BRANDI
RECHTSANWÄLTE

MITARBEITERDATENSCHUTZ – ALLGEMEINE GRUNDLAGEN

Informationen zum Datenschutz I Juli 2022

English version

Einleitung

Arbeitgeber kommen regelmäßig in Kontakt mit personenbezogenen Daten von Bewerbern und Arbeitnehmern. Zur Durchführung des Arbeitsverhältnisses muss der Arbeitgeber beispielsweise die Lohn- und Gehaltsabrechnung durchführen, den Einsatz der Arbeitnehmer im Unternehmen planen und dem Arbeitnehmer einen Arbeitsplatz sowie Kommunikationsmittel zur Verfügung stellen. Im Hinblick auf den Umgang mit personenbezogenen Daten von Mitarbeitern bestehen besondere datenschutzrechtliche Anforderungen. Einerseits ist die Verarbeitung von personenbezogenen Daten der Arbeitnehmer für den Arbeitgeber unerlässlich; andererseits haben die Arbeitnehmer ein Interesse daran und auch einen Anspruch darauf, dass ihre personenbezogenen Daten nur unter Beachtung der eigenen schutzwürdigen Interessen erhoben, verarbeitet und genutzt werden. Da das Thema insoweit im Arbeitsalltag jeden Unternehmens einen hohen Stellenwert einnimmt, wird der Umgang mit Mitarbeiterdaten im Rahmen dieses Newsletters näher beleuchtet.

Entgegen verschiedener Überlegungen in der Vergangenheit gibt es derzeit kein umfassendes Beschäftigtendatenschutzrecht. Zuletzt hat auch die Datenschutzkonferenz (DSK), der Zusammenschluss der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, in ihrer Entschließung vom 29.04.2022 erneut die Schaffung eines solchen Beschäftigtendatenschutzgesetzes gefordert. Die Datenschutz-Grundverordnung (DSGVO) enthält keine konkreten, bereichsspezifischen Regelungen für diese besondere Verarbeitungssituation, sodass insoweit auf die allgemeinen datenschutzrechtlichen Regelungen zurückzugreifen ist. Allerdings findet sich in Art. 88 Abs. 1 DSGVO eine sogenannte Öffnungsklausel, die es den einzelnen Mitgliedstaaten der EU ermöglicht, spezfische Regelungen für den Bereich des Mitarbeiterdatenschutzes zu erlassen. Entsprechende nationale Vorschriften müssen dabei den inhaltlichen Anforderungen des Art. 88 Abs. 2 DSGVO entsprechen. Der deutsche Gesetzgeber hat von dieser Öffnungsklausel Gebrauch gemacht und eine entsprechende Regelung in das Bundesdatenschutzgesetz (BDSG) aufgenommen. Darüber hinaus sind selbstverständlich auch die sonstigen allgemeinen datenschutzrechtlichen Vorschriften bei der Verarbeitung von Mitarbeiterdaten zu berücksichtigen.

Verarbeitung von Mitarbeiterdaten

Nach § 26 Abs. 1 S. 1 BDSG dürfen personenbezogene Daten von Beschäftigten insbesondere für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

Unter den Begriff der Beschäftigten fallen dabei gemäß § 26 Abs. 8 BDSG neben Arbeitnehmerinnen und Arbeitnehmern unter anderem auch Leiharbeitnehmer, Auszubildende sowie Bewerber und Personen, deren Beschäftigungsverhältnis beendet ist.

Entgegen der DSGVO, die eine automatisierte Verarbeitung oder alternativ die zumindest beabsichtigte Speicherung der personenbezogenen Daten in einem Dateisystem voraussetzt, findet die Regelungen zur Verarbeitung von Daten im Beschäftigungsverhältnis nach § 26 Abs. 7 auch dann Anwendung, wenn die maßgeblichen Daten nicht in einem Dateisystem gespeichert werden sollen. Dementsprechend sind auch bei der Verarbeitung von Mitarbeiterdaten in Papierform die Vorgaben des § 26 BDSG zu beachten.

