Personalrat aktuell

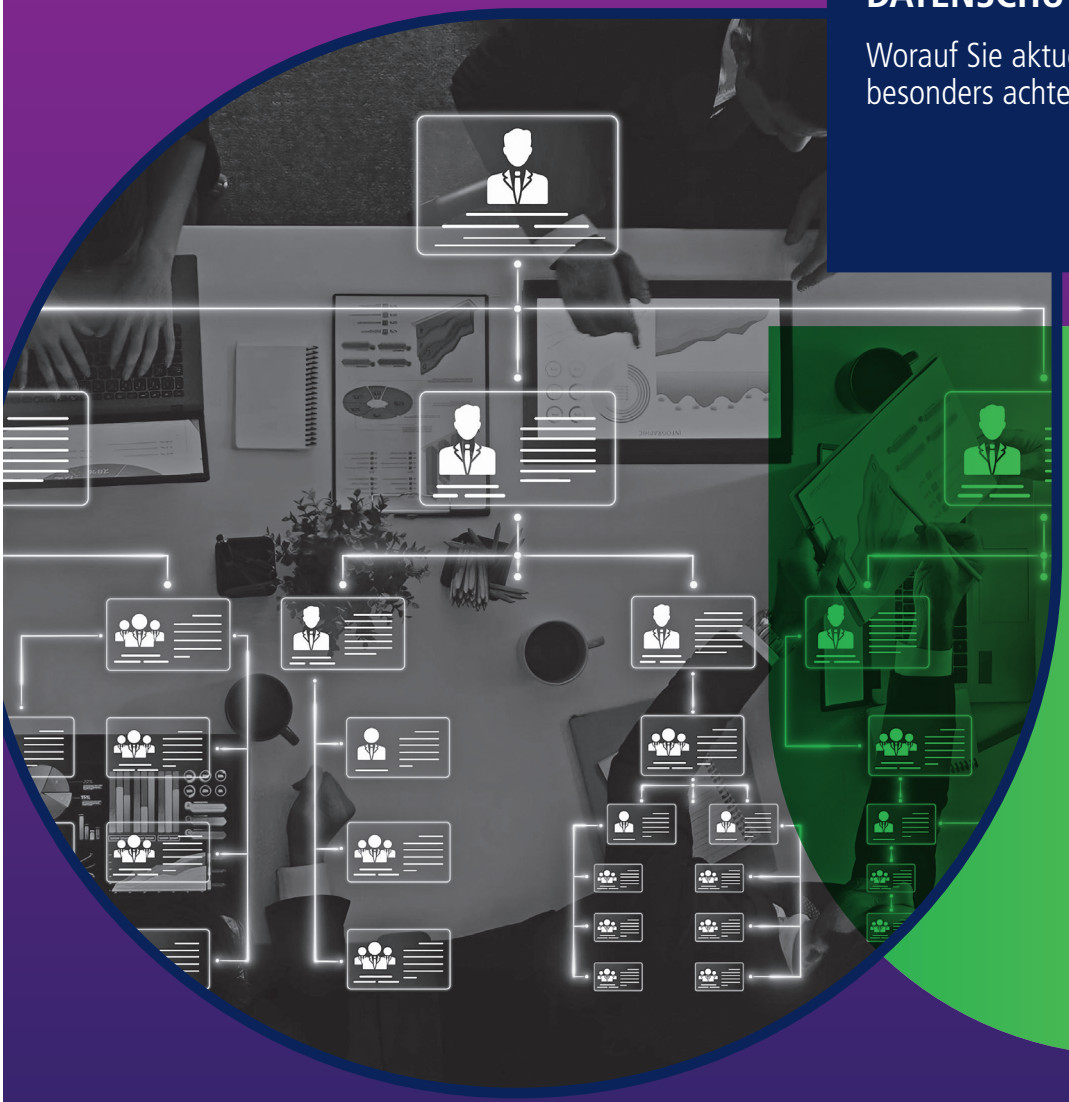
kompakt | konkret | rechtssicher

BEWÄHRTE 20 JAHRE QUALITÄT

SONDERAUSGABE:

DATENSCHUTZ 2026

Worauf Sie aktuell im Datenschutz besonders achten sollten



PERSONALRATSBÜRO

Nicht nur Ihr Dienstherr ist in Sachen Datenschutz gefordert, sondern auch das Personalratsgremium

SONDERAUSGABE SEPTEMBER 2026

ADIUVA



Maria Markatou

studierte Rechtswissenschaften in München und ist seit 2004 als Rechtsanwältin zugelassen. Sie ist mit eigener Kanzlei in München tätig. Ihre Tätigkeitsschwerpunkte liegen im Arbeitsrecht und hier in der Beratung und Vertretung von Arbeitnehmerinnen und Arbeitnehmern sowie Personalräten. Sie ist bereits seit dem Jahr 2005 Chefredakteurin von „Personalrat aktuell".

Editorial

Liebe Personalrätin, lieber Personalrat,

personenbezogene Daten begleiten uns jeden Tag – im Arbeitsalltag und natürlich auch bei Ihrer Gremiumsarbeit. Der Schutz dieser Daten ist deshalb nicht nur eine gesetzliche Verpflichtung, sondern vor allem auch eine Frage des Vertrauens. Gerade dort, wo sensible Informationen über Beschäftigte verarbeitet werden, muss besonders sorgfältig mit diesen Daten umgegangen werden. Die Datenschutz-Grundverordnung (DSGVO) setzt hierfür klare Maßstäbe.

Auch Sie tragen Verantwortung. Gleichzeitig ist Datenschutz kein Instrument, um berechtigte Informations- und Beteiligungsrechte Ihres Gremiums einzuschränken. Beides muss Hand in Hand gehen: der Schutz persönlicher Daten und eine wirksame Interessenvertretung der Beschäftigten.

In dieser Ausgabe schauen wir deshalb genauer hin: Was bedeutet die DSGVO für Ihre Arbeit? Welche Rechte haben Beschäftigte? Und worauf sollten Sie als Personalrat beim Umgang mit Unterlagen achten?

Datenschutz funktioniert am besten, wenn er nicht als lästige Pflicht verstanden wird, sondern als Bestandteil einer vertrauensvollen und respektvollen Arbeitskultur.

Maria Markatou

Chefredakteurin

Inhalt

GRUNDLAGEN
Datenschutz steht auf europäischen Füßen 3

ALLGEMEINES
Die 5 wichtigsten Säulen der DSGVO für Ihre Arbeit 4

AMTSFÜHRUNG
Personalratsdaten: Datenschutz gilt auch im Personalratsbüro 5

SCHWERPUNKTTHEMA
Diese Daten dürfen Sie im Gremium für Ihre Arbeit erheben..... 6+7

RECHTSPRECHUNG
BAG: Der Personalratsvorsitzende als Datenschutzbeauftragter?..... 8

VG Ansbach: Informationsanspruch: Sie müssen nicht alles wissen 9

BAG: Präklusion: Diese Auswirkung hat eine unzulässige Datenerhebung im Prozess 10

LAG, BGH, BAG: Auskunftsanspruch: Warum Sie Ihren Dienstherrn nach Ihren Daten fragen sollten..... 11

HÄTTEN SIE'S GEWUSST?
Whistleblowing: Datenschutz erfordert Hinweisgeberschutz – so reden Sie mit 12

Impressum: Personalrat aktuell

ADIUVA – ein Unternehmensbereich des VNR Verlags für die Deutsche Wirtschaft AG, Theodor-Heuss-Str. 2–4, 53177 Bonn | Telefon: 0228 9550160 | Fax: 0228 3696480 | ISSN: 1861-1265 | **Vorstand:** Richard Rentrop, Michael Schrader, Bonn | **Herausgeberin:** Dilan Wartenberg, verantwortlich, Adresse siehe oben | **Chefredakteurin:** Maria Markatou, RAin, München | **Produktmanagement:** Lisa Vogl, Bonn | **Lektorat:** Ulrike Floßdorf, Oberdürenbach | **Satz:** Schmelzer Medien GmbH, Siegen | **Gestaltung:** Nina Probst, Projektmanagement für Marketing & Kommunikation | **Bildrechte:** S. 1: InfiniteFlow; S. 9: Ferry; S. 12: DDRockstar – alle AdobeStock | **Druck:** Warlich Druck Meckenheim GmbH, Am Hambuch 5, 53340 Meckenheim | **Erscheinungsweise:** 24 x pro Jahr | Alle Angaben in „Personalrat aktuell" 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. | Dieses monothematische Supplement „Datenschutz 2026" liegt der Ausgabe 18 | SEPTEMBER II 2026 von „Personalrat aktuell" bei. | Dieses Produkt besteht aus FSC®-zertifiziertem Papier. |

