M|A|V

Mitarbeitende Aktiv Vertreten

BEWÄHRTE 20 JAHRE QUALITÄT

Rechtssicheres Praxiswissen für die Mitarbeitervertretung in kirchlichen & sozialen Einrichtungen

SONDERAUSGABE:

DATENSCHUTZ

Erfahren Sie, wie europäische Datenschutzvorgaben im kirchlichen Bereich umgesetzt werden.

KEIN DATENSCHUTZ OHNE SIE ALS MAV

Ihre Mitwirkung als MAV ist beim Datenschutz an verschiedenen Stellen möglich. Allerdings können Sie als MAV auch selbst Adressat des Datenschutzes sein.

SONDERAUSGABE MAI 2026

AD UVA

Dr. Michael Tillmann, Fachanwalt für Arbeitsrecht & Autor

Seit mittlerweile mehr als 20 Jahren beschäftige ich mich mit dem Arbeitsrecht von A wie Abmahnung über K wie Kündigung bis Z wie Zeugnis. Da ist es nicht ganz einfach, immer auf dem Laufenden zu bleiben und durchzublicken. Ich bereite in den Sonderausgaben immer jeweils ein Thema aktuell und leicht zugänglich für Sie auf, damit Sie den Durchblick behalten.

Editorial

Liebe Mitarbeitervertretung,

Datenschutz hat in Deutschland schon eine recht lange Tradition. Die ersten rechtlichen Grundlagen hat das Bundesverfassungsgericht in den 1980er-Jahren geschaffen. Mittlerweile steht mit der Datenschutz-Grundverordnung (DSGVO) das Thema sozusagen auch auf europäischen Füßen.

Die Kirche hat auch im Bereich Datenschutz ihr Selbstbestimmungsrecht genutzt und jeweils mit eigenen Gesetzen die europäischen Vorgaben umgesetzt. Inhaltlich ähnelt der kirchliche Datenschutz aber weitgehend dem staatlichen Datenschutz nach dem Bundesdatenschutzgesetz.

Die DSGVO ist die gemeinsame Basis. Viele Urteile zum Datenschutz sind daher auf den kirchlichen Bereich übertragbar.

Diese aktuelle Sonderausgabe gibt Ihnen einen Überblick über den Datenschutz. Und natürlich lernen Sie auch Ihre Rolle als MAV im Datenschutz kennen.

Ihr

Michael Tillmann, Chefredakteur

Inhalt

Impressum: Mitarbeitende Aktiv Vertreten

ADIUVA – ein Unternehmensbereich des VNR Verlags für die Deutsche Wirtschaft AG, Theodor-Heuss-Str. 2–4, 53177 Bonn | Telefon: 0228/955 01 60 | ISSN 2199-3378 | **Vorstand:** Richard Rentrop, Bonn | Amtsgericht Bonn, HRB 8165 | **Redaktionell Verantwortliche:** Dilan Wartenberg, VNR Verlag für die Deutsche Wirtschaft AG, Adresse siehe oben | **Autor:** Dr. Michael Tillmann, RA, Köln | **Lektorat/Schlussredaktion:** Ulrike Floßdorf, Oberdürenbach | **Satz:** Schmelzer Medien GmbH, Siegen | **Gestaltung:** Nina Probst, Projektmanagement für Marketing & Kommunikation | **Bildrechte:** S. 1+7: WrightStudio; S. 3: Oleksandr; S. 4: Rawf8; S. 8: Prabhash; S. 10: Yusri Adi – alle AdobeStock | **Druck:** Warlich Druck Meckenheim GmbH, Am Hambuch 5, 53340 Meckenheim | **Erscheinungsweise:** 12 x pro Jahr; Alle Angaben in „MAV – Mitarbeitende Aktiv Vertreten" 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" liegt der Ausgabe Nr. 08 | Mai 2026 von „MAV – Mitarbeitende Aktiv Vertreten" bei. | Dieses Produkt besteht aus FSC®-zertifiziertem Papier.

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

EU-Recht als Basis | Lesezeit 3 Minuten

Kirchlicher Datenschutz auf europäischen Füßen

Der Datenschutz hat mit der Datenschutz-Grundverordnung (DSGVO) eine europäische Basis. Die DSGVO gilt unmittelbar, also ohne eine Umsetzung in deutsches Recht. Allerdings lässt die DSGVO an vielen Stellen Handlungsspielraum. Die nationalen staatlichen sowie die kirchlichen Gesetze müssen daher die DSGVO beachten.

Staatlicherseits wurde in Deutschland vor diesem Hintergrund das Bundesdatenschutzgesetz an die DSGVO angepasst. Im kirchlichen Bereich gibt es jedoch aufgrund des kirchlichen Selbstbestimmungsrechts eigene Gesetze zum Datenschutz, und zwar

- im katholischen Bereich das KDG und
- im evangelischen Bereich das DSG-EKD.

Alle „Beschäftigten" genießen Datenschutz

In den Anwendungsbereich des kirchlichen Datenschutzes fallen gemäß § 4 Ziff. 24 KDG und § 4 Ziff. 20 DSG-EKD auch „Beschäftigte", vor allem

- Arbeitnehmende, also „ganz normale" Mitarbeitende.

