässig. Zulässig kann allenfalls die Einsicht in berufsbezogene Netzwerke (z. B. LinkedIn) sein, sofern die Informationen öffentlich zugänglich sind und einen klaren Bezug zur beruflichen Qualifikation haben. „Recherche" im privaten Umfeld überschreitet regelmäßig die datenschutzrechtlichen Grenzen.

Speicherfristen, Talentpools und das Ende des Auswahlverfahrens

Mit Abschluss des Auswahlverfahrens entfällt grundsätzlich der Zweck der Datenverarbeitung für nicht berücksichtigte Bewerber. Bewerbungsunterlagen sind dann zu löschen oder zu vernichten. Eine kurzfristige Aufbewahrung kann jedoch gerechtfertigt sein, um Entscheidungen zu dokumentieren und sich gegen mögliche Diskriminierungsvorwürfe zu verteidigen. Dies erlaubt eine befristete, nicht jedoch eine langfristige Vorratsspeicherung.

Anders verhält es sich bei Talentpools oder Initiativbewerbungen. Eine längere Speicherung kann hier im Interesse beider Seiten liegen, setzt jedoch eine klare, informierte und jederzeit widerrufliche Einwilligung sowie eine nachvollziehbar festgelegte Speicherdauer voraus. Intransparente „automatische Verlängerungen" oder unbestimmte Kontaktaufnahmen sind datenschutzrechtlich riskant.

Praxistipp für Sie als Datenschutzbeauftragten:

Überprüfen Sie die Löschkonzepte der eingesetzten Recruiting-Systeme und achten Sie darauf, dass Bewerbungsunterlagen abgelehnter oder nicht weiter berücksichtigter Bewerber fristgerecht und automatisiert gelöscht werden. Prüfen Sie zudem, ob klare Verantwortlichkeiten für die Löschung definiert und technisch umgesetzt sind. Dokumentieren Sie die Löschfristen nachvollziehbar, um im Fall einer Prüfung durch die Aufsichtsbehörde die datenschutzkonforme Umsetzung belegen zu können.

Praxis-Check: Umgang mit Bewerbungen und Bewerberdaten

Prüffrage	Beispiel	Ja / Nein
Gibt es eine separate E-Mail-Adresse oder ein eigenes System für Bewerbungen?	Keine Bewerbungen über allgemeine Info- oder Geschäftsadressen.	○ Ja ○ Nein
Ist das Bewerbermanagement als eigene Verarbeitungstätigkeit dokumentiert?	Im Verzeichnis der Verarbeitungstätigkeiten (VVT) erfasst; Prozessbeschreibung vorhanden und aktuell.	○ Ja ○ Nein
Ist das Bewerbungs-Postfach technisch und organisatorisch abgesichert?	Passwortschutz, Zwei-Faktor-Authentifizierung, keine Sammelzugänge.	○ Ja ○ Nein
Ist der Zugriff auf Bewerbungsunterlagen klar beschränkt und dokumentiert?	Zugriff nur für definierte HR-Mitarbeiter, im Rollen- und Berechtigungskonzept festgelegt, keine pauschalen Berechtigungen.	○ Ja ○ Nein
Erfolgt eine interne Weitergabe von Bewerbungsunterlagen nur bei Erforderlichkeit?	Weiterleitung an Fachabteilungen nur zur Auswahlentscheidung.	○ Ja ○ Nein
Werden Bewerbungen nicht unkontrolliert ausgedruckt oder lokal gespeichert?	Keine privaten Ablagen, keine offenen Papierakten.	○ Ja ○ Nein
Werden standardisierte Eingangsbestätigungen mit Datenschutzhinweisen genutzt?	Automatische Antwort mit Informationen zu Zweck und Speicherdauer.	○ Ja ○ Nein
Ist in der Datenschutzerklärung ein eigenständiger Abschnitt zum Bewerbungsverfahren enthalten?	Transparente Darstellung der Verarbeitungsschritte.	○ Ja ○ Nein
Sind klare Aufbewahrungs- und Löschkonzepte für Bewerbungen festgelegt?	Zeitgesteuerte Löschung nach Abschluss des Verfahrens.	○ Ja ○ Nein
Wird die Löschung oder Vernichtung dokumentiert?	Nachvollziehbarer Löschprozess, vor allem bei ausdrücklichen Löschverlangen von Bewerbern, kein „Vergessen".	○ Ja ○ Nein
Werden Bewerbungen sicher an externe Dienstleister übermittelt, falls diese eingebunden sind?	Verschlüsselte Übertragung an Recruiter oder HR-Softwareanbieter, erforderliche Auftragsverarbeitungsverträge (AVV) liegen vor.	○ Ja ○ Nein
Wird eine ausdrückliche Einwilligung eingeholt, wenn Bewerbungen länger gespeichert werden sollen?	Talentpool nur mit informierter, widerruflicher Zustimmung.	○ Ja ○ Nein
Ist die Speicherdauer im Talentpool klar begrenzt und transparent?	Keine automatische Verlängerung ohne erneute Zustimmung.	○ Ja ○ Nein
Ist sichergestellt, dass Auskunftsbegehren von Bewerbern nach Art. 15 DSGVO fristgerecht und vollständig bearbeitet werden können?	Prozesse zur Identifikation, Zusammenstellung und Bereitstellung der erforderlichen Informationen sind definiert.	○ Ja ○ Nein