© 2026 by ADIUVA, Bonn, Berlin, Bukarest, Jacksonville, Manchester, Passau, Warschau, HRB 8165

| E-Mail (Redaktion): markatou@mitbestimmung-heute.de | E-Mail (Kundenservice): service@adiuva.de | Internet: www.adiuva.de

DSGVO | Lesezeit 3 Minuten

Datenschutz steht auf europäischen Füßen

Der Schutz unserer Beschäftigtendaten ist längst kein rein nationales Thema mehr. Was der Dienstherr mit personenbezogenen Daten seiner Beschäftigten tun darf, welche Informationen er erheben, speichern oder weitergeben kann und welche Rechte Beschäftigte dabei haben, wird maßgeblich durch das europäische Datenschutzrecht geprägt. Für Sie als Personalrat ist es deshalb wichtig, die europarechtlichen Grundlagen des Beschäftigtendatenschutzes zu kennen und bei Ihrer täglichen Arbeit einzubeziehen.

Die DSGVO

Die Datenschutz-Grundverordnung (DSGVO) gilt in allen Mitgliedstaaten der Europäischen Union unmittelbar und sie setzt hohe, verbindliche Standards für den Umgang mit personenbezogenen Daten. Dabei geht es nicht nur um klassische Personaldaten wie Name, Anschrift, Besoldung oder dienstliche Beurteilungen. Auch Daten aus digitalen Personalakten, Zeiterfassungssystemen, E-Mail- und Kommunikationssystemen, Bewerbungsverfahren oder technischen Überwachungsinstrumenten können dem Beschäftigtendatenschutz unterliegen.

Für Sie bedeutet das: Datenschutz ist ein wesentlicher Bestandteil der Interessenvertretung. Immer dann, wenn der Dienstherr neue Systeme einführen, Daten auswerten oder Beschäftigtendaten verarbeiten möchte, sollten Sie genau hinsehen. Welche Daten werden erhoben? Zu welchem Zweck? Wer erhält Zugriff? Wie lange werden die Daten gespeichert? Und vor allem: Ist die Verarbeitung überhaupt rechtlich zulässig und verhältnismäßig?

MEIN TIPP

Fragen Sie nach

Reagieren Sie nicht erst, wenn ein neues System bereits eingeführt werden soll. Fragen Sie frühzeitig nach: Welche Beschäftigtendaten werden verarbeitet, zu welchem Zweck und auf welcher Rechtsgrundlage? So erhalten Sie rechtzeitig alle Informationen, die Sie benötigen.

Sie sollten von Anfang an dabei sein

Gerade mit der zunehmenden Digitalisierung der öffentlichen Verwaltung gewinnen diese Fragen an Bedeutung. Elektronische Personalakten, digitale Zeiterfassung, Videoüberwachung, automatisierte Auswertungen und der Einsatz künstlicher Intelligenz können erhebliche Auswirkungen auf die Persönlichkeitsrechte der Beschäftigten haben. Als Personalrat sollten Sie deshalb nicht erst dann aufmerksam werden, wenn Datenschutzprobleme bereits entstanden sind. Beschäftigtendatenschutz gehört von Anfang an auf die Tagesordnung der Personalratsarbeit.

Wichtig ist dabei auch, Datenschutzrecht und Personalvertretungsrecht zusammenzudenken. Der Dienstherr kann sich nicht allein darauf berufen, dass eine bestimmte Datenverarbeitung datenschutzrechtlich zulässig ist. Je nach Maßnahme können zusätzlich Beteiligungsrechte des Personalratsgremiums bestehen. Deshalb lohnt sich bei neuen digitalen Verfahren oder technischen Einrichtungen immer ein genauer Blick auf beide Rechtsbereiche.

Diese Ausgabe gibt Ihnen einen Überblick darüber, welche europarechtlichen Vorgaben für den Beschäftigtendatenschutz gelten, welche Bedeutung die DSGVO für das Dienstverhältnis hat und welche Rechte und Handlungsmöglichkeiten Sie als Personalrat besitzen. Beschäftigtendatenschutz ist kein Randthema. Er schützt die Persönlichkeitsrechte der Beschäftigten und gehört damit zum Kern einer verantwortungsvollen Personalratsarbeit.

MEIN TIPP

Zulässigkeit schließt Mitbestimmung nicht aus

Auch wenn eine Datenverarbeitung datenschutzrechtlich zulässig ist, heißt das nicht, dass Sie nicht mitbestimmen. Datenschutzprüfung und Beteiligung des Personalrats sind daher 2 Seiten derselben Medaille. Auch bei offensichtlicher Wirksamkeit bestimmen Sie mit.

Dabei geht es für Sie als Personalrat nicht darum, selbst zum Datenschutzexperten zu werden. Entscheidend ist vielmehr, die richtigen Fragen zu stellen und datenschutzrechtliche Risiken frühzeitig zu erkennen. Gerade bei neuen digitalen Verfahren sollten Sie sich die vorgesehenen Datenverarbeitungen und deren Zweck erläutern lassen. Auch die Frage, ob wirklich alle erhobenen Daten erforderlich sind oder ob weniger eingriffsintensive Lösungen möglich wären, gehört zur Prüfung. So können Sie die Interessen der Beschäftigten wirksam vertreten und zugleich dazu beitragen, dass Datenschutz nicht erst nach einer Einführung, sondern bereits bei der Planung einer Maßnahme berücksichtigt wird.

Nicht alles, was technisch möglich ist, ist auch datenschutzrechtlich zulässig. Die zunehmenden Möglichkeiten digitaler Systeme dürfen nicht dazu führen, dass immer mehr Daten über Beschäftigte gesammelt werden. Für Sie als Personalrat stellt sich deshalb immer auch die Frage nach der Verhältnismäßigkeit.

FAZIT

Schutz geht auch modern

Moderne und digitale Arbeitsverfahren können sinnvoll und entlastend sein. Sie müssen jedoch so gestaltet werden, dass sie die Persönlichkeitsrechte der Beschäftigten stets wahren. Sie als Personalrat sollten deshalb Digitalisierung konstruktiv begleiten, aber kritisch prüfen, wo Grenzen erreicht werden. Gerade darin liegt eine wichtige Aufgabe Ihrer Interessenvertretung.

DSGVO | Lesezeit 3 Minuten

Die 5 wichtigsten Säulen der DSGVO für Ihre Arbeit

Die Datenschutz-Grundverordnung (DSGVO) gewährt Personen diverse „Grundrechte“ und erlegt umgekehrt den Verantwortlichen diverse „Grundpflichten“ auf. Diese grundsätzlichen Rechte und Pflichten könnte man auch als Grundpfeiler bezeichnen. Einige der wichtigsten Grundpfeiler stelle ich nachfolgend dar.

Säule 1: Allgemeine Anforderungen (Art. 12)

Die DSGVO stellt zunächst einige allgemeine Anforderungen auf:

- Die Übermittlung von Informationen hat in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ zu erfolgen (Art. 12 Abs. 1 Satz 1 DSGVO).
- Verlangte Informationen sind „unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags“ zur Verfügung zu stellen (Art. 12 Abs. 3 DSGVO).
- Eine Begründung ist bei der Geltendmachung von Ansprüchen nicht erforderlich (Art. 12 Abs. 5 DSGVO).

