www.arbeitnehmerkammer.de

Arbeitnehmerkammer
Bremen

Veranstaltungsdokumentation

Veranstaltung 6 der Veranstaltungsreihe „Alles im Blick“ für neu gewählte Personalräte:

Datenschutz und Digitalisierung

Welche Beteiligungsrechte hat der Personalrat?

Zu den Aufgaben des Personalrats gehört die Mitbestimmung bei der Einführung und Anwendung von IT-Systemen, die zur Leistungs- und Verhaltenskontrolle der Beschäftigten geeignet sind. Da dies in der Regel gegeben ist, muss der Arbeitgeber die Zustimmung des Personalrats einholen bevor ein neues IT-System oder ein wesentliches Update eines bestehenden Systems in Betrieb genommen wird.

Unabhängig von konkreten Mitbestimmungsfällen hat der Personalrat darüber hinaus zu kontrollieren, ob beim Einsatz von IT-Systemen und der damit verbundenen Verarbeitung von Beschäftigtendaten die gesetzlichen Datenschutzbestimmungen eingehalten werden. Auf Grundlage und mit Hilfe dieser Rechtspositionen, die in den Personalvertretungs-gesetzen abgesichert sind, kann sich der Personalrat an der Ausgestaltung von IT-Systemen beteiligen, eigene Vorstellungen dabei geltend machen und dies in Form entsprechender Dienstvereinbarungen verpflichtend regeln. Oftmals geht es dabei um die Begrenzung der Möglichkeiten zur Leistungs- und Verhaltenskontrolle, die mit den technischen Funktionen der verschiedenen Systeme fast immer gegeben sind.

Umsetzung und Ausgestaltung der Datenschutzvorschriften

Wenn der Personalrat Beschäftigte vor einer allzu ausgreifenden Sammlung und Auswertung von Daten über die eigene Person schützen will, beginnt er nicht bei Null. In seinen Datenschutzgesetzen formuliert der Gesetzgeber einschränkende Bedingungen für das, was in dieser Frage erlaubt ist. Diese Regelungen zielen auf den Schutz der in der Verfassung garantierten Persönlichkeitsrechte des Einzelnen. Ob mit der Umsetzung des Datenschutzes im Betrieb bzw. der Dienststelle dieses Schutzniveau und die Interessen der Belegschaft hinreichend gewahrt sind, muss der Personalrat im Einzelfall beurteilen. Die Aufsichtsbehörden für den Datenschutz empfehlen jedenfalls ausdrücklich den Abschluss von Dienstvereinbarungen, um den gesetzlichen Datenschutz im Hinblick auf die jeweiligen betrieblichen Gegebenheiten im Sinne der Betroffenen zu konkretisieren.

Welche Grundprinzipien des Datenschutzes müssen beachtet werden?

Die EU-Datenschutzgrundverordnung - das "Grundgesetz" des Datenschutzes - besteht in ihren wesentlichen Teilen darin, die nachstehend genannten Prinzipien zu konkretisieren. Die Prinzipien selber sind in Artikel 5 der Datenschutzgrundverordnung in grundsätzlicher Weise verpflichtend gemacht.

Rechtmäßigkeit, Verarbeitung für legitime Zwecke

Die Verarbeitung von personenbezogenen Daten ist grundsätzlich verboten, es sei denn eine Rechtsnorm, in der Regel ein Gesetz, erlaubt eine konkrete Verarbeitung. Verarbeitet eine Dienstelle also personenbezogene Daten, müssen die Zwecke der Verarbeitung konkret und

eindeutig benannt sein und für diese Verarbeitungszwecke muss ein Erlaubnistatbestand vorliegen, also eine rechtliche Regelung, die diese Verarbeitung legitimiert.

Wesentliche Regelungen finden sich in der Datenschutzgrundverordnung selbst. Dort ist z.B. festgelegt, dass im Sinne des Rechts auf informationelle Selbstbestimmung eine Verarbeitung in jedem Fall dann legitim ist, wenn der Betroffene ihr aus freien Stücken zugestimmt hat. Der Arbeitnehmerdatenschutz, der Bereich für den der Personalrat zuständig ist, ist gesondert in § 26 des Bundesdatenschutzgesetzes geregelt.