Aber auch weitere Personengruppen fallen darunter, wie beispielsweise:

- Bewerber*innen
- Auszubildende
- Praktikant*innen
- ehemalige Mitarbeiter*innen
- Kirchenbeamte
- Freiwillige nach dem Bundesfreiwilligendienstgesetz oder dem Jugendfreiwilligendienstgesetz

Darum geht es beim Datenschutz

Beim Datenschutz – ganz gleich, ob im Arbeitsverhältnis oder in anderen Bereichen – geht es darum, das Recht der Mitarbeitenden bzw. der Betroffenen auf „informationelle Selbstbestimmung" zu schützen.

Dabei handelt es sich um ein wichtiges spezielles Grundrecht, das das Bundesverfassungsgericht (BVerfG) bereits vor über 30 Jahren aus dem allgemeinen Persönlichkeitsrecht gemäß Art. 2 Abs. 1 Grundgesetz (GG) in Verbindung mit Art. 1 Abs. 1 GG entwickelt hat. Es geht also um ein Grundrecht und damit sozusagen um die oberste Kategorie von Rechten in unserer Rechtsordnung.

Das heißt ganz konkret, dass der Datenschutz von seiner rechtlichen Bedeutung her „ganz weit oben" anzusiedeln ist.

Inhaltlich geht es beim Recht auf informationelle Selbstbestimmung darum, dass jeder Mensch und speziell jede*r Mitarbeiter*in grundsätzlich die Kontrolle darüber behalten soll, was mit den ihn*sie betreffenden Daten geschieht.

Aufgrund der rasanten technischen Entwicklung ist der Datenschutz in den letzten Jahren immer wichtiger geworden, da das Sammeln von Daten technisch immer einfacher geworden ist. Die heutigen Möglichkeiten waren vor 30 oder 40 Jahren kaum abzusehen.

Umso höher ist die Leistung des BVerfG einzuschätzen, bereits damals die Grundlagen für den Datenschutz gelegt zu haben.

Es geht um personenbezogene Daten

Beim Datenschutz geht es weder um den reinen Selbstzweck noch um die Daten an sich. Vielmehr ist der Datenschutz zum Wohl der Menschen da.

Deshalb geht es im Datenschutz auch nicht um irgendwelche Daten, sondern konkret um personenbezogene Daten. Dafür reicht es allerdings aus, dass Daten zumindest mittelbar einer Person zuzuordnen sind.

BEISPIEL

„Halbanonyme" Zeiterfassung

Das elektronische Zeiterfassungssystem in einem kirchlichen Krankenhaus weist in der Software lediglich die Anwesenheitszeiten von „Mitarbeiter*in 1, Mitarbeiter*in 2, Mitarbeiter*in 3" usw. entsprechend der jeweiligen Mitarbeitendenkarte aus.

Aus einer vom Dienstgeber geführten Liste ergibt sich aber, welche*r namentlich in der Liste benannte Mitarbeiter*in welche Mitarbeitendenkarte für die Zeiterfassung erhalten hat.

In diesem Fall handelt es sich um personenbezogene Daten, weil die hinter der zunächst für sich genommen anonymen Karte stehende Person identifizierbar ist.

DSGVO | Lesezeit 3 Minuten

Das sind die wichtigsten 5 Grundpfeiler der DSGVO

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. Sie gelten zumindest mittelbar auch im kirchlichen Arbeitsrecht und finden sich regelmäßig auch in den kirchlichen Datenschutzgesetzen wieder. Einige der wichtigsten Grundpfeiler werden nachfolgend dargestellt. Dabei sind im Grunde auch Sie selbst als MAV eine Art „Pfeiler“ des Datenschutzes – wie Sie auf Seite 6 + 7 lesen können.

Grundpfeiler 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).

Grundpfeiler 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*die Verantwortliche nachzukommen hat. Verantwortlich ist im Bereich des kirchlichen Arbeitsrechts der*die Dienstgebende.

Der*Die Dienstgebende hat dem*der Mitarbeitenden unter anderem mitzuteilen:

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

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

Grundpfeiler 3: Auskunftsrecht (Art. 15)

Der*Die betroffene Mitarbeitende 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 beim*bei der betroffenen Mitarbeitenden erhoben wurden

Grundpfeiler 4: Recht auf Löschung (Art. 17)

Was nicht mehr gebraucht wird, muss entsorgt werden. Niemand soll unnötig Daten „horten“ dürfen.

Daher kann der*die betroffene Mitarbeitende vom*von der Dienstgebenden 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*die Mitarbeitende seine*ihre Einwilligung widerrufen hat und es keine sonstige Rechtsgrundlage für die Verarbeitung gibt,
- die Daten unrechtmäßig verarbeitet wurden.

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

Der*Die verantwortliche Dienstgebende muss bei der Datenverarbeitung aber auch dann für Ordnung sorgen, wenn kein*e betroffene*r Mitarbeiter*in Auskunft oder Löschung verlangt oder sonstige Rechte geltend macht.

Vielmehr muss er*sie sozusagen schon von sich aus seine*ihre Datensammlung in Ordnung halten und dies auch jederzeit nachweisen können. Es reicht also nicht, wenn der*die Dienstgebende erst dann anfängt, sich mit der Ordnungsgemäßheit seiner Datenverarbeitung zu beschäftigen, wenn ein*e Mitarbeiter*in „aktiv“ wird.

Der*Die Dienstgebende 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*die Dienstgeber*in eine Nachweispflicht gemäß Art. 5 Abs. 2 DSGVO. Er*Sie muss jederzeit den Nachweis führen können, dass er*sie die hier genannten Pflichten eingehalten hat.