Säule 2: Informationspflichten (Art. 13, 14)

Wenn personenbezogene Daten entweder bei der betroffenen Person oder auch anderweitig erhoben werden, löst dies zahlreiche Informationspflichten gemäß Art. 13, 14 DSGVO aus, denen der Verantwortliche nachzukommen hat. Verantwortlich ist im Bereich der Dienstherr. Der Dienstherr hat den Mitarbeitern unter anderem mitzuteilen:

- Name und Kontaktdaten der Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten
- Zweck und Rechtsgrundlage der Datenverarbeitung
- Dauer der Speicherung oder Kriterien für die Dauer der Speicherung
- Informationen über diverse Rechte der Mitarbeiter wie Auskunftsrecht, Recht auf Löschung, Widerspruchsrecht
- Information über Beschwerderecht bei der Behörde

Wenn die Daten nicht bei der betroffenen Person erhoben werden, hat der Verantwortliche insbesondere noch mitzuteilen, aus welcher Quelle die Daten stammen.

Säule 3: Auskunftsrecht (Art. 15)

Der betroffene Mitarbeiter hat zudem ein Auskunftsrecht gemäß Art. 15 DSGVO bezüglich zahlreicher Punkte, insbesondere über:

- die Frage, ob personenbezogene Daten verarbeitet wurden
- den Zweck der Verarbeitung
- die Dauer der Speicherung oder Kriterien für die Dauer der Speicherung
- das Beschwerderecht bei der Aufsichtsbehörde
- alle verfügbaren Informationen über die Quelle der Daten, wenn die Daten nicht bei den betroffenen Mitarbeitern erhoben wurden

Säule 4: Recht auf Löschung (Art. 17)

Was nicht mehr gebraucht wird, muss entsorgt werden. Niemand soll unnötig Daten „horten“ dürfen. Daher kann der Mitarbeiter vom Dienstherrn nach Art. 17 DSGVO die Löschung der über ihn gespeicherten Daten verlangen, insbesondere wenn

- die Daten für den angestrebten Zweck nicht mehr notwendig sind,
- der Mitarbeiter seine Einwilligung widerrufen hat und es keine sonstige Rechtsgrundlage für die Verarbeitung gibt,
- die Daten unrechtmäßig verarbeitet wurden.

Säule 5: Nachweispflicht (Art. 5 Abs. 2)

Der verantwortliche Dienstgeber muss bei der Datenverarbeitung auch dann für Ordnung sorgen, wenn kein betroffener Mitarbeiter Auskunft oder Löschung verlangt.

Vielmehr muss er schon von sich aus seine Datensammlung in Ordnung halten und dies auch jederzeit nachweisen können. Es reicht also nicht, wenn der Dienstherr erst dann anfängt, sich mit der Ordnungsgemäßheit seiner Datenverarbeitung zu beschäftigen, wenn ein Mitarbeiter „aktiv“ wird. Der Dienstherr muss gemäß Art. 5 Abs. 1 DSGVO unter anderem darauf achten, dass

- die Datenverarbeitung transparent ist,
- die Bindung an den Zweck der Verarbeitung gewährleistet ist,
- nicht mehr Daten als für die Zweckerreichung nötig verarbeitet werden und
- die Daten korrekt und aktuell sind.

Bei alledem trifft den Dienstherrn eine Nachweispflicht gemäß Art. 5 Abs. 2 DSGVO. Er muss jederzeit den Nachweis führen können, dass er die hier genannten Pflichten eingehalten hat.

Nehmen Sie diese 5 Säulen als Orientierungsliste für den Datenschutz im Arbeitsalltag. Verantwortliche im Gremium sollten regelmäßig prüfen, ob Informationen verständlich bereitgestellt werden, Betroffene ausreichend informiert sind und Anfragen zu Auskunft oder Löschung fristgerecht bearbeitet werden. Besonders wichtig ist außerdem, die Datenverarbeitung von Anfang an ordnungsgemäß zu dokumentieren, damit die Einhaltung der DSGVO jederzeit nachgewiesen werden kann.

FAZIT

Datenschutz beginnt schon vor dem Konflikt

Die 5 Säulen zeigen, dass Datenschutz nicht erst dann wichtig wird, wenn ein Mitarbeiter seine Rechte geltend macht. Die DSGVO verpflichtet Verantwortliche vielmehr zu einem transparenten, sparsamen und nachvollziehbaren Umgang mit personenbezogenen Daten. Wirken Sie daher immer darauf hin, dass Ihr Dienstherr die Informations-, Auskunfts- und Löschungsrechte beachtet und gleichzeitig seine Verarbeitungsvorgänge dokumentiert. So schaffen Sie eine wichtige Grundlage für einen rechtssicheren Datenschutz.

Personalratsdaten | Lesezeit 3 Minuten

Datenschutz gilt auch in Ihrem Personalratsbüro

Nach der DSGVO sind Maßnahmen zu treffen, um die Datensicherheit zu garantieren. Das gilt aber nicht nur für den Dienstherrn, sondern auch für Sie. Achten Sie auf die folgenden Punkte.

1. Umfassender Systemschutz

Stellen Sie sicher, dass es auf allen Computern, Tablets, Laptops etc., auf denen Sie personalratsbezogene Daten speichern, einen umfassenden und aktuellen Virenschutz gibt. Ihre Dienststelle muss dafür Sorge tragen, dass Ihre Systeme mit einer Firewall geschützt sind.

2. Richtiger Umgang mit Passwörtern

Ihre Passwörter sollten sicher sein – nicht „12345" – und gemischt Buchstaben, Zahlen, Sonderzeichen, Groß- und Kleinschreibung enthalten. Zudem sollten Sie die Passwörter regelmäßig ändern, d. h. mindestens jeden Monat.

3. Vorsicht bei Mithörern!

Es sollte selbstverständlich sein, dass Telefonate, in denen personenbezogene Daten besprochen werden, nur so geführt werden, dass keine Unbefugten mithören. Dazu gehört auch das berühmte Telefonieren im Zug. Hier erlebt man es immer wieder, dass Reisende über personenbezogene Daten sprechen – für alle Mitreisenden hörbar.

4. Türen und Schränke immer abschließen

Sobald ein Raum verlassen wird, sind Schränke, Rollcontainer usw., in denen personenbezogene Daten (auch in Papierform) oder Datenträger aufbewahrt werden, abzuschließen. Das gilt selbstverständlich auch für das Personalratsbüro selbst. Die Schlüssel sind sorgfältig aufzubewahren.

5. Keine Unbefugten am PC oder an anderen Datenträgern

Ihre PCs benutzen nur Sie und sonst keiner. Sie lassen nicht mal schnell den Kollegen X was ausdrucken oder Frau Y schnell die Mails checken.

6. Richtige Entsorgung von Datenträgern

Hier besteht das Problem in erster Linie (aber nicht nur) bei der Entsorgung von privaten Datenträgern, auf denen Personalratsmitglieder personenbezogene Daten über Kollegen gespeichert haben.

Es gibt eine ganze Reihe von Presseberichterstattungen – auch in Bezug auf Personalräte und Gewerkschaften –, in denen verkaufte Computer oder Festplatten untersucht wurden. Häufig waren die Verkäufer der Auffassung, dass die Datenträger ausreichend geleert worden waren. Das war in der Regel aber nicht der Fall. Datenträger, auf denen personenbezogene Daten gespeichert sind, müssen (!) Sie professionell entsorgen lassen.

7. Papierunterlagen richtig entsorgen

Tipp 6 gilt analog auch für die Entsorgung von Papierunterlagen, sowohl im Personalratsbüro als auch zu Hause. Achten Sie darauf, dass nach einer Personalratssitzung sämtliche Unterlagen, aus denen sich personenbezogene Daten ergeben, wieder sicher verschlossen werden. Nicht mehr benötigte Daten und Unterlagen sollten Sie professionell entsorgen lassen.

8. E-Mails verschlüsseln

Die unverschlüsselte Übertragung von personenbezogenen Daten per E-Mail ist ein weiteres Problem. Im Rahmen der Personalratsarbeit passiert dies gelegentlich dann, wenn Personalratskollegen Informationen mit personenbezogenen Daten per E-Mail an ihre private E-Mail-Adresse schicken, um sie zu Hause weiterzubearbeiten. Sofern die Datenübertragung nicht verschlüsselt erfolgt, besteht hier ein Problem.