Demnach ist die Verarbeitung von Beschäftigtendaten zulässig, wenn sie der Durchführung des Beschäftigungsverhältnisses dient und erforderlich ist. Die Erforderlichkeit ist vielfach fraglos gegeben, z.B. im Rahmen der Gehaltsabrechnung. Sie liegt aber nicht allein schon deshalb vor, weil eine Datenverarbeitung für die Interessen des Arbeitgebers bzw. der Dienststelle nützlich ist. Hier haben die Arbeitsgerichte in ihrer Rechtsprechung weitergehende Bedingungen formuliert und den Begriff der Erforderlichkeit konkretisiert.

Wenn ein Verarbeitungszweck in zumutbarer Weise durch andere Mittel erreicht werden kann, die ohne die Verarbeitung personenbezogener Daten auskommen, muss eine entsprechende Datenverarbeitung unterbleiben. Ebenso müssen schutzwürdige Interessen der Betroffenen berücksichtigt werden und es ist zu prüfen, ob diese Interessen im Sinne der Verhältnismäßigkeit überwiegen und eine Verarbeitung ausschließen.

Zweckbindung

Das Speichern von personenbezogenen Daten für eine noch unbestimmte Verwendung stellt eine unzulässige Vorratsdatenspeicherung dar. Bereits beim Erheben von Daten muss deren legitimer Verarbeitungszweck festgelegt sein. Die spätere Änderung des Verarbeitungszwecks unterliegt strengen Einschränkungen und muss mit der ursprünglichen Zwecksetzung vereinbar sein.

Datenminimierung und Speicherbegrenzung

Weil jede Verarbeitung von Daten einen Eingriff in das Persönlichkeitsrecht der Betroffen darstellt, sollten so wenig Daten wie möglich erhoben werden, ihr Umfang also auf das für den Verarbeitungszweck absolut notwendige Maß beschränkt bleiben. Der Grundsatz der Speicherbegrenzung erfordert, dass die Daten nur so lange gespeichert bleiben, wie es für den Verarbeitungszweck wirklich notwendig ist. Um dies sicherzustellen, sollte der Verantwortliche von vornherein Fristen für ihre Löschung festlegen oder regelmäßig überprüfen, ob Daten gelöscht werden können. Ebenso ist zu prüfen, ob der Personenbezug in Datenbeständen benötigt wird oder Daten anonymisiert bzw. pseudonymisiert werden können.

Richtigkeit, Integrität und Vertraulichkeit

Daten müssen soweit erfordert auf dem neuesten Stand sein und unrichtige Daten sind umgehend zu löschen bzw. zu korrigieren. Ansonsten muss der Verantwortliche alles Zumutbare unternehmen, um zu verhindern, dass Daten manipuliert werden, verloren gehen oder in falsche Hände geraten. Zu diesen technisch-organisatorischen Maßnahmen, die die Datensicherheit gewährleisten sollen, zählen z.B. die Abwehr von Viren oder anderer Schadsoftware, die Vergabe von restriktiven Zugriffsrechten für die Datenverarbeitung, die Beschränkung des Zutritts bzw. Zugangs zu IT-Arbeitsplätzen, die Verschlüsselung von sensiblen Daten, die über das Internet übertragen werden und vieles andere mehr.