Datenschutz im laufenden Arbeitsverhältnis

Mit der Einstellung ist das Thema Datenschutz nicht erledigt – im Gegenteil. Ab diesem Moment begleitet die Datenverarbeitung den Arbeitsalltag dauerhaft. Während es im Bewerbungsverfahren um die Frage geht, *wer* eingestellt wird, geht es im laufenden Arbeitsverhältnis darum, *wie* gearbeitet wird: Arbeitszeiten, Leistung, Kommunikation, Verhalten. Die Menge der erfassten Daten wächst – und mit ihr die Möglichkeit, Arbeitsabläufe und Beschäftigte immer genauer nachzuverfolgen. Gerade deshalb muss Datenschutz im Arbeitsalltag greifen – nicht erst im Konfliktfall.

Zweckbindung statt Datensammeln „für alle Fälle"

Im laufenden Arbeitsverhältnis fallen personenbezogene Daten nahezu automatisch an: Arbeitszeiten werden erfasst, Fehlzeiten dokumentiert, Leistungsdaten ausgewertet, Kommunikation gespeichert. Datenschutzrechtlich gilt jedoch auch hier der zentrale Grundsatz: Daten dürfen nur für einen klar bestimmten, legitimen Zweck verarbeitet werden.

§ 26 Bundesdatenschutzgesetz erlaubt die Verarbeitung von Beschäftigtendaten, vor allem soweit sie für die Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses erforderlich ist. In der anwaltlichen Praxis zeigt sich jedoch immer wieder, dass dieser Maßstab deutlich enger ist, als er im Arbeitsalltag häufig verstanden wird. Er rechtfertigt keine Vorratsspeicherung und keine „vorsorgliche" Datenerhebung für unbestimmte spätere Zwecke. Gerade Maßnahmen mit Kontroll- oder Überwachungscharakter bedürfen einer besonders sorgfältigen datenschutzrechtlichen Begründung.

Typische Datenverarbeitungen – und ihre Grenzen

Für Sie als Datenschutzbeauftragten zeigen sich im Arbeitsalltag gerade in diesen Bereichen typische Konstellationen, in denen die Grenzen zulässiger Datennutzung besonders deutlich werden:

- **Arbeitszeit und Anwesenheit**
  Die Erfassung von Arbeitszeiten ist zur Abrechnung und Einhaltung arbeitsrechtlicher Pflichten zulässig. Problematisch wird es, wenn Zeiterfassungssysteme Bewegungsprofile, Standortdaten oder detaillierte Verhaltensanalysen ermöglichen, ohne dass hierfür ein sachlicher Anlass oder eine rechtliche Grundlage besteht.
- **Leistungs- und Verhaltensdaten**
  Leistungsbewertungen sind zulässig, wenn sie sachlich, transparent und klar arbeitsbezogen sowie nachvollziehbar ausgestaltet sind. Unzulässig sind verdeckte Leistungsüberwachungen oder dauerhaft angelegte Auswertungen, die Beschäftigte unter einen ständigen Beobachtungs- und Rechtfertigungsdruck setzen.
- **Kommunikation und IT-Nutzung**
  Dienstliche E-Mail-Accounts und IT-Systeme dürfen aus organisatorischen und sicherheitsbezogenen Gründen administriert werden. Eine anlasslose oder inhaltsbezogene Durchsicht von Kommunikationsinhalten ist jedoch unzulässig. Wird private Nutzung – ausdrücklich oder stillschweigend – gestattet, erhöht sich das datenschutzrechtliche Schutzniveau deutlich, insbesondere im Hinblick auf Vertraulichkeit und Zugriffsbeschränkungen.
- **Gesundheitsdaten**
  Auch im bestehenden Arbeitsverhältnis gelten strenge datenschutzrechtliche Maßstäbe. Zulässig sind nur solche Angaben, die für konkrete arbeitsrechtliche Maßnahmen unmittelbar erforderlich sind, etwa zur Beurteilung der Einsatzfähigkeit oder zur Umsetzung von Arbeitsschutzpflichten. Informationen darüber hinaus – insbesondere Diagnosen, Krankheitsursachen oder detaillierte Behandlungsverläufe – gehen regelmäßig über das zulässige Maß hinaus und sind datenschutzrechtlich nicht gerechtfertigt.
- **Fehlzeiten und Rückkehrgespräche**
  Fehlzeiten sind arbeitsorganisatorisch relevant, berühren aber regelmäßig sensible Gesundheitsdaten. Führungskräfte dürfen im Rückkehrgespräch klären, ob die Arbeitsfähigkeit wieder besteht und ob Anpassungen des Einsatzes erforderlich sind. Unzulässig sind Fragen nach Diagnosen, Krankheitsursachen oder persönlichen Hintergründen. Beschäftigte müssen solche Angaben nicht machen; freiwillige Informationen dürfen nicht dokumentiert oder für Leistungs- oder Verhaltensbewertungen verwendet werden.

Homeoffice-Status in Microsoft Teams

Ab 2026 plant Microsoft, in Teams automatisch anzuzeigen, ob Beschäftigte aus dem Büro oder dem Homeoffice arbeiten. Die Erkennung erfolgt über das Unternehmens-WLAN (SSID): Ist ein Gerät mit dem hinterlegten Netzwerk verbunden, wird der Status entsprechend gesetzt. Eine dauerhafte Geolokalisierung ist laut Microsoft nicht vorgesehen; die Funktion soll nicht heimlich aktiviert werden und erfordert eine Entscheidung des Unternehmens. Auch diese Information erlaubt Rückschlüsse auf das Arbeitsverhalten und birgt Kontrollpotenzial. Die Zulässigkeit hängt von Zweckbindung, Transparenz und ggf. Freiwilligkeit ab. Für Sie als Datenschutzbeauftragten besteht hier vor allem die Aufgabe, eine Nutzung zu Kontroll- oder Überwachungszwecken auszuschließen und klare interne Regelungen sicherzustellen. Besteht ein Mitbestimmungsrecht, ist eine Betriebsvereinbarung erforderlich. Fehlen Zweckbindung oder freiwillige Zustimmung, drohen Verstöße gegen die Datenschutz-Grundverordnung (DSGVO) und Arbeitsrecht.

Was passiert mit Beschäftigtendaten nach Beendigung des Arbeitsverhältnisses?

Nach Beendigung des Beschäftigungsverhältnisses gilt der Grundsatz der DSGVO: Personenbezogene Daten sind zu löschen, sobald sie für ihre ursprünglichen Zwecke nicht mehr erforderlich sind. Als Datenschutzbeauftragter sollten Sie darauf hinwirken, verbindliche Löschfristen in einem strukturierten Löschkonzept festzulegen und umzusetzen. Eine befristete Weiterverarbeitung ist zulässig, soweit Daten noch für arbeitsrechtliche Auseinandersetzungen (z. B. Kündigungsschutzklagen), nachvertragliche Pflichten oder zur Erfüllung gesetzlicher Nachweispflichten benötigt werden. Darüber hinaus können gesetzliche Aufbewahrungspflichten eine längere Speicherung rechtfertigen, etwa für Entgeltunterlagen, steuerlich relevante Dokumente oder Unterlagen zur betrieblichen Altersversorgung.

Nach Ablauf der jeweiligen Fristen sind die Daten datenschutzkonform zu löschen oder zu vernichten. Die Löschung ist zu dokumentieren und so umzusetzen, dass ein unbefugter Zugriff ausgeschlossen ist.