9. Backups anfertigen

Zur Datensicherheit gehört auch, dass verloren gegangene oder beschädigte Daten wiederhergestellt werden können. An einem regelmäßigen Backup führt also weder aus praktischen noch aus datenschutzrechtlichen Gründen ein Weg vorbei. Stellen Sie sicher, dass der Personalrats-PC automatisiert entsprechende Backups anfertigt. Prüfen Sie, ob sich die Backups problemlos zurückspielen lassen. Hier fühlen sich viele mit ihren Backups schon in Sicherheit – doch der Schein trügt, wenn die Rückspeicherung nicht sauber funktioniert.

BEISPIEL

Löschen allein reicht nicht

Ein Mitglied eines fünfköpfigen Personalrats nutzt für die Personalratsarbeit seinen privaten Laptop. Als er sich ein neues Gerät angeschafft hat, verkauft er den bisher genutzten Laptop auf eBay. Natürlich hat er mit den Funktionen zur Datenlöschung die Daten aus der Personalratsarbeit vorher „gelöscht". Leider weiß er aber nicht, dass es technisch ohne Weiteres möglich ist, diese Daten wiederherzustellen.

FAZIT

Dienstliches bleibt in der Dienststelle!

Schicken Sie sich dienstliche Daten nicht auf private PCs oder Laptops, etwa um sich zu Hause auf eine Sitzung vorzubereiten. Datenschutzrechtlich ist dies in vielfacher Hinsicht problematisch: Zum einen müssten Sie die Daten natürlich auch auf dem privaten Laptop löschen. Zum anderen ist der Schutz auf dem privaten PC, den eventuell auch die Kinder und der Ehepartner nutzen, nicht so gegeben wie in der Dienststelle. Zum Dritten möchte der betroffene Mitarbeiter vielleicht nicht, dass seine Daten einfach so durchs WWW gejagt werden.

Lassen Sie also Dienstliches so weit wie möglich in der Dienststelle. Sicher ist sicher!

Datensammlung | Lesezeit 8 Minuten

Diese Daten dürfen Sie als Personalratsgremium für Ihre Arbeit erheben

Ohne Daten geht es auch bei Ihnen nicht. Wie sollten Sie sonst prüfen, ob eine Kündigung gerechtfertigt ist, ob diskriminiert wird …? Daten müssen wir also erheben – aber immer mit Augenmaß!

Denken Sie immer daran: Als Personalrat sind Sie in Ihrer Aufgabenerfüllung unabhängig. Das heißt, dass weder Ihr Dienstherr noch der Datenschutzbeauftragte Kontrollbefugnisse hat, ob Sie das BDSG innerhalb der Personalratsarbeit einhalten. Dennoch bewegen Sie sich nicht im rechtsfreien Raum. Wenn Sie Daten bearbeiten, müssen Sie die Anforderungen des BDSG einhalten. Was Sie dabei wissen und beachten sollten, erfahren Sie nachstehend.

Das sind die Grundregeln des Datenschutzes

Wenn Sie Daten erheben oder verarbeiten, ist dies nur gestattet, wenn entweder das BDSG oder eine andere Norm dies ausdrücklich gestattet oder – soweit überhaupt möglich – der Betroffene selbst eingewilligt hat. Für Mitarbeiterdaten gilt: Die Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn

- der Betroffene eingewilligt hat,
- das Gesetz dies gestattet oder
- die Erlaubnis sich in einem Tarifvertrag oder einer Dienstvereinbarung findet.

Ergeben sich aus anderen Gesetzen andere Vorgaben, gehen solche Sonderregelungen dem BDSG immer vor! Im öffentlichen Dienst sollte Ihnen hier sofort § 3 Abs. 1 TVöD einfallen, der alle Beschäftigten zur Geheimhaltung verpflichtet. § 3 Abs. 1 TVöD geht Hand in Hand mit dem BDSG und Ihrer Geheimhaltungspflicht als Personalrat.

Denken Sie hier etwa an die gesetzlichen Auskunfts- und Meldepflichten gegenüber Behörden (zum Beispiel nach § 41 Jugendarbeitsschutzgesetz) sowie an die steuer- und sozialversicherungsrechtlichen Meldepflichten.

Für den Bereich der Telekommunikation, etwa Telefon- und E-Mail-Kommunikation, sind insbesondere die Vorschriften des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes (TDDDG) zu beachten. Für digitale Dienste wie Webseiten, Suchmaschinen und Webshops gelten ebenfalls die einschlägigen Vorschriften des TDDDG sowie – soweit personenbezogene Daten verarbeitet werden – die DSGVO. Das frühere Telemediengesetz (TMG) ist seit dem 14.5.2024 nicht mehr in Kraft.

Datenerhebung muss notwendig sein

Personenbezogene Daten dürfen im Personalratsbüro nur dann erhoben werden, wenn diese Daten zwingend für Ihre Aufgabenerfüllung erforderlich sind. Sie als Personalrat müssen unter Umständen auch Daten verarbeiten, die sich aus Ihren Aufgaben aus dem BPersVG oder aus dem für Sie einschlägigen Landespersonalvertretungsgesetz herleiten lassen. Sie sollten jedoch konkret begründen können, aus welchen rechtlichen Vorgaben sich die Datenverarbeitung ableiten lässt.

Sie als Personalrat sind ja zur Verschwiegenheit verpflichtet und müssen deshalb auch eigene Datenschutzmaßnahmen treffen. Aus diesem Grund kann Ihnen der Dienstherr auch keine Daten aus Datenschutzgründen verweigern. Verwenden Sie das folgende Muster-Schreiben:



Muster-Schreiben: Einwilligung in die Datenerhebung

Ort, Datum

Liebe Frau …, / Lieber Herr …,

für die Mitarbeiterbefragung benötigen wir folgende Angaben von Ihnen: …, diese tragen Sie bitte unten unter „Meine Daten" ein.

Zur Datenerhebung und -verarbeitung benötigen wir Ihre Zustimmung, um die wir mit diesem Schreiben bitten. Bitte geben Sie uns die Daten im Fall Ihres Einverständnisses auf dem unteren Abschnitt des Schreibens an, kreuzen Sie das entsprechende Feld an und lassen Sie uns das Schreiben möglichst umgehend unterzeichnet zukommen.

Ihre Daten werden im Fall der Zustimmung elektronisch verarbeitet und nach Auswertung noch 12 Monate lang aufbewahrt. Danach werden sie gelöscht.

Sie haben die Möglichkeit, der Datenverarbeitung und -erhebung zu widersprechen. Falls Sie dies tun möchten, kreuzen Sie einfach das entsprechende Feld unten an.

Mit freundlichen Grüßen

Ihr Personalrat

Meine Daten: .....

Mit der Erhebung meiner Daten bin ich, Frau/Herr .....,

- einverstanden.
- nicht einverstanden.

Ort, Datum: .....

Zu finden unter www.adiuva.de unter Eingabe des Titels im Suchfeld

BPersVG setzt die Grenze

Dies gilt natürlich nur für die Daten, die Sie als Personalrat im Rahmen Ihrer Aufgabenerfüllung nach dem BPersVG benötigen. Darüber hinaus müssen Ihnen keine Auskünfte gegeben werden.

Als Personalrat unterliegen Sie hinsichtlich der Beschäftigtendaten einer besonderen Geheimhaltungspflicht. Allerdings haben Sie

auch eine Überwachungspflicht. Diese erstreckt sich auch auf die Arbeit des Datenschutzbeauftragten. Gleichzeitig bestehen umfangreiche Mitbestimmungsrechte bei der Einführung von Verhaltenspflichten oder der Einführung technischer Anlagen zur Überwachung, wie zum Beispiel bei der Installation von Videokameras.

MEIN TIPP

Sichern Sie sich ab!