Transparenz

Oftmals - auch im Arbeitsverhältnis - weiß man nicht, oder jedenfalls nicht genau, welche Daten über die eigene Person gespeichert sind, was mit diesen Daten geschieht und welche - möglicherweise negative - Folge dies hat. Dies ist mit dem Grundrecht auf informationelle Selbstbestimmung schlecht vereinbar. Der Grundsatz der Transparenz ist deshalb ein zentraler Baustein der Datenschutzgrundverordnung. So ist der Verantwortliche verpflichtet die Betroffenen umfassend zu informieren, so dass sie die Verarbeitung ihrer Daten nachvollziehen können, also wissen, welche Daten in welchem Umfang verarbeitet werden, wer Zugang zu diesen Daten hat und auf welche Art und Weise und zu welchen Zwecken sie verarbeitet werden. Hierfür müssen alle Informationen und Mitteilungen leicht zugänglich und in klarer und verständlicher Sprache abgefasst sein. Die Informationspflicht des Arbeitgebers schließt weitergehend ein, die Beschäftigten über ihre Rechte in Bezug auf die Verarbeitung ihrer Daten zu informieren und darüber aufzuklären, wie sie ihre Rechte geltend machen können.

Unabhängig von der Informationspflicht des Verantwortlichen haben die Betroffenen das Recht, umfassende Auskunft über die oben genannten Umstände der Verarbeitung ihrer Daten zu verlangen. Bei Zweifeln über die Rechtmäßigkeit der Verarbeitung oder die Erfüllung von Informationspflichten kann man sich bei der Aufsichtsbehörde beschweren. Auf Wunsch werden solche Beschwerden anonym behandelt.

Rechenschaftspflicht

Der Arbeitgeber ist für die konkrete Umsetzung der oben genannten Grundsätze verantwortlich und muss ihre Einhaltung nachweisen können, ggf. auch gegenüber der Aufsichtsbehörde. Eine fehlende oder lückenhafte Dokumentation der Datenverarbeitung stellt schon einen Datenschutzverstoß dar. Für den Personalrat ist diese Dokumentation eine wichtige Grundlage um die Einhaltung von Datenschutzvorschriften kontrollieren zu können. So verlangt die Datenschutzgrundverordnung z.B. das Führen eines sogenannten Verzeichnisses der Verarbeitungstätigkeiten. Darin müssen für die einzelnen IT-Systeme

bzw. Verarbeitungsvorgänge folgende Punkte dokumentiert sein: der konkrete Zweck der jeweiligen Verarbeitung, ihre Rechtsgrundlage, die Kategorien der verarbeiteten Daten und der Kreis der Betroffenen. Ferner müssen die mögliche Übermittlung von Daten an Dritte, vorgesehene Löschfristen sowie eine Beschreibung der technisch-organisatorischen Maßnahmen zur Datensicherheit, also z.B. das Berechtigungskonzept für den Datenzugriff erfasst werden. Der Personalrat kann sich mit Hilfe dieses Verzeichnisses einen ersten Überblick darüber verschaffen, welche IT-Systeme Daten von Beschäftigten verarbeiten und was mit diesen Daten geschieht.

Welche wichtigen Eckpunkte sollten Dienstvereinbarungen unter dem Gesichtspunkt „Leistung- & Verhaltenskontrolle“ bei digitalen Technologien enthalten?

Es ist eigentlich unstrittig, dass bei der Einführung von Technologien, die zur Leistungs- und Verhaltenskontrolle geeignet sind, das Mitbestimmungsrecht von dem jeweils zuständigen Personalrat ausgelöst wird. Was auf den ersten Blick wie der Auftakt zur Ausarbeitung und Verhandlung einer entsprechenden Dienstvereinbarung erscheint, erweist sich in der Praxis häufig als langfristiger und komplizierter Prozess – sofern es überhaupt dazu kommt. Denn häufig herrscht Unsicherheit, was darunter fällt und was es alles zu beachten gilt. Im Folgenden werden Regelungsbereiche von Dienstvereinbarungen vorgestellt, die unabhängig vom jeweiligen Einsatzzweck eines IT-Systems bei eigentlich allen digitalen Technologien geregelt werden sollten.