Achtung: Auch „harmlose" Personaldaten müssen gelöscht werden

Das Arbeitsgericht Neuruppin hat mit Urteil vom 14.12.2021 (Az. 2 Ca 554/21) entschieden, dass selbst scheinbar unkritische Angaben ehemaliger Beschäftigter – etwa Name und Funktion auf der Unternehmenswebsite – unverzüglich zu entfernen sind, sobald kein aktueller Bezug mehr besteht. Eine fortgesetzte Veröffentlichung ohne Rechtsgrundlage kann Schadensersatz nach Art. 82 DSGVO auslösen. Für Unternehmen bedeutet das: Löschpflichten betreffen nicht nur Personalakten, sondern auch Websites, Intranets, Organigramme und Kommunikationsarchive.

Praxis-Checkliste: Beschäftigtendaten im laufenden Arbeitsverhältnis

Prüffrage	Beispiel/Konkretisierung	Ja / Nein
Sind alle verarbeiteten Beschäftigtendaten einem klar definierten Zweck zugeordnet?	Arbeitszeiten zur Abrechnung, Leistungsdaten zur Funktionsbewertung.	○ Ja ○ Nein
Gibt es im Verzeichnis von Verarbeitungstätigkeiten Verarbeitungen, die Beschäftigtendaten betreffen?	Alle relevanten Datenarten, Zwecke, Rechtsgrundlagen dokumentiert.	○ Ja ○ Nein
Sind Verantwortlichkeiten für den Datenschutz klar geregelt?	Zuständigkeiten für Verarbeitung, Löschung, Auskunft etc. definiert.	○ Ja ○ Nein
Sind technische und organisatorische Maßnahmen (TOM) dokumentiert und umgesetzt?	Zugriffsschutz, Verschlüsselung, Passwortregeln etc.	○ Ja ○ Nein
Werden Zugriffsrechte beschränkt und regelmäßig überprüft?	Nur befugte Personen in HR/Admin zugänglich.	○ Ja ○ Nein
Sind Datenverarbeitungen mit erhöhter Risikoeinschätzung bewertet?	Z. B. Gesundheitsdaten, Standortdaten, KI-Analysen.	○ Ja ○ Nein
Wird bei Einsatz von automatisierten oder algorithmischen Systemen sichergestellt, dass eine menschliche Kontrolle besteht?	Entscheidungsverfahren überprüfbar, nicht rein autonom.	○ Ja ○ Nein
Besteht eine Betriebsratsbeteiligung bei Systemen mit Überwachungscharakter?	Zeiterfassung, IT-Monitoring, Video.	○ Ja ○ Nein
Werden Beschäftigte transparent über die Datenverarbeitung informiert?	Datenschutzinformationen, Zweck, Rechte.	○ Ja ○ Nein
Haben Beschäftigte einfachen Zugang zu Auskunft, Berichtigung, Löschung ihrer Daten?	Prozesse zur Rechtsausübung eingerichtet.	○ Ja ○ Nein
Gibt es klar geregelte Löschfristen und -prozesse auch für laufende Daten?	Daten werden gelöscht, sobald Zweck entfällt.	○ Ja ○ Nein
Werden Gesundheitsdaten nur in dem Umfang verarbeitet, der für den Arbeitsplatz nötig ist?	Diagnosen werden nicht gespeichert, nur Arbeitsfähigkeit.	○ Ja ○ Nein
Werden Daten über Fehlzeiten und Abwesenheiten nicht für pauschale Leistungsbewertungen genutzt?	Keine Korrelation mit persönlichem Leistungsverhalten.	○ Ja ○ Nein
Sind Kontrollmaßnahmen im IT-Bereich datenschutzgerecht geregelt?	Keine anlasslose Durchsicht von Kommunikationsdaten.	○ Ja ○ Nein
Gibt es eine regelmäßige Datenschutz-Schulung für Beschäftigte und Verantwortliche?	Mindestens jährliche Sensibilisierung.	○ Ja ○ Nein
Werden technische Risiken bei mobiler Arbeit/Homeoffice adressiert?	VPN, sichere Endgeräte, klar definierte Homeoffice-Regeln.	○ Ja ○ Nein
Sind Prozesse bei Datenschutzverletzungen/Incident Response definiert?	Meldewege, Fristen, Dokumentation.	○ Ja ○ Nein
Gibt es eine gültige Rechtsgrundlage für jede Verarbeitung (z. B. Vertrag, Gesetz, berechtigtes Interesse)?	Ohne Rechtsgrundlage erfolgt keine Verarbeitung.	○ Ja ○ Nein
Werden Auftragsverarbeiter (z. B. HR-Software, Cloud-Dienste) datenschutzrechtlich geprüft?	AVV vorhanden, Sicherheitsstandards geprüft, Drittstaatsübermittlung besonders abgesichert (z.B. SCC, TIA).	○ Ja ○ Nein
Ist der Einsatz von HR-Software DSGVO-konform implementiert?	Datenschutz-Folgenabschätzung, Zugriffsrechte, Updates.	○ Ja ○ Nein