Holen Sie als Personalrat für jede Datenverarbeitung, die sich nicht unmittelbar aus dem BDSG oder BPersVG ableiten lässt, eine schriftliche Einwilligung der betroffenen Kollegen ein. Dies gilt zum Beispiel für die Jubiläumslisten, die Sie erheben und veröffentlichen, und auch, wenn Sie personenbezogene Daten an Gewerkschaften übermitteln wollen.

Das sind Ihre Informationsrechte und Ihre Grenzen

Im Rahmen Ihrer Überwachungspflicht haben Sie auch das Recht, Informationen anzufordern und Unterlagen einzusehen. Was Sie hierbei dürfen und was nicht, ist immer wieder ein Streitpunkt.

So hat das Bundesarbeitsgericht (BAG) mittlerweile entschieden, dass der Betriebsrat kein Recht auf einen Onlinezugriff auf Beschäftigtendaten hat. Der Arbeitgeber kann ihm die gewünschten Informationen auch mithilfe von Papierausdrucken geben (BAG, 16.8.2011, Az. 1 ABR 22/10). Diese Entscheidung ist auf die Personalratsarbeit übertragbar.

Gehaltslisten dürfen Sie als Personalrat auch in nicht anonymisierter Form anfordern. Diese Listen sind nicht Bestandteil der Personalakte und unterliegen daher auch nicht dem besonderen Datenschutz einer Personalakte (Hamburgisches Oberverwaltungsgericht, 29.11.2011, Az. 8 Bf 138/11.PVL).

Und wenn Ihr Dienstherr ein betriebliches Eingliederungsmanagement für Langzeiterkrankte durchführen muss, haben Sie als Personalrat das Recht auf Auskunft und namentliche Benennung aller Personen, die hierfür in Betracht kommen. Datenschutzrechtliche Gründe stehen der namentlichen Nennung dabei nicht entgegen (BAG, 7.2.2012, Az. 1 ABR 46/10).

MEIN TIPP

Handeln Sie nie leichtfertig

Datenschutz ist ein heikles Thema. Wenn Sie sich unsicher sind, ob Sie Daten erheben dürfen oder nicht, holen Sie sich eine Einwilligung des Betroffenen; verweigert er sie, erheben Sie die Daten besser nicht.

Diese Informationsrechte haben Sie

Um Ihrer Überwachungspflicht nachkommen und Ihre Mitbestimmungsrechte umsetzen zu können, steht Ihnen als Personalrat ein umfassendes Informationsrecht zu.

So informiert Ihr Dienstherr Sie richtig

Nach § 66 BPersVG sind Sie rechtzeitig und umfassend zu unterrichten. „Rechtzeitig" heißt auf alle Fälle vor der zu treffenden Maßnahme. Sie müssen noch Einfluss nehmen können. „Umfassend" heißt, dass Ihr Dienstherr Ihnen grundsätzlich alle entsprechenden Unterlagen und Informationen zuleiten muss, die er auch selbst hat.

MEIN TIPP

Nur informiert können Sie richtig arbeiten

Sie können von Ihrer Dienststellenleitung jederzeit die Unterlagen verlangen, die Sie benötigen, um Ihre Aufgaben erfüllen zu können. Nur so werden Sie in die Lage versetzt, in eigener Verantwortung zu prüfen, ob sich für Sie Aufgaben ergeben und Sie tätig werden müssen.

Diese Unterlagen dürfen Sie einsehen

Ihr Dienstherr darf Ihnen die Einsicht in folgende Unterlagen nicht verwehren:

- **personenbezogene Daten,** die beim Dienstherrn selbst verarbeitet werden und die für Ihre Arbeit relevant sind
- **personenbezogene Daten,** die an Externe übermittelt werden
- **Maßnahmen,** die getroffen werden, um sicherzustellen, dass die an andere Unternehmen übermittelten Daten nur zu den vereinbarten Zwecken verarbeitet werden
- **die eingesetzten Programme** mit Namen und Kurzbeschreibung
- **Pflichtenheft, Datenflussplan und Systembeschreibung**

MEIN TIPP

Arbeiten Sie Hand in Hand

Letztgenannte Informationen entsprechen den Übersichten, die Ihr Dienstherr auch dem betrieblichen Datenschutzbeauftragten zur Verfügung stellen muss. Schließen Sie sich also im Zweifel mit diesem kurz.

Lassen Sie sich aber nicht zu tief vom Datenschutzbeauftragten in die Karten schauen. Das BAG hat bereits 1997 (11.11.1997, Az. 1 ABR 21/97) festgestellt, dass der Datenschutzbeauftragte die Arbeitnehmervertretung nicht kontrollieren darf. Der Grund ist, dass Sie ein unabhängiges Organ sind und bleiben sollen.

Zudem sind Sie bzw. das Personalratsgremium ja selbst dem BDSG unterworfen. Sprich: Sie müssen die Einhaltung des Datenschutzes im Personalrat überwachen und kontrollieren und sicherstellen. Sie brauchen also nicht noch eine externe Kontrolle durch den Datenschutzbeauftragten.

FAZIT

Denken Sie an Schulungen

Datenschutz ist und bleibt ein schwieriges Thema. Gerade durch die KI und die Digitalisierung ist hier vieles im Fluss. Denken Sie also gern auch mal wieder an eine Schulung zum Thema.

Personalunion | Lesezeit 4 Minuten

Vorsitzender als Datenschutzbeauftragter?

Vorsitzender des Personalratsgremiums sein und gleichzeitig das Amt des Datenschutzbeauftragten bekleiden? Das geht nicht! Hier stehen sich Interessen gegenüber, die nicht vereinbar sind. Daher ist eine Abberufung des Datenschutzbeauftragten in diesem Fall gerechtfertigt, so das Bundesarbeitsgericht (BAG) (6.6.2023, Az. 9 AZR 383/19).

Der Fall: Hier ging es um den Vorsitzenden des Betriebsrats, der für die Ausübung seines Amts teilweise freigestellt war. Mit Wirkung zum 1.6.2015 bestellten ihn der Arbeitgeber und die weiteren in Deutschland ansässigen Tochtergesellschaften zum Datenschutzbeauftragten. Auf Veranlassung des Thüringer Landesbeauftragten für Datenschutz und Informationsfreiheit widerriefen der Arbeitgeber und die weiteren Konzernunternehmen die Bestellung des Betriebsratsvorsitzenden jedoch am 1.12.2017 mit sofortiger Wirkung wegen einer Inkompatibilität der Ämter. Dagegen wehrte sich der Betroffene.

Arbeitgeber hat recht

Die Entscheidung: Vor dem BAG unterlag der Betriebsratsvorsitzende. Die Aufgaben eines Betriebsratsvorsitzenden und eines Datenschutzbeauftragten können nach Ansicht der Richter typischerweise nicht durch dieselbe Person ohne Interessenkonflikt ausgeübt werden. Personenbezogene Daten dürfen dem Betriebsrat nur zu Zwecken zur Verfügung gestellt werden, die das Betriebsverfassungsgesetz ausdrücklich vorsieht.

Wer Datenschutzbeauftragter werden kann

Wer das Amt des Datenschutzbeauftragten bekleidet, entscheidet grundsätzlich der Verantwortliche der Dienststelle. Die ausgewählte Person muss jedoch über die erforderliche berufliche Qualifikation und das erforderliche Fachwissen im Datenschutzrecht und in der Datenschutzpraxis verfügen. Außerdem muss sie in der Lage sein, die Aufgaben des Datenschutzbeauftragten ordnungsgemäß zu erfüllen. Maßgeblich sind insbesondere Art. 37 Abs. 5 und Art. 39 DSGVO.

Bei der Auswahl ist darüber hinaus darauf zu achten, dass die Person ihre Aufgaben unabhängig und frei von Interessenkonflikten wahrnehmen kann. Art. 38 Abs. 6 DSGVO erlaubt dem Datenschutzbeauftragten zwar grundsätzlich die Wahrnehmung weiterer Aufgaben, diese dürfen jedoch nicht zu einem Interessenkonflikt führen.

Wann muss ein Datenschutzbeauftragter benannt werden?