Protokolldateien

Oft beginnt die Auseinandersetzung zwischen Personalrat und Dienstherren darüber, dass letztgenanntem die „Einsicht“ fehlt, dass die geplanten Technologien – auch aus dem Bereich „Digitalisierung“ – überhaupt mitbestimmungspflichtig sind. Hier wird vom Arbeitgeber gerne so argumentiert, dass bspw. eine neue Software gar nicht mit dem Zweck der Leistungs- und Verhaltenskontrolle eingeführt wird und deswegen auch nicht der Mitbestimmung unterliege. Das Mitbestimmungsrecht greift aber bereits dann, wenn die entsprechende Technologie zur Leistungs- und Verhaltenskontrolle geeignet (sic!) ist. Und für Softwares bzw. computergestützte Technologien gilt das fast ausnahmslos. Grund hierfür ist die Konzeption von Softwares und Computersystemen, die unter anderem Protokolldateien erstellen, um die Fehlersuche sowie die unberechtigte Nutzung der Software (oder das Nachverfolgen von Einbrüchen in das Softwaresystem) zu ermöglichen. Dazu wird unter anderem festhalten, wann, wie lange und ggf. auch von wo ein Zugriff auf die Software/das System erfolgt. Da in der Regel die Nutzung einer Software mit einem eindeutig identifizierbaren Account der Beschäftigten verknüpft ist, kann dann damit ihr Verhalten – und wie auch immer davon abgeleitet ihre Leistung – kontrolliert werden. Gleichzeitig ist die Erstellung von Protokolldateien aus den bereits genannten Gründen für den Einsatz der Software und Computersysteme unumgänglich. Hier bewegen sich der Personalrat also in einem Spannungsverhältnis aus technisch notwendigen Funktionen und

den Möglichkeiten zur (umfassenden) Überwachung der Kolleginnen und Kollegen. Eine entsprechende Dienstvereinbarung sollte deshalb auch den Umgang mit den Protokolldateien regeln. Ziel ist es, dass Vorgesetze nicht den Zugriff auf diese bekommen, sondern nur der Teil des EDV-Personals, der mit der administrativen Pflege des jeweiligen Systems beauftragt ist. Neben der organisatorischen Regelung, wer wann für welche Zwecke Zugriff auf die Daten bekommt, sollte nach Möglichkeit auch eine technische Vorkehrung geschaffen werden, die die Auswertung zum Zwecke der Leistungs- und Verhaltenskontrolle unterbindet. Eine häufig gewünschte unumkehrbare Anonymisierung der Daten ist dabei in der Regel schon deshalb nicht möglich, weil eine personell eindeutige Zuordnung beispielsweise bei der Nachverfolgung von strafrechtlichen Verstößen erforderlich ist. Hier bietet es sich eher an, dass die Protokolldateien selbst verschlüsselt gespeichert werden und idealerweise nur durch ein zweigeteiltes Passwort, das zu einen Hälfte der EDV und zur anderen dem Personalrat bekannt ist, einsehbar sind. Dadurch kann eine Auswertung nur unter Einbeziehung des Personalrats und für vorher in der Dienstvereinbarung festgesetzte Zwecken erfolgen. Sollte sich dieser Ansatz nicht umsetzen lassen, ist in jedem Fall in der Dienstvereinbarung festzuhalten, dass der Arbeitgeber keine Einblicke in die Protokolldateien ohne Genehmigung des Personalrats bekommt und aus der Einsicht gewonnene Erkenntnisse nicht zur Leistungs- und Verhaltenskontrolle genutzt werden dürfen. Da es sich hierbei um einen eher schwachen Schutz vor Leistungs- und Verhaltenskontrolle handelt, sollte nach Möglichkeit vereinbart werden, dass Einblicke in die Protokolldaten selbst protokolliert werden. Neben Datum und Zweck werden dabei die anwesenden Personen benannt. In der Dienstvereinbarung wird dann festgelegt, dass der Personalrat stichprobenartig Einblick in diese Protokollierung bekommen und damit Verstöße gegen die Dienstvereinbarungen aufdecken kann.

Generell sollte in jeder Dienstvereinbarung festgehalten werden, wer für den Personalrat Ansprechpartner rund um das Thema digitale Technologien ist und in welchem Zeitfenster ihm benötigte Informationen zur Ausübung seines Mandats überlassen werden. Fristen von mehr als 72 Stunden sollten nicht akzeptiert werden, da sie die Kontrollmöglichkeiten des Personalrats zu stark einschränken.