Kirchlicher Datenschutz | Lesezeit 3 Minuten

So sieht die Grundstruktur des kirchlichen Datenschutzes aus

Der Datenschutz ist schon von seiner Grundstruktur her darauf angelegt, auf keinen Fall zu viel zuzulassen. Bei der Datenverarbeitung besteht nämlich ein „grundsätzliches Verbot mit Erlaubnisvorbehalt". Dieser etwas sperrige Rechtsbegriff bedeutet, dass jegliche Datenverarbeitung zunächst einmal verboten ist – es sei denn, sie ist im Einzelfall zugelassen.

Die Verarbeitung von personenbezogenen Daten ist nur gestattet, wenn die in § 6 KDG bzw. § 6 DSG-EKD genannten Bedingungen erfüllt sind. Danach ist eine Datenverarbeitung insbesondere zulässig, wenn

- eine Einwilligung des*der Betroffenen vorliegt oder
- eine Rechtsvorschrift die Datenverarbeitung erlaubt.

Möglichkeit 1: Einwilligung als Basis

An eine Einwilligung sind recht hohe Anforderungen zu stellen. Sie muss gemäß § 4 Nr. 13 KDG bzw. § 4 Nr. 13 DSG-EKD

- freiwillig,
- in informierter Weise und
- unmissverständlich

erfolgen.

Es soll unbedingt vermieden werden, dass die Einwilligung „so nebenbei als kleine Formalie" erteilt wird. Der*Die Betroffene soll sich über die Bedeutung seiner*ihrer Einwilligung im Klaren sein.

Dem dient auch die vorgeschriebene Schriftform. Eine Ausnahme vom Schriftformerfordernis soll jedenfalls nur ausnahmsweise gelten, wenn aufgrund „besonderer Umstände eine andere Form angemessen" ist. Zudem muss der*die Betroffene über den Zweck der Datenverarbeitung und über sein*ihr Widerrufsrecht aufgeklärt werden.

Angesichts der regelmäßigen Abhängigkeit im Beschäftigungsverhältnis kann man die Frage aufwerfen, ob überhaupt eine „freiwillige" Einwilligung eines*einer Mitarbeitenden gegenüber dem*der Dienstgebenden möglich ist.

Nach der Rechtsprechung des Bundesarbeitsgerichts soll das aber möglich sein. Gemäß § 49 Abs. 3 DSG-EKD ist jedoch bei der Beurteilung der Freiwilligkeit die Abhängigkeit im Beschäftigungsverhältnis zu berücksichtigen. Außerdem bedarf die Einwilligung auch nach dieser Vorschrift grundsätzlich der Schriftform.

Möglichkeit 2: Rechtsvorschrift als Basis

Auch ohne Einwilligung kann die Verarbeitung personenbezogener Daten im Arbeitsverhältnis erlaubt sein, insbesondere wenn eine Rechtsvorschrift die Verarbeitung gestattet.

Solche Rechtsvorschriften speziell für den Bereich von Arbeitsverhältnissen enthalten § 53 KDG bzw. § 49 DSG-EKD. Danach dürfen Daten verarbeitet werden, soweit dies zur

- Begründung,
- Durchführung oder
- Beendigung oder Abwicklung

des Beschäftigungsverhältnisses erforderlich ist.

Im Zusammenhang mit dem Verdacht auf Straftaten ist eine Datenverarbeitung zulässig, solange der Verdacht nicht ausgeräumt ist und die Interessen von möglichen Betroffenen dies erfordern.

Das versteht man unter Datenverarbeitung

Nun haben Sie schon einiges darüber erfahren, unter welchen Voraussetzungen Datenverarbeitung zulässig ist. Was aber ist denn eigentlich Datenverarbeitung? Haben Sie sich das auch schon mal gefragt?

Der Begriff begegnet einem heutzutage so oft, dass man seine Bedeutung leicht für selbstverständlich halten kann. Es ist aber durchaus wichtig, die genaue juristische Definition von Datenverarbeitung zu kennen. Denn für Vorgänge, die nicht unter diesen Begriff fallen, besteht eben kein besonderer Schutz nach Datenschutzrecht.

Glücklicherweise ist die Definition der „Verarbeitung" von Daten aber ziemlich umfassend, sodass folglich der Schutzbereich für Ihre Kolleg*innen sehr weit geht.

Unter die Verarbeitung von Daten fallen nach § 4 Nr. 3 KDG bzw. § 4 Nr. 3 DSG-EKD:

- das Erheben
- das Erfassen
- die Organisation
- das Ordnen
- die Speicherung
- die Anpassung oder Veränderung,
- das Auslesen
- das Abfragen
- die Verwendung
- die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung
- der Abgleich oder die Verknüpfung
- die Einschränkung
- das Löschen oder die Vernichtung

Was genau personenbezogenen Daten sind

Personenbezogene Daten sind gemäß § 4 Nr. 1 KDG bzw. § 4 Nr. 1 DSG-EKD alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Daten sind also auch dann personenbezogen, wenn man sie nicht unmittelbar einer Person zuordnen kann, aber diese Zuordnung beispielsweise mithilfe einer anderen Datensammlung erfolgen kann – wie in dem Beispiel auf **Seite 3**.

Ihre Rechte als MAV bei der Verarbeitung personenbezogener Daten finden Sie auf den beiden folgenden Seiten.