Für Dienststellen ergibt sich die Pflicht zur Benennung eines Datenschutzbeauftragten vornehmlich aus Art. 37 Abs. 1 DSGVO und ergänzend aus § 38 BDSG.

Nach § 38 Abs. 1 BDSG muss ein Datenschutzbeauftragter grundsätzlich benannt werden, wenn in einer Dienststelle in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

Unabhängig von der Anzahl der Beschäftigten besteht eine Benennungspflicht z. B. dann, wenn es Verarbeitungen gibt, die einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO unterliegen, oder wenn personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet werden.

Aber auch unabhängig von diesen Schwellenwerten kann sich eine Benennungspflicht unmittelbar aus Art. 37 Abs. 1 DSGVO ergeben, etwa wenn die Kerntätigkeit des Verantwortlichen oder Auftragsverarbeiters eine umfangreiche regelmäßige und systematische Überwachung von Personen oder eine umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten umfasst.

Personalratsmitglied als Datenschutzbeauftragter?

Nicht jedes Personalratsmitglied ist allein aufgrund seines Mandats generell von der Tätigkeit als Datenschutzbeauftragter ausgeschlossen. Entscheidend ist vielmehr, ob die konkrete Doppelfunktion zu einem Interessenkonflikt führt.

Einen solchen Interessenkonflikt sah das BAG beim Vorsitzenden. Bei einem einfachen Mitglied ist daher eine Einzelfallprüfung erforderlich. Die bloße Mitgliedschaft im Personalrat führt nicht automatisch zur Unvereinbarkeit. Entscheidend sind die konkreten Aufgaben und Verantwortlichkeiten der betreffenden Person. Ich wäre hier aber generell vorsichtig.

Interner oder externer Datenschutzbeauftragter?

Der Datenschutzbeauftragte kann grundsätzlich entweder ein Mitarbeiter der Dienststelle oder ein externer Dienstleister sein. Bei der Benennung eines internen Datenschutzbeauftragten muss die Dienststelle insbesondere darauf achten, dass dessen sonstige Aufgaben nicht zu einem Interessenkonflikt führen.

Ein externer Datenschutzbeauftragter kann deshalb vor allem dann sinnvoll sein, wenn es innerhalb der Dienststelle keine Person gibt, die die erforderliche Fachkunde besitzt und gleichzeitig unabhängig tätig werden kann.

Datenschutzbeauftragte genießen einen besonderen Schutz

Datenschutzbeauftragte nehmen eine besondere Stellung innerhalb der Dienststelle ein. Nach Art. 38 Abs. 3 DSGVO dürfen sie bei der Erfüllung ihrer Aufgaben keine Weisungen erhalten. Sie dürfen wegen der Erfüllung ihrer Aufgaben weder abberufen noch benachteiligt werden. Außerdem müssen sie unmittelbar der höchsten Managementebene berichten können.

FAZIT

Saubere Trennung erforderlich

Wann immer eine Person 2 Ämter ausführt, sollte grundsätzlich ganz genau hingesehen werden, ob eine Interessenkollision entstehen kann. Man kann schließlich nicht 2 Herren gleichzeitig dienen!

Informationsanspruch | Lesezeit 3 Minuten

Sie dürfen nicht alles wissen

Natürlich ist der Datenschutz auch bei Ihnen im Gremium höchst relevant. Sie haben ja einen Informationsanspruch gegen Ihre Dienststelle. Nur, wie genau muss die diesem Anspruch nachkommen? Hierzu hat das Verwaltungsgericht (VG) Ansbach entschieden (22.3.2024, Az. AN 8 P 21.01338).

Der Fall: In dem Verfahren ging es um einen Streit zwischen einem Personalrat einer staatlichen Hochschule in Bayern und der Leitung der Hochschule. Der Personalrat wollte regelmäßig Informationen über die personelle Besetzung der Dienststelle erhalten. Konkret verlangte er einen sogenannten Soll-Ist-Stellenplan. Ein solcher Stellenplan zeigt, welche Stellen in einer Dienststelle vorhanden sind, wie diese Stellen besetzt sind und welche Beschäftigten auf welchen Stellen eingesetzt werden. Der Personalrat wollte allerdings nicht nur eine anonymisierte Übersicht. Er verlangte einen Stellenplan mit konkreten personenbezogenen Angaben.

Der Personalrat begründete seine Forderung damit, dass er diese Informationen für seine gesetzlichen Aufgaben benötige. Er wollte deshalb bereits im Vorfeld einen Überblick über die Beschäftigten und Stellen haben. Nur so könne er nach seiner Auffassung beurteilen, ob bei späteren Personalentscheidungen möglicherweise andere Beschäftigte benachteiligt würden oder ob die gesetzlichen Vorgaben eingehalten würden.

Namen müssen nicht sein

Die Hochschule sah das anders. Sie meinte, der Personalrat habe keinen Anspruch darauf, regelmäßig und ohne konkreten Anlass eine umfangreiche Liste mit Namen und weiteren persönlichen Angaben zu bekommen. Er könne seinen Aufgaben auch mit weniger personenbezogenen Informationen nachkommen.

Der Streit landete beim VG Ansbach.

Personalrat muss nicht alles wissen

Das VG Ansbach gab der Hochschule recht und lehnte die Anträge des Personalrats ab. Sie als Personalrat können also nicht verlangen, dass Ihnen regelmäßig und ohne konkreten Anlass ein umfassender Stellenplan mit den Namen und weiteren personenbezogenen Daten aller Beschäftigten zur Verfügung gestellt wird. Der entscheidende Punkt des Gerichts: Sie als Personalrat haben zwar einen Informationsanspruch, dieser ist aber nicht grenzenlos.



Das Gericht hat den Informationsanspruch eng an die konkreten gesetzlichen Aufgaben des Personalrats gebunden. Informationen müssen also einen nachvollziehbaren Bezug zu einer Aufgabe haben, die Sie als Personalrat tatsächlich wahrzunehmen haben.

Warum spielt der Datenschutz eine so große Rolle?

Das Gericht hat ausdrücklich festgestellt, dass die Namen, Arbeitszeiten, Eingruppierungen und sonstigen Angaben zu einzelnen Beschäftigten personenbezogene Daten im Sinne der DSGVO sind. Wenn Ihnen die Dienststelle diese Daten gibt, findet damit eine Verarbeitung personenbezogener Daten statt. Deshalb reicht es nicht aus, lediglich zu sagen: „Der Personalrat braucht die Daten für seine Arbeit."

Vielmehr muss zusätzlich geprüft werden, ob gerade diese personenbezogenen Daten erforderlich sind.

BVerwG verlangt Differenzierung

Das Bundesverwaltungsgericht (BVerwG) hat entschieden, dass bei Informationsverlangen des Personalrats besonders geprüft werden muss, ob die Namensnennung tatsächlich erforderlich ist (29.4.2025, Az. 5 P 7.23). Sind anonymisierte oder pseudonymisierte Informationen ausreichend, müssen nicht auch die Namen der Beschäftigten mitgeteilt werden. Die Identität eines Beschäftigten kann vielmehr erst dann offengelegt werden, wenn dies zur Aufklärung des konkreten Sachverhalts notwendig ist.

Das BVerwG beschreibt damit einen Stufenansatz: zunächst möglichst wenige personenbezogene Informationen. Erst wenn damit die Aufgabe des Personalrats nicht sachgerecht erfüllt werden kann, kommt eine weitergehende Identifizierung in Betracht. Die Namensnennung ist also eher das Mittel für den konkreten Einzelfall und nicht der automatische Ausgangspunkt.

Kurz gesagt: Sie als Personalrat haben ein Recht auf Information, aber kein Recht auf „alles". Je stärker eine Information in die Privatsphäre der Beschäftigten eingreift, desto genauer muss begründet werden, warum gerade diese Information für die konkrete Personalratsaufgabe erforderlich ist. Genau hier treffen Personalvertretungsrecht und Datenschutzrecht aufeinander.