Personalakte

Die personenbezogenen Daten der Mitarbeiter werden in der Regel in der Personalakte abgelegt oder gespeichert. Die zugehörigen Datenverarbeitungsprozesse lassen sich dabei vor allem auf § 26 BDSG (Zwecke des Beschäftigungsverhältnisses) sowie die Vertragserfüllung nach Art. 6 Abs. 1 S. 1 lit. b) DSGVO stützen. Unter Berücksichtigung des Grundsatzes der Datenminimierung dürfen seitens des Unternehmens jedoch nicht beliebig viele Daten erhoben und verarbeitet werden. Die vorgehaltenen Personaldaten sind vielmehr auf die erforderlichen Kerndaten zu beschränken. Gleichwohl enthält die Personalakte eine Vielzahl vertraulicher mitunter auch sensibler Informationen über den Mitarbeiter, die sich zu einem Profil zusammenfügen lassen, weshalb die Personalakte und die in ihr enthaltenen Informationen auch besonders zu schützen sind. Das erforderliche Schutzniveau sowie die konkret zu ergreifenden Maßnahmen ergeben sich dabei jeweils aus der Sensibilität und der Art der unterschiedlichen Daten. Gleiches gilt auch im Hinblick auf die Frage, wie lange die einzelnen Daten des Mitarbeiters gespeichert werden dürfen. Pauschale Gestaltungen können sich insoweit als datenschutzrechtlich problematisch darstellen; vielmehr sollte jeweils eine Einzelfallbetrachtung erfolgen. Aus diesem Grund ist in jedem Fall darauf zu achten, dass eine sorgfältige Aufbewahrung der Personalakte erfolgt, der Kreis der Zugriffsberechtigten auf das notwendige Maß beschränkt wird und die Inhalte vor unberechtigter Einsichtnahme geschützt sind. In der Regel sollte die Möglichkeit der Einsichtnahme auf den Arbeitgeber und die Personalverwaltung beschränkt sein.

Verarbeitung besonderer Kategorien personenbezogener Daten
Im Rahmen des Beschäftigungsverhältnisses werden zudem regelmäßig auch Gesundheitsdaten verarbeitet. Diese fallen unter die Kategorie der besonderen Daten i.S.v. Art. 9 DSGVO und sind aufgrund ihrer Sensibilität besonders zu schützen. Durch § 26 Abs. 3 BDSG werden die bereits strengen Anforderungen der DSGVO für den Fall der Verarbeitung im Rahmen des Arbeitsverhältnisses noch zusätzlich verschärft. Eine Verarbeitung besonders sensibler Daten ist insoweit nur zulässig, soweit diese zur Ausübung bzw. Erfüllung von Rechten und Pflichten aus dem Arbeits- oder Sozialrecht erforderlich ist und nicht anzunehmen ist, dass entgegenstehende Interessen überwiegen. Gesundheitsdaten wie Krankheitsinformationen dürfen zudem nicht in der Personalakte abgelegt oder gespeichert werden, sondern sind grundsätzlich separat aufzubewahren. Der Kreis der Zugriffsberechtigten sollte ebenfalls auf den Vorgesetzten sowie den Personalverantwortlichen begrenzt werden.

Weitergabe von Mitarbeiterdaten
Sollen Mitarbeiterdaten an einen Dienstleister oder an eine andere Konzerngesellschaft übermittelt werden, sind die allgemeinen Vorschriften der DSGVO über die Auftragsverarbeitung (Art. 28 DSGVO) bzw. die Gemeinsame Verantwortlichkeit (Art. 26 DSGVO) einzuhalten. Hat ein Unternehmen beispielsweise seine Buchhaltung an ein externes Lohnbüro ausgelagert und werden etwa zur Durchführung der Gehaltsabrechnung Mitarbeiterdaten an das Lohnbüro übermittelt und von diesem verarbeitet, ist zur Absicherung dieser Datenverarbeitungsprozesse der Abschluss einer Vereinbarung zur Auftragsverarbeitung mit dem einbezogenen Dienstleister erforderlich. Mitarbeiterdaten dürfen auch im Übrigen grundsätzlich nicht ohne eine entsprechende Rechtsgrundlage an andere Unternehmen weitergegeben werden. Handelt es sich um ein „konzerndimensionales Arbeitsverhältnis" kommen als Rechtsgrundlage für die Datenübermittlung zusätzlich die Vertragserfüllung nach Art. 6 Abs. 1 S. 1 lit. b) DSGVO sowie § 26 BDSG in Betracht. Ein solches liegt unter anderem vor, wenn die arbeitsvertraglich vereinbarte Tätigkeit eindeutig Bezug zum Konzern aufweist oder der jeweilige Mitarbeiter bei verschiedenen Unternehmen des Konzerns eingesetzt wird.