Mitbestimmung MAV | Lesezeit 7 Minuten

Beim Datenschutz mischen Sie als MAV mit

Datenschutz und Mitbestimmung haben auf den ersten Blick nicht viel miteinander zu tun. Auf den zweiten Blick sieht das aber ein bisschen anders aus. Zwar gibt es kein spezifisches Mitbestimmungsrecht zum Datenschutz, jedoch mehrere Mitbestimmungsrechte, die im Zusammenhang mit dem Datenschutz eine Rolle spielen können.

Gemäß § 53 Abs. 4 KDG werden Ihre Beteiligungsrechte als MAV durch die Regelungen zum Datenschutz nicht eingeschränkt.

Das DSG-EKD enthält eine solche klarstellende Regelung nicht, legt aber ebenfalls keine Einschränkungen der Beteiligungsrechte der MAV fest.

So reden Sie als MAV bei technischen Einrichtungen mit

Im katholischen Bereich gilt: Gemäß § 36 Abs. 1 Nr. 9 MAVO bedürfen die Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Mitarbeitenden zu überwachen, Ihrer Zustimmung als MAV.

Im evangelischen Bereich gilt: Gemäß § 40j) MVG-EKD haben Sie als MAV ein Mitbestimmungsrecht bei der Einführung und Anwendung von Maßnahmen oder technischen Einrichtungen, die dazu geeignet sind, das Verhalten oder die Leistung der Mitarbeitenden zu überwachen.

Inhaltlich besteht kein wesentlicher Unterschied zwischen der Regelung im katholischen Bereich und der Regelung im evangelischen Bereich.

Bei der Frage, ob eine technische Einrichtung gemäß der katholischen Regelung zur Überwachung „bestimmt" ist, kommt es nicht auf die subjektive Zielrichtung des*der Dienstgebenden an, sondern nur auf die „objektive" Bestimmung, also letztlich auch wie in der evangelischen Regelung nur darauf, ob die technische Einrichtung zur Überwachung geeignet ist.

Es kommt auf den Gestaltungsspielraum an, ob Sie mitbestimmen dürfen

Voraussetzung für Ihr Mitbestimmungsrecht ist aber stets, dass dem*der Dienstgebenden überhaupt noch ein **Gestaltungsspielraum** verbleibt.

Wenn der*die Dienstgebende nach den gesetzlichen Vorgaben oder sonstigen einschlägigen Vorschriften zwingend eine ganz bestimmte Handlung vornehmen muss, fehlt es an einem solchen Gestaltungsspielraum.

Dann entfällt automatisch auch Ihr Mitbestimmungsrecht. Denn in solchen Fällen gibt es eben keine verschiedenen Handlungsoptionen, an deren Auswahl Sie als MAV beteiligt werden könnten.

Ein solches Mitbestimmungsrecht kommt insbesondere in Betracht bei Einführung oder Anwendung von:

- elektronischer Zeiterfassung
- elektronischen Arbeitszeitkonten
- elektronischen Personalakten
- Videoüberwachung
- elektronischen Zugangskontrollen

BEISPIEL

Elektronisches Arbeitszeitkonto

Ihr Dienstgeber möchte das bereits vorhandene Arbeitszeitkonto, das bislang handschriftlich geführt wurde, auf elektronische Zeiterfassung umstellen.

Der Dienstgeber beteuert, dass es ihm nur um eine effizientere Abwicklung des Arbeitszeitkontos gehe und nicht um eine Überwachung. Dies spielt jedoch keine Rolle. Ihr Mitbestimmungsrecht als MAV besteht, da eine elektronische Zeiterfassung jedenfalls geeignet bzw. objektiv bestimmt ist, Mitarbeitende bei ihrer Arbeitszeit zu überwachen.

So bestimmen Sie als MAV bei Personalfragebögen mit

Im katholischen Bereich gilt: Gemäß § 36 Abs. 1 Nr. 5 MAVO bedarf der Inhalt von Personalfragebögen für Mitarbeiterinnen und Mitarbeiter der Zustimmung der MAV.

Im evangelischen Bereich gilt: Gemäß § 39a) MVG-EKD hat die MAV ein Mitbestimmungsrecht bezüglich Inhalt und Verwendung von Personalfragebögen und sonstigen Fragebogen zur Erhebung personenbezogener Daten, soweit nicht eine gesetzliche Regelung besteht.

BEISPIEL

Fragebögen für Bewerber*innen

Ihr Dienstgeber möchte Bewerberfragebögen einführen. Wie Sie gehört haben, sollen darin auch Fragen nach einer Schwangerschaft enthalten sein. In diesem Fall können Sie durch Ihr Mitbestimmungsrecht verhindern, dass eine solche unzulässige Frage in den Fragebogen aufgenommen wird.

Zwar muss ein*e Bewerber*in eine unzulässige Frage nicht wahrheitsgemäß beantworten. Aber das ist dem*der Bewerber*in vielleicht nicht bekannt. Außerdem befindet er*sie sich in einer Drucksituation, sodass er*sie die Frage vielleicht doch beantwortet. Als MAV haben Sie die Möglichkeit, dafür zu sorgen, dass Bewerber*nnen erst gar nicht in eine solche Situation kommen. Diese Möglichkeit sollten Sie unbedingt nutzen.