Wenn Mitarbeitende selbst posten, erzählen und teilen

Was gilt eigentlich, wenn Arbeitnehmer selbst Daten über sich oder ihre Arbeit teilen? Soziale Netzwerke, Messenger oder Team-Chats machen das Teilen von Informationen einfach. Oft geschieht es beiläufig – ein Foto aus dem Büro, ein Kommentar zum Arbeitsalltag oder ein Beitrag über ein Projekt. Darf das Unternehmen diese Daten einfach nutzen? Nicht automatisch.

Freiwillig heißt nicht folgenlos

Dass Beschäftigte Informationen selbst veröffentlichen, ändert nichts an ihrer rechtlichen Einordnung. Auch öffentlich zugängliche Inhalte bleiben personenbezogene Daten und unterliegen den datenschutzrechtlichen Vorgaben. Für Arbeitgeber bedeutet das: Sie bleiben an Zweckbindung, Erforderlichkeit und eine tragfähige Rechtsgrundlage gebunden – unabhängig vom verwendeten Kanal. Maßgeblich ist nicht die Offenheit der Information, sondern der konkrete Verarbeitungszweck. Die öffentliche Sichtbarkeit allein begründet keine freie Nutzungsmöglichkeit. Solche Informationen dürfen insbesondere nicht ohne klar definierten Zweck weiterverarbeitet werden, etwa zur Leistungsbewertung, zur Erstellung interner Profile oder als Grundlage personalbezogener Entscheidungen. Zugleich kann eine freiwillige Veröffentlichung auch zur unbeabsichtigten Offenlegung von Geschäftsgeheimnissen oder vertraulichen Informationen führen. In diesen Fällen darf der Arbeitgeber anlassbezogen prüfen, ob Schutzmaßnahmen erforderlich sind; eine dauerhafte Beobachtung ist damit jedoch nicht verbunden.

Soziale Netzwerke: öffentlich, aber nicht grenzenlos

Soziale Netzwerke spielen bei der Selbstdatenpreisgabe eine zentrale Rolle. Mitarbeitende teilen dort berufliche Erfolge, Arbeitsorte oder Einblicke in ihren Arbeitsalltag, wovon auch Arbeitgeber etwa durch Reichweite, Außenwirkung oder Recruiting profitieren können. Gleichzeitig gilt: Solche Inhalte werden dadurch nicht automatisch zu HR-Daten. Ein systematisches Beobachten oder Auswerten von Social-Media-Aktivitäten ist nur in engen Grenzen zulässig und setzt einen konkreten Zweck sowie Transparenz voraus.

Für Datenschutzbeauftragte ergibt sich daraus ein klarer Praxisauftrag: Neben der datenschutzrechtlichen Einordnung freiwillig geteilter Informationen sollten Sie auf präventive Sensibilisierung setzen. Klare Social-Media-Leitlinien und regelmäßige Awareness-Maßnahmen helfen, Datenschutzverstöße zu vermeiden und Mitarbeitende dafür zu sensibilisieren, dass auch Firmeninterna oder vertrauliche Informationen nicht unbeabsichtigt öffentlich zugänglich gemacht werden.

Wenn Mitarbeitende selbst Informationen preisgeben – Leitlinien für Arbeitgeber

Regel 1: Freiwillige Offenlegung begründet kein Verwertungsrecht

Teilen Mitarbeitende Informationen freiwillig in sozialen Netzwerken, im Intranet oder in internen Tools, bedeutet dies nicht, dass diese Inhalte ohne Weiteres weiterverarbeitet werden dürfen. Allein die Tatsache, dass Informationen sichtbar oder zugänglich sind – ob öffentlich oder unternehmensintern –, stellt keine datenschutzrechtliche Erlaubnis dar. Weder die Speicherung noch eine Nutzung für Zwecke der Personalsteuerung, Leistungsbewertung oder Entscheidungsfindung lassen sich hierauf stützen.