Software-Updates und -erweiterungen

Softwares und computergestützte Systeme unterliegen wie alle technischen Hilfsmittel der Wartungen und werden in der Regel mit Updates versorgt, die primär Fehler beseitigen sollen um die Stabilität und Sicherheit des Systems zu verbessern. Allerdings werden vermehrt auch neue Funktionen für die jeweilige Software durch ein Update installiert, ohne dass das von Seiten des Softwarenutzers verlangt worden ist. Diese neuen „Features“ sind zum Teil nicht deaktivierbar bzw. das Update ist nicht ohne sie zu haben. Was zunächst nach einem (kostenlosen) Mehrwert klingt, stellt die Mitbestimmung auch hier vor Herausforderungen. Denn analog zu den Protokolldateien kann aus technischer und systemsicherheitsorientierter Sicht nicht auf solche Updates verzichtet werden. Gleichzeitig können die Updates Funktionen mitbringen, die eine Leistung- und Verhaltenskontrolle

ermöglichen, wenn beispielsweise das neue „Feature“ darin besteht, dass in Echtzeit der Onlinestatus der Beschäftigten an andere Nutzer gesendet wird. Da solche und ähnliche Funktionen einerseits unbedingt geregelt werden müssen, um die Interessen der Beschäftigten zu wahren, andererseits deswegen nicht jedes Mal eine neue Dienstvereinbarung abgeschlossen werden sollte, bietet sich eine Anlage an die bereits bestehende Dienstvereinbarung an. Während die eigentliche Dienstvereinbarung den grundlegenden Einsatz der Software/des Systems mit den bei Abschluss vorhandenen Funktionen regelt, wird die Anlage genutzt, um Änderungen an der Funktionalität zu beschreiben und den Einsatz neuer Features mit beidseitigem Einverständnis festzulegen. Zusätzlich sollte der Personalrat darauf dringen, dass ihm – zum Beispiel vierteljährlich – eine kurze Übersicht über alle neu installierten Updates und deren Zweck bzw. Auswirkung auf das System vorgelegt wird. Diese Übersicht erleichtert es dem Gremium zu entscheiden, ob eine Anpassung der Anlage notwendig ist.

Neben den regelmäßigen Updates bieten viele Softwareanbieter speziell zu erwerbende Erweiterungen an, die den Funktionsumfang der Grundsoftware erweitern. Auch hier ist es möglich durch eine Anlage den Aufwand bei der Regelung des Einsatzes gering zu halten und gleichzeitig nicht auf die Mitbestimmung zu verzichten. Analog zu den Updates kann in der Anlage festgehalten werden, welche Erweiterungen erworben und ihr Einsatz geregelt werden. Vom Verfahren her sollte es so sein, dass alle Regelungen aus dem Haupttext der Dienstvereinbarung auch für die in den Anlagen aufgeführten Updates und Erweiterungen gelten und entsprechende Ausnahmen davon dort noch einmal explizit aufgeführt werden müssen.