Personalfragebögen müssen nicht als solche bezeichnet sein. Nicht die Bezeichnung, sondern der Inhalt ist entscheidend. Ein

Personalfragebogen im rechtlichen Sinne liegt vor, wenn standardisiert personenbezogene Fragen zu beantworten sind. So können beispielsweise auch folgende Dokumente und Einrichtungen Personalfragenbögen sein, die ein Mitbestimmungsrecht auslösen:

- Arbeitsplatzerhebungsbögen
- Checklisten
- formalisierte Krankenrückkehrgespräche

Mit Dienstvereinbarungen Datenverarbeitung mitgestalten

Gemäß § 88 Abs. 2 Datenschutz-Grundverordnung (DSGVO) können durch Kollektivvereinbarungen, also auch durch Dienstvereinbarungen, im kirchlichen Bereich „spezifischere Vorschriften" zum Datenschutz eingeführt werden. Sie haben also als MAV gemeinsam mit dem*der Arbeitgebenden einen gewissen Gestaltungsspielraum, den Datenschutz im konkreten Fall in Ihrer Einrichtung im Rahmen der gesetzlichen Vorschriften zu konkretisieren. Dies gilt insbesondere in den Bereichen:

- Einstellung
- Erfüllung der arbeitsvertraglichen Pflichten, die durch Vertrag, Gesetz oder Kollektivvereinbarung festgelegt sind
- individuelle und kollektive Rechte der Mitarbeitenden
- Arbeitsplanung, Arbeitsorganisation
- Arbeits- und Gesundheitsschutz
- Schutz des Eigentums des*der Dienstgebenden
- Schutz des Kund*inneneigentums
- Beendigung des Arbeitsverhältnisses

Gemäß § 38 Abs. 1 Nr. 12 MAVO kann über Maßnahmen zur Verhütung von Dienst- und Arbeitsunfällen und sonstigen Gesundheitsgefahren, also auch über ein Betriebliches Eingliederungsmanagement (BEM), eine Dienstvereinbarung abgeschlossen werden. Im Bereich der evangelischen Kirche ergibt sich die Zulässigkeit aus § 36 MVG-EKD.

MEIN TIPP

Nutzen Sie Ihren Spielraum

Gehen Sie das Thema Datenschutz und Dienstvereinbarung gemeinsam mit Ihrem*Ihrer Dienstgebenden offensiv an. Machen Sie sich klar, dass Sie bei Dienstvereinbarungen hinsichtlich des Datenschutzes immer 2 Seiten betrachten sollten:

Einerseits müssen die Dienstvereinbarungen die gesetzlichen Grenzen des Datenschutzes beachten.

Andererseits haben Sie gemeinsam mit dem*der Dienstgebenden aber auch die Möglichkeit, Datenschutzregelungen im Rahmen der Gesetze selbst zu schaffen. Diesen Spielraum sollten Sie zum Wohle der Mitarbeitenden in Ihrer Einrichtung nutzen.

Starten Sie eine „Entrümpelungsaktion"

Einerseits haben Sie als MAV wie gezeigt gemeinsam mit dem*der Dienstgebenden die Möglichkeit, Rechtsgrundlagen im Bereich des Datenschutzes durch Dienstvereinbarungen zu schaffen. Andererseits können Sie diese Rechtsgrundlagen natürlich nicht „nach Lust und Laune" schaffen, sondern müssen sich im Rahmen der Gesetze und insbesondere im Rahmen der DSGVO halten.

Beachten Sie dabei, dass die DSGVO auch für bereits bestehende Dienstvereinbarungen, also für den „Altbestand", gilt. Am besten sollten Sie als MAV daher gemeinsam mit dem*der Arbeitgebenden eine „Entrümpelungsaktion" starten und alle Dienstvereinbarungen kritisch daraufhin durchsehen, ob sie möglicherweise nicht mehr den aktuellen Datenschutzvorgaben entsprechen.

WICHTIGER HINWEIS!

Auch Sie als MAV können Adressat des Datenschutzes sein

Der Datenschutz gibt Ihnen als MAV nicht nur Rechte, sondern legt Ihnen – möglicherweise – auch Pflichten auf. Zumindest teilweise wird in der Rechtsprechung die Auffassung vertreten, dass eine Arbeitnehmerinteressenvertretung wie ein Betriebsrat oder eine MAV neben dem*der Arbeit-/Dienstgebenden ebenfalls ein „Verantwortlicher" im Sinne des Datenschutzes sei. Prüfen Sie als MAV daher vorsichtshalber, welche personenbezogenen Daten, die Sie im Zusammenhang mit der MAV-Tätigkeit erhalten haben, noch benötigt werden. Daten, die Sie nicht mehr benötigen, sollten Sie löschen.

Überwachung | Lesezeit 3 Minuten

So setzt der Datenschutz der Überwachung Grenzen

Wer hat nicht gerne alles unter Kontrolle? Da sind Dienstgebende sicherlich grundsätzlich nicht anders gestrickt als jede*r von uns. Aber anders als im privaten Bereich gilt in einem Dienstverhältnis der Datenschutz. Dieser setzt dem Kontrollbestreben Ihres*Ihrer Dienstgebenden Grenzen.

Auf der anderen Seite ist aber auch nicht jegliche Überwachung verboten. Der Datenschutz in Gestalt von Gesetzgebung und Rechtsprechung sieht durchaus beide Seiten der Medaille und versucht, einen vernünftigen Ausgleich vorzunehmen und eine gerechte Bewertung der einzelnen Fälle zu erreichen.