Informationspflichten des Arbeitgebers und datenschutzrechtliche Verpflichtung der Mitarbeiter

Werden personenbezogene Daten erhoben, besteht für Verantwortliche nach Art. 13 Abs. 1 DSGVO die Pflicht, den betroffenen Personen verschiedene datenschutzrechtliche Pflichtinformationen mitzuteilen bzw. zur Verfügung zu stellen. Die Informationspflichten nach Art. 13 DSGVO gelten dabei nicht nur für Datenverarbeitungsprozesse im Rahmen des Bewerbungsverfahrens, sondern auch für die Verarbeitung personenbezogener Daten während des Beschäftigungsverhältnisses. Zu informieren sind die Mitarbeiter unter anderem über die Zwecke, für die die Daten verarbeitet werden sollen, die Rechtsgrundlage für die Verarbeitung sowie die Speicherdauer. Darüber hinaus sind den Betroffenen Informationen über die verschiedenen Betroffenenrechte wie etwa das Recht auf Auskunft und das Recht auf Löschung zur Verfügung zu stellen.

In zeitlicher Hinsicht hat die datenschutzrechtliche Information der Mitarbeiter „zum Zeitpunkt der Erhebung" zu erfolgen. Soweit Mitarbeiter nicht bereits im Rahmen des Bewerbungsverfahrens umfassend datenschutzrechtlich informiert wurden, sollten die Mitarbeiter mit Unterzeichnung des Arbeitsvertrages oder Aufnahme ihrer Tätigkeit noch einmal separat über Art und Umfang der Datenverarbeitung anlässlich des Beschäftigungsverhältnisses, etwaige Besonderheiten sowie die ihnen zustehenden Rechte informiert werden.

Darüber hinaus ist es empfehlenswert, alle Mitarbeiter des Unternehmens zu Beginn ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Unternehmen unterliegen unter der DSGVO der sog. „Rechenschaftspflicht". Dies bedeutet, dass sie nachweisen müssen, dass sie die Vorgaben der DSGVO einhalten. Hierzu gehört nach Art. 24 DSGVO auch das Ergreifen der erforderlichen organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten. Ein Nachweis für die korrekte Umsetzung dieser Maßnahmen wird aber nur dann möglich sein, wenn alle Mitarbeiter, die in Kontakt mit personenbezogenen Daten kommen, schriftlich zur Wahrung der Vertraulichkeit und der anwendbaren datenschutzrechtlichen Vorschriften sowie der ihnen obliegenden Pflichten verpflichtet werden. Die Verpflichtung besteht sodann auch über das Ende des Arbeitsverhältnisses hinaus.

Einwilligung im Beschäftigtenverhältnis

Eine mögliche Rechtsgrundlage zur Rechtfertigung von Datenverarbeitungsprozessen ist die Einwilligung des Betroffenen nach Art. 6 Abs. 1 S. 1 lit. a) DSGVO in die konkrete Datenverarbeitung. Damit eine Einwilligung wirksam ist, muss diese durch den Betroffenen in informierter Weise, für den bestimmten Fall, freiwillig und unmissverständlich durch eine Erklärung oder eindeutig bestätigende Handlung erteilt werden. Soll eine Datenverarbeitung des Arbeitsgebers auf eine Einwilligung des Arbeitnehmers i.S.v. Art. 6 Abs. 1 S. 1 lit. a) DSGVO gestützt werden, sind einige Besonderheiten zu beachten. Problematisch ist insoweit insbesondere der Aspekt der Freiwilligkeit der Einwilligung.