FAZIT

Begründen Sie sauber

Gerade wenn es um persönliche Daten Ihrer Kollegen geht, sollten Sie immer noch mal innehalten, bevor Sie diese verlangen: Benötigen Sie diese Daten wirklich? Welche konkrete Personalratsaufgabe steht hinter Ihrem Verlangen? Je sensibler die Daten, umso sauberer und tiefgehender müssen Sie Ihre Anfrage begründen können. Sie möchten selbst ja auch, dass Ihre persönlichen Daten so gut geschützt werden, wie es geht.

Beweisverwertungsverbote | Lesezeit 3 Minuten

Diese Auswirkung hat eine unzulässige Datenerhebung im Prozess

Wie hoch der Stellenwert des Datenschutzes ist, kann man am besten erkennen, wenn es darum geht, welche Folgen ein Verstoß hat. Das Bundesarbeitsgericht (BAG) setzt den Stellenwert des Datenschutzes offenbar sehr hoch an. Es zieht nämlich überraschende Konsequenzen.

Der Keylogger

Fall 1: Ein IT-Fachmann war als Web-Entwickler beschäftigt. Im April 2015 teilte der Arbeitgeber den Arbeitnehmenden mit, dass der gesamte Internet-Traffic und die Benutzung ihrer Systeme „mitgeloggt" würden. Er installierte auf dem Dienst-PC des IT-Fachmanns eine Software, die sämtliche Tastatureingaben protokollierte und regelmäßig Bildschirmfotos (Screenshots) anfertigte.

Nach Auswertung der so erstellten Dateien bat der Arbeitgeber den Mitarbeiter zum Gespräch. Der Mitarbeiter räumte zwar ein, seinen Dienst-PC während der Arbeitszeit privat genutzt zu haben, aber nur in geringem Umfang und in der Regel in seinen Pausen. Der Arbeitgeber konnte aber aus dem vom „Keylogger" erfassten Datenmaterial davon ausgehen, dass der Mitarbeiter den Dienst-PC offenbar in viel größerem Umfang privat genutzt hatte. Er kündigte das Arbeitsverhältnis fristlos.

Nicht alles darf im Prozess verwertet werden

Das Urteil: Der Arbeitgeber durfte die durch die Keylogger-Software gewonnenen Erkenntnisse über die Privattätigkeiten des Mitarbeiters im gerichtlichen Verfahren nicht verwerten (BAG, 27.7.2017, Az. 2 AZR 681/16). Der Einsatz des speziellen Software-Programms hat das allgemeine Persönlichkeitsrecht des Mitarbeiters auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) verletzt. Die Informationsgewinnung war nach § 32 Abs. 1 BDSG nicht zulässig.

Der Arbeitgeber hatte beim Einsatz der Software gegenüber dem Mitarbeiter keinen auf Tatsachen beruhenden Verdacht einer Straftat oder einer anderen schwerwiegenden Pflichtverletzung. Die sozusagen „ins Blaue hinein" veranlasste Kontrollmaßnahme war daher unverhältnismäßig. Das Gericht musste für die Entscheidung davon ausgehen, dass der Mitarbeiter den Dienst-PC nur in geringem Umfang privat genutzt hatte – obwohl natürlich auch die Richter sahen, dass das offenbar nicht stimmte! Die vom Mitarbeiter eingeräumte geringe Privatnutzung dagegen reichte ohne Abmahnung nicht für eine Kündigung.

Grenzen der „Überwachung" durch Abmahnung

Eine Abmahnung enthält regelmäßig personenbezogene Daten, die Eingang in die Personalakte finden. Auch hier findet also eine Art „Überwachung" personenbezogener Daten statt. Daher kann ein Anspruch auf Entfernung einer Abmahnung nicht nur aus den allgemeinen zivilrechtlichen Regelungen des BGB abgeleitet werden, sondern eventuell auch aus datenschutzrechtlichen Vorschriften. Das Landesarbeitsgericht (LAG) Sachsen-Anhalt hatte in diesem Zusammenhang über folgenden Fall zu entscheiden:

Fall 2: Ein Mitarbeiter stritt mit seinem Arbeitgeber vor Gericht unter anderem über die Wirksamkeit einer arbeitgeberseitigen Kündigung und über die Entfernung einer Abmahnung aus der Personalakte. Die Abmahnung hatte der Mitarbeiter erhalten, weil der Arbeitgeber ihm vorwarf, einer seiner Weisungen pflichtwidrig nicht nachgekommen zu sein. Der Mitarbeiter hat das Arbeitsverhältnis dann einige Zeit später selbst gekündigt.

DSGVO schafft Anspruch auf Löschung der Abmahnung

Das Urteil: Das LAG Sachsen-Anhalt urteilte, der Mitarbeiter habe nach Art. 17 Abs. 1 DSGVO einen Anspruch auf Entfernung der Abmahnung (23.11.2018, Az. 5 Sa 7/17). Bei der Abmahnung handle es sich um personenbezogene Daten. Diese müssten gelöscht werden, wenn sie nicht mehr benötigt würden. Die Abmahnung hat einen doppelten Zweck: zum einen die Rüge- und Dokumentationsfunktion, zum anderen werden Konsequenzen für den Fall einer weiteren Pflichtverletzung in Aussicht gestellt (Warnfunktion). Nach Beendigung des Arbeitsverhältnisses sei die Warnfunktion entfallen. An der Rüge- und Dokumentationsfunktion könne der Arbeitgeber hingegen noch ein Interesse haben, soweit es um die Abwehr von etwaigen Ansprüchen des Arbeitnehmers gehe. Hier sah das Gericht ein solches Interesse nicht.

WICHTIG

Interesse an Abmahnung darlegen

Grundsätzlich sind Ihre Kollegen nach Beendigung des Arbeitsverhältnisses in einer guten Position, wenn es darum geht, eine Abmahnung zu entfernen, da ein Recht auf Löschung der personenbezogenen Daten bzw. auf Entfernung der Abmahnung besteht. Wenn Ihr Dienstherr meint, noch ein berechtigtes Interesse an der Aufbewahrung des Dokuments zu haben, muss er dies darlegen.

Datenschutz ist kein Täterschutz

In diesem Sinne hat das BAG zur Videoüberwachung entschieden (29.6.2023, Az. 2 AZR 296/22). Hier ging es um die Frage, ob Erkenntnisse aus einer möglicherweise datenschutzwidrigen offenen Videoüberwachung im Kündigungsschutzprozess verwertet werden dürfen. Das BAG hat klargestellt, dass ein Datenschutzverstoß nicht automatisch zu einem Beweisverwertungsverbot führt.

FAZIT

Der Einzelfall entscheidet

Grundsätzlich dürfen rechtswidrig gewonnene Daten nicht im Prozess verwertet werden. Schlussendlich kommt es aber auch hier auf den Einzelfall an.

Auskunftsanspruch | Lesezeit 4 Minuten

Warum Sie Ihren Dienstherrn nach Ihren Daten fragen sollten

Beschäftigte haben nach der Datenschutz-Grundverordnung (DSGVO) grundsätzlich ein Recht auf Auskunft über die zu ihrer Person gespeicherten Daten. Das kann insbesondere im Rahmen eines Kündigungsschutzprozesses interessant sein. Allerdings hat sich in der Rechtsprechung noch keine einheitliche Linie gebildet, was genau dieser Anspruch beinhaltet.

So „weit" sieht das LAG Baden-Württemberg den Anspruch

Zunächst ein Fall, der vor dem Landesarbeitsgericht (LAG) Baden-Württemberg verhandelt wurde.

Der Fall: Ein führender Mitarbeiter in einem großen Unternehmen erhielt eine Kündigung wegen angeblicher Minderleistung. Gegen diese Kündigung erhob er Kündigungsschutzklage. Im Kündigungsschutzprozess beanspruchte der Mitarbeiter Auskunft vom Arbeitgeber über sämtliche zu seiner Person gespeicherten Daten. Der Arbeitgeber hielt dagegen und berief sich auf den Schutz berechtigter Interessen im Zusammenhang mit „Whistleblowern". Das sind Personen, die Informationen zur Aufdeckung von Straftaten oder sonstigen Verstößen liefern. Der Arbeitgeber meinte, es müssten hier Personen geschützt werden, die Informationen über Verstöße des Klägers geliefert hätten.