Videoüberwachung ist nur unter bestimmten Umständen erlaubt

Ein*e Arbeit- bzw. Dienstgeber*in darf nicht generell seine Mitarbeitenden per Video überwachen. Im Einzelfall kann es aber durchaus erlaubt sein, eine*n Mitarbeiter*in, der*die „lange Finger" macht, per Videokamera zu überführen.

BEISPIEL

Verwertung eines Videos trotz Verstoßes

Ein Autohaus betrieb unter anderem ein Ersatzteillager. Bei Inventuren wurden dort erhebliche Fehlbestände festgestellt. Nachdem andere Maßnahmen keine Aufklärung gebracht hatten, ließ der Arbeitgeber eine Videokamera im Ersatzteillager installieren. Den Betriebsrat beteiligte der Arbeitgeber dabei nicht. Durch die Videoüberwachung kam der Arbeitgeber einem Mitarbeiter auf die Schliche, der Bremsklötze entwendete.

Der Mitarbeiter berief sich im Kündigungsschutzprozess darauf, der Arbeitgeber habe die Videoaufzeichnungen unter Verstoß gegen Mitbestimmungsrecht und Datenschutz erlangt und dürfe sie daher im Prozess nicht verwerten.

Das sah das Bundesarbeitsgericht anders (BAG, 20.10.2016, Az. 2 AzR 395/15). Ein Verstoß gegen Mitbestimmungsrechte des Betriebsrats führe nicht automatisch zu einem Verwertungsverbot. Vielmehr sei zu prüfen, ob die Überwachungsmaßnahme auch im Verhältnis zu dem betroffenen Mitarbeiter rechtswidrig war.

Dabei komme es vor allem darauf an, ob die Maßnahme verhältnismäßig war und andere Mittel der Aufklärung ausgeschöpft waren.

Sie haben als MAV Einfluss – aber begrenzt

Zusammenfassend lässt sich für Sie als MAV festhalten:

Auch das kirchliche Mitarbeitervertretungsrecht sieht wie gezeigt ein Mitbestimmungsrecht bei der Überwachung durch technische Einrichtungen – also auch bei Videoüberwachung – vor. Solche Maßnahmen sind gemäß § 36 Abs. 1 Nr. 9 MAVO bzw. § 40j) MVG-EKD mitbestimmungspflichtig.

Aber: Auch wenn der*die Dienstgebende ohne Ihre Beteiligung als MAV eine Videoüberwachung durchführen lässt, kann es sein, dass er*sie die daraus gewonnenen Erkenntnisse trotzdem im Prozess gegen eine*n Mitarbeiter*in verwenden darf. Es kommt dann nämlich wie gezeigt nur darauf an, ob die Maßnahme auch gegenüber diesem Mitarbeiter bzw. dieser Mitarbeiterin unzulässig war.

Auch eine „manuelle" Datensammlung hat Grenzen

Daten kann man nicht nur durch die Videoüberwachung oder sonstige technische Mittel beschaffen, sondern auch ganz „manuell" – z. B. durch das Beauftragen eines Detektivbüros. Aber auch eine solche Datensammlung ist nicht unbeschränkt erlaubt.

BEISPIEL

Detektivkosten zahlt am Ende der Mitarbeiter

Eine Firma, die Stanzwerkzeuge herstellte, entdeckte, dass einer ihrer Mitarbeiter mit seiner Familie selbst Stanzformen auf dem Markt anbot. Daraufhin schaltete die Firma ein Detektivbüro ein. Dieses fand heraus, dass der Mitarbeiter tatsächlich seinem Arbeitgeber Konkurrenz machte – was natürlich verboten ist.

Die Firma kündigte dem Mitarbeiter fristlos und verlangte im Kündigungsschutzprozess auch noch, dass der Mitarbeiter die Kosten für den Einsatz des Detektivbüros übernehmen solle.

Das sah das BAG (29.6.2017, Az. 2 AzR 597/16) grundsätzlich genauso. Wenn der Einsatz des Detektivbüros verhältnismäßig gewesen sei, komme auch eine Kostenübernahme durch den Mitarbeiter in Betracht. Hierzu müsse das Landesarbeitsgericht aber noch einmal die genauen Umstände aufklären.

Im kirchlichen Bereich gibt es keine „Konkurrenz" – aber leider manchmal Kriminalität

Auch wenn Konkurrenztätigkeit im hier beschriebenen Sinne im kirchlichen Bereich nicht denkbar ist, kommt es doch auch unter kirchlichen Mitarbeitenden mitunter zu kriminellen Handlungen wie Diebstahl oder Unterschlagung. Dienstgebende haben dann ein Interesse an einer zweifelsfreien Aufklärung – eventuell auch durch den Einsatz eines Detektivbüros.

Die Kosten dafür kann der*die Arbeitgebende dann eventuell auf den*die Mitarbeiter*in abwälzen. Das gilt aber natürlich nur, wenn der Vorwurf auch tatsächlich nachgewiesen werden kann.

Daten im Prozess | 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.

Fall 1: Ein IT-Fachmann war seit 2011 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) fertigte.