Regel 2: Selbstdatenpreisgabe ersetzt keine Rechtsgrundlage

Auch selbst veröffentlichte oder intern geteilte Informationen dürfen nicht ohne eine eigenständige datenschutzrechtliche Rechtsgrundlage dokumentiert, ausgewertet oder in Personalakten übernommen werden. Dies gilt unabhängig vom Kommunikationskanal. Besonders sensibel ist der Umgang mit Angaben zu Gesundheit, Belastung, privaten Umständen oder persönlichen Einstellungen, da hier regelmäßig erhöhte rechtliche Anforderungen bestehen und eine Verarbeitung nur in eng begrenzten Ausnahmefällen zulässig ist.

Regel 3: Keine Schlussfolgerungen aus Offenheit ziehen

Aus freiwilligen Beiträgen von Beschäftigten dürfen keine Rückschlüsse auf Leistungsfähigkeit, Loyalität, Belastbarkeit oder persönliche Eignung gezogen werden. Offenheit oder Zurückhaltung im Umgang mit eigenen Informationen sind kein sachlicher Maßstab für Bewertungen. Entsprechende Annahmen dürfen weder positiv noch negativ in Personalentscheidungen oder Beurteilungen einfließen.

Regel 4: Klare Trennung zwischen Kommunikation und Personalverwaltung

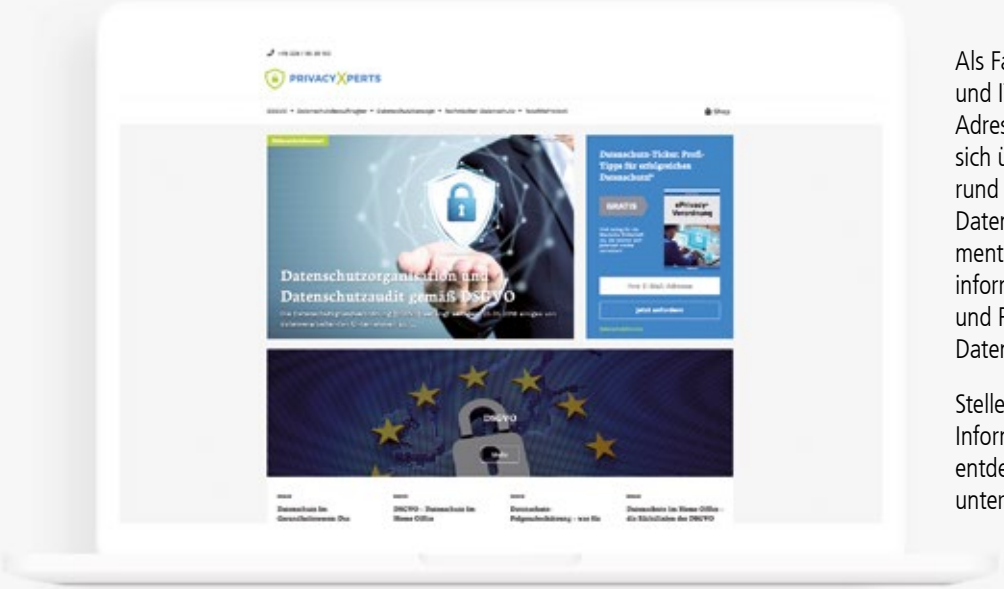
Beiträge, Kommentare, Likes oder Chatnachrichten sind primär Kommunikationsinhalte und keine Personal- oder HR-Daten. Sie dürfen daher nicht gesammelt, systematisch ausgewertet oder mit anderen Informationen verknüpft werden, um Profile zu erstellen oder Rückschlüsse auf Beschäftigte zu ziehen. Dies gilt auch für technisch automatisierte Auswertungen „im Hintergrund". Eine Zweckverschiebung von Kommunikation hin zur Personalverwaltung ist datenschutzrechtlich unzulässig.

Regel 5: Schutzpflicht statt Kontrollrecht

Arbeitgeber haben nicht das Recht, ihre Beschäftigten zu überwachen oder zu bestrafen, weil sie persönliche Informationen selbst weitergeben. Stattdessen haben sie eine Schutzaufgabe gegenüber ihren Beschäftigten. Dazu gehört, Mitarbeitende für die Reichweite, die Dauerhaftigkeit und mögliche Missverständnisse digitaler Inhalte zu sensibilisieren.

Hilfreich sind Aufklärung, Prävention und klare interne Regeln – nicht Kontrolle oder nachträgliche disziplinarische Maßnahmen.

„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

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