In der Vergangenheit wurde hierzu mitunter die Auffassung vertreten, dass eine datenschutzrechtliche Einwilligung im Rahmen des Arbeitsverhältnisses problematisch sei, gar nicht erteilt werden könne, da aufgrund der bestehenden Abhängigkeit des Arbeitnehmers vom Arbeitgeber nicht von einer freien Entscheidung ausgegangen werden könne (Gola/Schomerus, BDSG, § 4a Rn. 6 m.w.N.). Inzwischen hat die Rechtsprechung jedoch klargestellt, dass eine wirksame datenschutzrechtliche Einwilligung grundsätzlich auch im Rahmen eines Arbeitsverhältnisses erteilt werden kann, da der Arbeitnehmer auch in diesem Kontext frei von seinem Recht auf informationelle Selbstbestimmung Gebrauch machen darf (BAG, Urt. v. 11.12.2014, Az. 8 AZR 1010/13). Das Recht, über seine Daten durch Einwilligung zu verfügen, werde ihm durch das Eingehen eines Arbeitsverhältnisses gerade nicht genommen.

Gleichwohl kommt eine Einwilligung im Beschäftigtenverhältnis in der Regel nur in Ausnahmefällen und bei Vorliegen der zusätzlichen Voraussetzungen des § 26 Abs. 2 BDSG in Betracht. Entsprechend der Vorschrift bedarf es bei der Beurteilung der Freiwilligkeit der Einwilligung insbesondere der Berücksichtigung der im Beschäftigtenverhältnis bestehenden Abhängigkeit der beschäftigten Person sowie der Umstände, unter denen die Einwilligung erteilt worden ist. Der Aspekt der Freiwilligkeit ist nach § 26 Abs. 2 S. 2 BDSG insbesondere dann zu bejahen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und Arbeitnehmer gleichgelagerte Interessen verfolgen. Unabhängig von dieser beispielhaften Aufzählung sollte gleichwohl in jedem Fall geprüft werden, ob tatsächlich von einer freiwilligen Entscheidung des Arbeitnehmers ausgegangen werden kann, da es ansonsten an einer wirksamen Einwilligung und damit in der Regel sodann auch an einer Rechtsgrundlage für die Datenverarbeitung fehlt.

Um den Arbeitnehmer vor einem übereilten Handeln zu schützen und ihm die Relevanz seiner Entscheidung zu verdeutlichen sowie zu Nachweiszwecken, bedarf jede Einwilligung im Rahmen eines

Beschäftigungsverhältnisses der Schriftform, soweit nicht aufgrund anderer Umstände eine andere Form angemessen ist. Zudem muss der Arbeitnehmer die tatsächliche Möglichkeit haben, die Einwilligung jederzeit zu widerrufen, und muss über diese Möglichkeit auch informiert werden. Darüber hinaus empfiehlt es sich, im Rahmen der Einwilligung bzw. der zugehörigen Datenschutzinformation auch ausdrücklich darauf hinzuweisen, dass die Verweigerung der Einwilligung oder der spätere Widerruf nicht mit nachteiligen Folgen für den Mitarbeiter verbunden ist. Um etwaige Rechtsunsicherheiten zu vermeiden, bietet es sich – soweit möglich – an, Datenverarbeitungsprozesse im Kontext des Arbeitsverhältnisses auf eine andere Rechtsgrundlage als die Einwilligung zu stützen.