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 Grundgesetz) verletzt. Die Informationsgewinnung war nicht nach § 32 Abs. 1 Bundesdatenschutzgesetz 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 insoweit findet also eine Art „Überwachung" personenbezogener Daten statt. Daher kann ein Anspruch auf Entfernung einer Abmahnung nicht nur aus den allgemeinen zivilrechtlichen Regelungen des Bürgerlichen Gesetzbuchs 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 Weisung des Arbeitgebers 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 Datenschutz-Grundverordnung 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 diene einem doppelten Zweck: Zum einen werde der Arbeitnehmer auf die vertraglichen Pflichten hingewiesen und auf eine Pflichtverletzung aufmerksam gemacht (Rüge- und Dokumentationsfunktion). Zum anderen würden 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

Manchmal gilt eine sehr spezielle Wahrheit

Die Rechtsprechung setzt hier den Datenschutz konsequent um. Das führt zu dem kuriosen Ergebnis, dass das Gericht von einem bestimmten Sachverhalt (hier: geringe Privatnutzung) ausgeht, obwohl alle Beteiligten wissen, dass ein anderer Sachverhalt (hier: erhebliche Privatnutzung) wahr ist. Es kommt nämlich im Prozess nur auf die nach den prozessualen Regeln wirksam festgestellte Wahrheit an.

FAZIT

Interesse an Abmahnung darlegen

Grundsätzlich sind Ihre Kolleg*innen jedenfalls 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. Entfernung der Abmahnung besteht. Wenn der*die Arbeitgebende meint, doch noch ein berechtigtes Interesse an der Aufbewahrung des Dokuments zu haben, muss er*sie dies darlegen.

Auskunftsrecht | Lesezeit 3 Minuten

So steht es um das Auskunftsrecht Ihrer Kolleg*innen über gespeicherte Daten

Arbeitnehmende 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. In dem 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 Information über Verstöße des Klägers geliefert hätten.

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 einen interessanten Hebel darstellen, 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 daher nicht.

So „eng" sieht das LAG Niedersachsen den Auskunftsanspruch

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 bzw. sah sie enger im Rahmen der Gesetze. 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 nichts 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 (Az. 6 ZR 576/19) einen recht weitgehenden Auskunftsanspruch angenommen hat, also eher der Linie des LAG Baden-Württemberg als derjenigen des LAG Niedersachen gefolgt ist. 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 (Az. 2 AZR 235/21) für den Bereich des Arbeitsrechts immerhin festgestellt, dass ein Klageantrag auf Auskunftserteilung nicht zu unbestimmt sein dürfe. Es reiche jedenfalls nicht aus, einfach nur den Gesetzeswortlaut des Art. 15 DSGVO zu wiederholen.

Das sind die Konsequenzen für die Praxis

Es scheint so, dass die Arbeitsgerichte im Moment überwiegend eher der zurückhaltenden Linie des LAG Niedersachsen folgen als der weiten Linie des LAG Baden-Württemberg und des BGH. Aber solange keine höchstrichterliche Klärung im arbeitsrechtlichen Bereich vorliegt, bleibt die Frage offen und spannend und kann in jedem neuen arbeitsgerichtlichen Verfahren wieder eine neue Antwort erhalten.

Einige Gerichte sehen es auch als rechtsmissbräuchlich, wenn ein datenschutzrechtlicher Auskunftsanspruch benutzt wird, um Ansprüche außerhalb des Datenschutzes durchzusetzen. Denn Ziel des Datenschutzes ist es ja, dass Menschen Kontrolle über ihre personenbezogenen Daten haben, aber nicht, dass sie sich eine günstige Position z. B. in einem Kündigungsschutzprozess verschaffen.

Auflösung Betriebsrat | Lesezeit 2 Minuten

Warnendes Beispiel: Auflösung des Betriebsrats nach Verstoß gegen Datenschutz

Der Datenschutz ist nicht nur ein Instrument, das Ihre Kolleg*innen schützt und Ihnen als MAV Mitwirkungsrechte einräumt. Sie müssen auch aufpassen, dass Sie nicht selbst gegen den Datenschutz verstoßen. Das Schicksal eines Betriebsrats kann als warnendes Beispiel dienen.

Der Fall: 2 Arbeitgeber in der Privatwirtschaft fassten den Entschluss, einen von ihnen gemeinschaftlich geführten Betrieb stillzulegen, und kündigten daher allen Mitarbeitenden. Der Betriebsrat versandte daraufhin eine E-Mail an die Anwälte der Kolleg*innen, die gegen die Kündigung geklagt hatten. Mit dieser E-Mail wurde unter anderem eine große Datenmenge (mehr als 150 MB) zur Verfügung gestellt, die der Betriebsrat über bestimmte Mitglieder systematisch gesammelt hatte. Dabei ging es auch um nicht anonymisierte Listen von Kolleg*innen mit personenbezogenen Daten wie Tätigkeit, Entgeltgruppe usw. sowie Bescheinigungen über schwangere Mitarbeiterinnen.

Die beiden Arbeitgeber beantragten daraufhin die Auflösung des Betriebsrats.

Die Entscheidung: Das Arbeitsgericht Iserlohn (14.1.2020, Az. 2 BV 5/19) löste den Betriebsrat antragsgemäß auf, und zwar nach § 23 Abs. 1 Satz 1 Betriebsverfassungsgesetz wegen groben Pflichtverstoßes. Auf ein Verschulden komme es nicht an. Der Betriebsrat müsse sich das Handeln seines Vorsitzenden und eines Betriebsratsmitglieds zurechnen lassen, weil der ganze Betriebsrat das Handeln geduldet habe. Insbesondere das systematische Sammeln von Daten beanstandete das Gericht.