Auskunftsanspruch des Mitarbeiters: LAG = ja

Das Urteil: Das LAG Baden-Württemberg folgte der Argumentation des Arbeitgebers nicht (20.12.2018, Az. 17 Sa 11/18). Vielmehr bejahte es den Auskunftsanspruch des Mitarbeiters. Zwar könne der Schutz von Informanten bzw. „Whistleblowern" ein berechtigtes Geheimhaltungsinteresse begründen. Allerdings müsse der Arbeitgeber, der sich darauf berufe, im Einzelnen darlegen, woraus sich das Geheimhaltungsinteresse ergebe. Pauschale Hinweise auf die Notwendigkeit der Anonymität für das Funktionieren eines Informantensystems reichten nicht aus.

Gerade in Kündigungsschutzprozessen kann der umfassende Auskunftsanspruch ein interessanter Hebel sein, um an Informationen zu kommen, die man dann möglicherweise erfolgreich im Prozess einsetzen kann. So ist es natürlich kein Wunder, dass sich Arbeitgebende mit aller Macht dagegen wehren. Auch im vorliegenden Fall hat der Arbeitgeber das Urteil vor der nächsten Instanz angegriffen und wollte zunächst eine Entscheidung des Bundesarbeitsgerichts (BAG) erreichen. Vor dem BAG haben sich die Parteien dann aber geeinigt. Eine höchstrichterliche Entscheidung gab es in dieser Sache daher nicht.

Das LAG Niedersachsen sieht es enger

Nicht ganz so weit wollte das LAG Niedersachsen in seiner Entscheidung vom 6.6.2020 (Az. 9 Sa 608/19) gehen. Das Gericht schränkte die Auskunftspflicht des Arbeitgebers ein. Der Auskunftsanspruch gehe nicht über die in Art. 15 Abs. 1 DSGVO geregelten Pflichtangaben hinaus.

Bei großen Datenmengen müsse die Person, die die Auskunft verlangt, konkretisieren, welche Dokumente sie verlange, und begründen, warum ihr die jeweiligen Dokumente nicht bereits vorlägen.

Ein Anspruch auf Überlassung ganzer Datensätze bestehe nicht. Sinn und Zweck des Auskunftsanspruchs sei es, eine Überprüfung der Datenverarbeitung zu ermöglichen, aber nicht, vollständige Kopien aller Unterlagen zu erhalten. Dem Mitarbeiter sei der E-Mail-Verkehr, den er geführt habe, ja bekannt. Auch in diesem Fall gab es keine inhaltliche höchstrichterliche Entscheidung.

So sieht es der BGH

Interessant ist in diesem Zusammenhang, dass der Bundesgerichtshof (BGH) in einer Entscheidung vom 15.6.2021 einen recht weitgehenden Auskunftsanspruch angenommen hat, also eher der Linie des LAG Baden-Württemberg als derjenigen des LAG Niedersachsen gefolgt ist (Az. VI ZR 576/19). Allerdings ist der BGH für Arbeitsrechtsfragen nicht zuständig. Dementsprechend ging es in dem Verfahren vor dem BGH auch nicht um den Auskunftsanspruch gegen einen Arbeitgeber, sondern gegen eine Versicherung.

Das sagt das BAG

Das BAG hat in einer Entscheidung vom 16.12.2021 für den Bereich des Arbeitsrechts immerhin festgestellt, dass ein Klageantrag auf Auskunftserteilung nicht zu unbestimmt sein dürfe (Az. 2 AZR 235/21). Es reiche jedenfalls nicht aus, einfach nur den Gesetzeswortlaut des Art. 15 DSGVO zu wiederholen.

Das BAG sagt auch: Der Auskunftsanspruch nach Art. 15 Abs. 1 i. V. m. Abs. 3 Satz 1 DSGVO bezieht sich grundsätzlich auf die personenbezogenen Daten, die in einem Dokument enthalten sind – nicht automatisch auf das gesamte Dokument (BAG, 16.4.2026, Az. 8 AZR 169/25).

Die Empfänger müssen Sie kennen

In München ging es um die Frage, ob ein Beschäftigter aufgrund von Art. 15 Abs. 1 lit. c DSGVO nicht nur die Kategorien von Empfängern, sondern auch die Identität der konkreten Empfänger seiner personenbezogenen Daten erfahren kann. Das LAG München hat grundsätzlich bejaht: Verlangt der Beschäftigte die Identität der Empfänger, muss der Arbeitgeber diese grundsätzlich mitteilen, soweit ihm das möglich ist (LAG München, 8.4.2024, Az. 11 Ta 37/24).

FAZIT

Nichts ist in Stein gemeißelt

Wie Sie sehen, ist die Rechtsprechung (noch) nicht einheitlich. Es ist also jeder Einzelfall für sich zu betrachten. Sie dürfen und sollten aber ruhig mal nachfragen, welche Daten Ihr Dienstherr über Sie gespeichert hat, und zu welchem Zweck.

Whistleblowing | Lesezeit 1 Minute

Datenschutz erfordert Hinweisgeberschutz

Datenschutz kann Mitarbeiter in eine Zwickmühle bringen. Einerseits sind die Daten des Dienstherrn zu schützen, andererseits müssen manchmal Dinge ans Licht gebracht werden. Etwa, wenn es um Straftaten geht. Viele Mitarbeiter trauen sich nicht, etwas zu sagen, aus Angst vor Repressalien. Das Hinweisgeberschutzgesetz (HinSchG) versucht, die Aufdeckung von Straftaten zu fördern und gleichzeitig auch Arbeitgeberinteressen angemessen zu berücksichtigen.



So schützt der Gesetzgeber die Hinweisgeber

Das HinSchG gilt für Dienststellen ab 50 Mitarbeitern. Ziel des Gesetzes ist es, Whistleblowern Schutz zu bieten. Der Schutz der Whistleblower soll dazu beitragen, Missstände aufzudecken.

Dienststellen sind verpflichtet, interne Meldestellen einzurichten. Es gibt aber auch staatliche externe Meldestellen. Mitarbeitende können sich grundsätzlich frei entscheiden und aussuchen, ob sie eine interne oder eine externe Meldestelle kontaktieren. Das Gesetz sieht lediglich vor, dass vorzugsweise eine interne Meldestelle kontaktiert werden „soll".

Bei der Ausgestaltung reden Sie mit

Richtet Ihr Dienstherr eine interne Meldestelle ein, ist diese als solche mitbestimmungsfrei. Bei der Ausgestaltung reden Sie aber mit.

Also z. B. bei den Fragen:

- Wer übernimmt die Meldestelle – eigene Beschäftigte oder Externe?
- Wie können die Hinweise abgegeben werden – z. B. digital oder persönlich?
- Welche Software wird dafür eingesetzt und wer hat Zugriff darauf?
- Wie wird das Verfahren innerhalb der Dienststelle organisiert?
- Welche Beschäftigten werden mit welchen zusätzlichen Aufgaben betraut?
- Welche organisatorischen Regelungen gelten für die Bearbeitung der Hinweise?

Unser Service für Sie:

Expertensprechstunde: Stellen Sie Maria Markatou Ihre Frage

Stellen Sie mir Ihre Frage per E-Mail an markatou@mitbestimmung-heute.de.
Sie erhalten dann innerhalb von 24 Stunden eine Antwort. Die Antwort verfasse ich als Ihre Chefredakteurin persönlich. So haben Sie eine schriftliche Aussage, auf deren Basis Sie im Gremium weiterarbeiten können.

Onlinebereich: Hier erhalten Sie alle Arbeitshilfen zum Download

Wir stellen Ihnen online auf www.adiuva.de alle Arbeitshilfen (Checklisten, Übersichten und Musterschreiben) der Ausgaben als Download zur Verfügung.

Folgen Sie ADIUVA auch auf:

Freuen Sie sich schon auf die nächste Sonderausgabe zu einem wichtigen und interessanten Thema!