Überwachung von Mitarbeitern

Fraglich ist häufig, inwieweit vorhandene Daten genutzt werden dürfen, um die Einhaltung rechtlicher und vertraglicher Vorgaben durch die Mitarbeiter zu überwachen. Denkbar ist insoweit etwa die Auswertung einer Videoüberwachung oder der Telefon-, E-Mail- und Internetnutzung. Unter Berücksichtigung des Grundsatzes der Zweckbindung, dürfen personenbezogenen Daten nur für die Zwecke verarbeitet werden, die ursprünglich im Rahmen der Datenverarbeitung vorgesehen waren. Wurde eine Videoüberwachung etwa installiert, um Ladendiebstähle zu verhindern, dürfen die Aufzeichnungen nicht ohne Weiteres für andere Zwecke wie etwa die Einhaltung von Pausenzeiten genutzt werden. Eine Änderung des ursprünglichen Zwecks der Datenverarbeitung ist dabei nur unter den engen Voraussetzungen gem. Art. 6 Abs. 4 DSGVO möglich. Die verdeckte Überwachung von Mitarbeitern ist zudem grundsätzlich untersagt. Darüber hinaus hat für jegliche Form von Überwachungsmaßnahmen eine Interessenabwägung zwischen den Interessen von Arbeitgeber und Arbeitnehmer zu erfolgen, mittels derer festzustellen ist, ob eine Maßnahme nicht übermäßig in die Rechte der Mitarbeiter eingreift. Dabei sollte in jedem Fall auch die einschlägige Rechtsprechung berücksichtigt werden.

Prinzipiell dürfen Beschäftigtendaten nach § 26 Abs. 1 S. 2 BDSG darüber hinaus auch zur Aufdeckung von Straftaten verarbeitet werden. Dies gilt jedoch nur dann, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Rahmen des Arbeitsverhältnisses eine Straftat begangen hat. Die Datenverarbeitung muss darüber hinaus zur Aufdeckung des Falls erforderlich sein und es hat in jedem Fall eine Abwägung mit den Interessen des Mitarbeiters zu erfolgen, wobei die Datenverarbeitung insbesondere nicht unverhältnismäßig mit Blick auf den konkreten Vorfall sein darf. Zu berücksichtigen ist hierbei auch, dass die Datenverarbeitung nur durch eine autorisierte Person, etwa der Personal- oder IT-Abteilung, bestenfalls in Absprache mit dem Datenschutzbeauftragten durchzuführen ist.

Fazit

Neben der Einhaltung der allgemeinen datenschutzrechtlichen Vorschriften sind bei der Verarbeitung von Mitarbeiterdaten einige Besonderheiten zu beachten und zusätzliche Anforderungen zu erfüllen. Letztere ergeben sich im deutschen Recht insbesondere aus § 26 BDSG.

Vor allem die Personalakte enthält eine Vielzahl von Mitarbeiterdaten und ist deshalb vertraulich zu behandeln. Es dürfen nur solche Daten abgelegt oder gespeichert werden, die zur Durchführung des Arbeitsverhältnisses auch erforderlich sind. Wird gegen diesen Grundsatz verstoßen, kann dies mitunter auch Bußgelder in empfindlicher Höhe zur Folge haben. Gegen den Konzern H & M wurde etwa ein Bußgeld in Höhe von über 35 Millionen Euro verhängt, weil Führungskräfte unrechtmäßigerweise Informationen aus dem Privatleben ihrer Mitarbeiter sammelten und diese zur Personalakte speicherten.

Soweit eine Datenverarbeitung im Rahmen des Arbeitsverhältnisses auf die Rechtsgrundlage der Einwilligung gestützt werden soll, ist hinsichtlich der Rechtmäßigkeit grundsätzliche eine genaue Prüfung des Einzelfalls unter Berücksichtigung der jeweiligen Umstände erforderlich. Dabei ist insbesondere darauf zu achten, ob die Einwilligung des Mitarbeiters auch tatsächlich freiwillig erteilt wurde.

Sollen personenbezogene Daten von Mitarbeitern auch zu Überwachungszwecken genutzt werden, ist dies nur unter sehr engen Voraussetzungen möglich. Die Mitarbeiter sollten über den Umstand der Überwachung in jedem Fall transparent und umfassend informiert und die jeweilige Rechtsprechung berücksichtigt werden. Soweit ein Betriebsrat besteht, sollte dieser in die Überlegungen und Vorgänge einbezogen werden, um Streitigkeiten zu vermeiden.

Christina Prowald

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Wissenschaftliche Mitarbeiterin

T +49 521 96535 - 890
F +49 521 96535 - 113
M christina.prowald@brandi.net