FAZIT

Halten Sie den Datenschutz ein

Auch die kirchlichen Gesetze (§ 13 Abs. 3 Ziff. 6 MAVO im katholischen Bereich und § 17 MVG.EKD im evangelischen Bereich) sehen die Möglichkeit einer Auflösung der MAV bei schweren Verstößen vor. Sie müssen daher zwar nicht gleich bei jedem Fehler, der Ihnen möglicherweise im Datenschutz mal unterläuft, gleich eine Auflösung Ihres Gremiums fürchten.

Aber Sie sollten eben den Datenschutz auch nicht völlig und systematisch ignorieren, indem Sie dauerhaft und gezielt dagegen verstoßen.

Social Media | Lesezeit 2 Minuten

Facebook-Auftritt des Unternehmens unterliegt der Mitbestimmung

Manche Leute glauben, im Internet seien die Regeln etwas lockerer und man könne diesen Bereich ohnehin nicht wirksam beeinflussen. Dies ist aber keineswegs so, wie der folgende Fall zeigt.

Der Fall: Der Arbeitgeber, der Blutspendedienste betrieb, richtete im April 2013 bei Facebook eine Seite zu Marketingzwecken ein. Bei Facebook registrierte Nutzer konnten dort Postings einstellen.

Einige Facebook-Nutzer machten davon eifrig Gebrauch und bewerteten das Verhalten von Mitarbeitenden bei den vom Arbeitgeber betriebenen Blutspendediensten. Die Mitarbeitenden kamen bei diesen Bewertungen wohl nicht immer gut weg.

Der Betriebsrat wollte die Mitarbeitenden schützen und machte geltend, der Arbeitgeber dürfe solche Postings gar nicht veröffentlichen, ohne den Betriebsrat dabei mitbestimmen zu lassen. Dies gelte auch für den Betrieb von weiteren Auswertungsmöglichkeiten auf der Facebook-Seite.

Die Entscheidung: Der Betriebsrat hatte vor dem Bundesarbeitsgericht (BAG) im Wesentlichen Erfolg, nachdem das Landesarbeitsgericht zuvor noch anders entschieden hatte (BAG, 13.12.2016, Az. 1 ABR 7/15).

Das BAG urteilte, die Entscheidung des Arbeitgebers, Postings von Nutzern auf der Facebook-Seite unmittelbar zu veröffentlichen, unterliege der Mitbestimmung. Postings, die sich auf das Verhalten von Arbeitnehmenden beziehen, führen nämlich nach Ansicht des BAG zu einer Überwachung von Arbeitnehmenden durch eine technische Einrichtung im Sinne des § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz.

FAZIT

Facebook ist kein rechtsfreier Raum

Auch das kirchliche Recht sieht ein entsprechendes Mitbestimmungsrecht vor, nämlich in § 35 Abs. 1 Nr. 9 MAVO bzw. in § 40j) MVG-EKD. Facebook ist also auch im kirchlichen Bereich kein rechtsfreier Raum. Warnen Sie ggf. Ihre Kolleg*innen vor unbedachten Äußerungen.

Hinweisgeberschutz | Lesezeit 1 Minute

So reden Sie bei der Hinweisgeberstelle mit

Wie Sie sehen konnten, geht es in vielen Vorschriften darum, Daten vor bestimmten Zugriffen zu schützen. Manchmal kann es aber auch wünschenswert sein, dass bestimmte Daten zur Aufdeckung von Straftaten nicht unbekannt bleiben. Das betrifft explizit die Beziehung zwischen Arbeitgebenden und Mitarbeitenden. 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 aus dem Jahr 2023 gilt für Unternehmen ab 50 Mitarbeiter*innen. Ziel des Gesetzes ist es, sogenannten Whistleblowern Schutz zu bieten. Dieser englische Begriff bezeichnet Personen, die jemanden „verpfeifen" – ohne dass damit der negative Beigeschmack verbunden wäre, den das deutsche Wort hat. Vielmehr ist dieser Begriff im Rahmen des neuen Gesetzes grundsätzlich positiv besetzt. Der Schutz der Whistleblower soll zur Aufdeckung von Missständen und Straftaten in Unternehmen beitragen.

Unternehmen, die dem Gesetz unterfallen, werden verpflichtet, interne Meldestellen einzurichten. Es werden aber auch staatlicherseits externe Meldestellen eingerichtet bei diversen Ämtern, z. B. beim Bundesjustizamt.

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".

Dieses Wort bedeutet, dass der Gesetzgeber schon eine Präferenz erkennen lässt, aber eben keine Verbindlichkeit schafft.

In bestimmten Fällen reden Sie als MAV mit

Richtet der*die Arbeitgebende eine interne Meldestelle ein, ist diese als solche mitbestimmungsfrei. Allerdings unterliegt es der Mitbestimmung, wenn ein*e Arbeitgeber*in eine Meldepflicht bei einer internen Stelle schaffen will. Dasselbe soll auch gelten bei der Einführung verbindlicher Regelungen für Meldewege.

So ist es neben dem weltlichen Bereich nach dem Betriebsverfassungsgesetz jedenfalls auch im evangelischen Bereich nach § 40j) MVG-EKD, während im katholischen Bereich eine entsprechende Mitbestimmungsvorschrift fehlt.

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