Pseudonymisierung

Viele Softwarepakete bieten inzwischen Tools zur Auswertung der Nutzung der Software an. Dies geht über eine reine Übersicht, wer wann sich angemeldet hat, weit hinaus. Es wird mit skalierbaren Statistikfunktionen, Einsichten in und Prognosen für die Arbeitsleistung, Abteilungs- und Mitarbeitervergleichen, Zielerfüllungsauswertungen bis hin zu (halb)automatisierten Bewertungen und Vorschlägen für Personalmaßnahmen geworben. Um Bedenken hinsichtlich des Datenschutzes sowie der Sorge vor übermäßiger Leistungs- und Verhaltenskontrolle zu zerstreuen, wird vor allem auf dem europäischen Markt gerne mit der Möglichkeit zur Pseudonymisierung geworben, wodurch der einzelne Mitarbeiter nicht mehr identifizierbar sein soll. Bei diesem Vorgang wird der Name des jeweiligen Mitarbeiters durch eine (zufällige) Zeichenfolge ersetzt, sodass es den Anschein hat, dass damit nicht mehr Rückschlüsse auf den einzelnen Beschäftigten und seine Leistung vorgenommen werden können. Allerdings reicht dies nicht aus, um die Identität hinter der Zeichenfolge zu verbergen, da die Sammlung und Zusammenführung von verschiedenen Datenquellen innerhalb des Software häufig ein sehr eindeutiges Profil ergeben, durch das der einzelne Mitarbeiter auch ohne Nennung seines Namens identifizierbar ist. In Dienstvereinbarungen sollte daher versucht werden die Nutzung dieser Auswertungstools generell zu untersagen oder sie gleich zu deaktivieren. Lässt sich dies nicht umsetzen, sollte

die Ebene, auf der eine Auswertung stattfindet, möglichst abstrakt sein (beispielsweise bloß auf Abteilungsebene sofern die Abteilungen hinreichend groß sind). Hier ist auch gegebenenfalls der Datenschutz ein Argument, da insbesondere Auswertungstools häufig in einem Umfang Daten sammeln, der nicht DSGVO konform ist. In jedem Fall darf die Pseudonymisierung der einzelnen Mitarbeiter nicht als ausreichend angesehen werden. Auch muss die Behauptung, dass die Daten anonymisiert werden, in Zweifel gezogen werden, da eine echte Anonymisierung in Zeiten von Big Data nur schwer realisierbar ist. In der Regel handelt es sich auch dabei um eine bloße Pseudonymisierung.

Schnittstellen und Datenweitergabe

Neben der Regelung von Softwarefunktionen, mit denen explizit die Leistung und das Verhalten des Beschäftigten ausgewertet werden soll, muss auch die Möglichkeit der Dateiweitergabe sowie der Zugriff durch Drittprogramme auf erzeugte Daten geregelt werden. Durch Programmierschnittstellen können diese Drittprogramme, die im eigentlichen Softwarepaket/System nicht enthalten sind aber nachträglich erworben werden, Zugriff auf Funktionen und bereits generierte Daten erlangen. Genauso ist es möglich, dass nach dem (manuellen) Exportieren von Daten diese von Drittprogrammen einlesen werden und eine Leistungs- und Verhaltenskontrolle durchgeführt wird. Was zunächst nach einer eher aufwändigen und abstrakten Möglichkeit klingt, ist längst Realität. Viele Softwarehersteller werben damit, dass beispielsweise ihre Office-Suite zunehmend eine Plattform für Drittprogramme (bekannt als Apps) wird, die sich nahtlos in die Office-Suite einfügen, bereits erzeugte Daten verarbeiten und selber neue generieren, die von weiteren Apps weiterverarbeitet werden können. Hier gilt es von Beginn an in der Dienstvereinbarung zu untersagen, dass die erzeugten Daten durch Drittprogramme zur Leistungs- und Verhaltenskontrolle genutzt werden dürfen. Wichtig ist in diesem Zusammenhang auch, dass in der Dienstvereinbarung der Arbeitgeber dazu verpflichtet wird dafür Sorge zu tragen, dass externe Dienstleister, die beispielweise für die technische Pflege und Administration eines Softwaresystems zuständig sind, sich ebenfalls an die Bestimmungen der Dienstvereinbarung zu halten haben. Zudem muss es ihnen untersagt werden, die ihnen zukommenden Daten über die Mitarbeiter an Dritte weiterzugeben und der Personalrat sollte den Nachweis verlangen, dass sie DSGVO konform mit den Daten umgehen. In diesem Zusammenhang ist es auch notwendig, dass dem Personalrat in der Dienstvereinbarung ein Ansprechpartner bei dem jeweiligen Dienstleister genannt wird.

Christian Nienstedt
Berater Mitbestimmung und Technologieberatung

Moritz Hanke
Berater Mitbestimmung und Technologieberatung

November 2020