STIFTUNG DATENSCHUTZ

BESCHÄFTIGTEN DATENSCHUTZ

EINE HANDREICHUNG

THEMEN

VORWORT

LIEBE LESERIN, LIEBER LESER,

seit Mai 2018 ist die EU-Datenschutz-Grundverordnung verbindlich anzuwenden. Seither nehmen viele Organisationen, Einrichtungen, Privatpersonen und Unternehmen den Schutz personenbezogener Daten viel wichtiger als vorher.

Eine Vielzahl von personenbezogenen Daten über Beschäftigte und BewerberInnen fällt in den Personalabteilungen der Unternehmen an. Diese Daten sind oft besonders sensibel, betreffen sie doch meist auch die Privatsphäre der Menschen: Familienverhältnisse, Erkrankungen, und überhaupt Informationen, die manche nicht gern mit Vorgesetzten und ArbeitskollegInnen teilen möchten. Dazu kommt, dass Beschäftigungsverhältnisse für die Einzelnen besonders wichtig sind, weil sie die wirtschaftliche Existenz sichern. Daher sind Beschäftigungsverhältnisse auch im Rahmen des Arbeitsrechts besonders geschützt.

Umso verwunderlicher ist es, dass es noch kein spezielles Recht für den Beschäftigtendatenschutz gibt, obwohl dies schon seit vielen Jahren von DatenschutzexpterInnen, Personalprofis, Betriebsräten und anderen gefordert wird. Dies hat sich auch mit der EU-Datenschutz-Grundverordnung nicht geändert.

Die vorliegende Handreichung trägt die wichtigsten Grundsätze und Regeln zusammen, die für den Datenschutz in Beschäftigungsverhältnissen gelten.

Sie wendet sich vor allem an Personalverantwortliche in kleinen und mittelständischen Unternehmen, aber auch an Betriebsräte und ganz allgemein an Beschäftigte. Ihr Ziel ist es, Leitlinien für den praktischen Unternehmensalltag zu vermitteln. Dabei ersetzt diese Handreichung natürlich nicht den Austausch mit dem/der Datenschutzbeauftragen, oder – in komplizierteren Fällen – mit einer spezialisierten Rechtsanwaltskanzlei.

Eine ausführlichere Version mit weiterführenden Links finden unter diesem Link: sds-links.de/handreichung-BSDS. Veröffentlichungen der Aufsichtsbehörden sind über unser Infoplattform stiftungdatenschutz.org/dsgvo-info abrufbar.

Wir haben uns um eine klare und verständliche Sprache bemüht. Wenn Sie Verbesserungsvorschläge haben, schreiben Sie uns: mail@stiftungdatenschutz.org

Und schließlich möchten wir Sie noch auf unsere allgemeine Handreichung zum „Datenschutz im Betrieb“ hinweisen, die Sie auf unserer Website finden.

Freundliche Grüße von

Frederick Richter
Vorstand
der Stiftung Datenschutz

GRUNDSÄTZLICHES

WELCHE GESETZE REGELN DEN DATENSCHUTZ FÜR BESCHÄFTIGTE?

Die EU-Datenschutz-Grundverordnung (DSGVO) ist seit Mai 2018 in allen EU-Ländern verbindlich anzuwenden und regelt wesentliche Punkte der Verarbeitung personenbezogener Daten. Dazu gehören

- die Pflichten der Unternehmen, Einrichtungen und Organisationen, welche die Daten verarbeiten („verantwortliche Stellen"),
- die Rechte der Personen, deren Daten verarbeitet werden (die „Betroffenen"),
- die Benennung von Datenschutzbeauftragten und -aufsichtsbehörden,
- die Übermittlung von Daten an Dritte und in Drittländer,
- das Vorgehen und die Sanktionen bei Datenschutzverstößen und viele andere Aspekte.

Die DSGVO ermöglicht es den EU-Mitgliedsländern, bestimmte allgemeine Vorschriften an ihre speziellen Bedürfnisse anzupassen. Eine solche sogenannte Öffnungsklausel gibt es auch für den Beschäftigtendatenschutz. Deutschland hat das Bundesdatenschutzgesetz (BDSG) an die DSGVO angepasst und dabei die „alte" Regelung in den § 26 BDSG übernommen[1]. Ein eigenes Gesetz, das den Schutz der personenbezogenen Daten in Beschäftigungsverhältnissen umfassend regelt, gibt es bislang nicht.

Neben der Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz enthalten zahlreiche andere gesetzliche Regelungen Vorschriften für den Datenschutz. So ist die Verschwiegenheitspflicht von medizinischem Personal im Strafgesetzbuch, der Umgang mit Briefen im Postgesetz und der Umgang mit Gesundheitsdaten bei Versicherungen im Sozialgesetzbuch V geregelt.

FÜR WEN GELTEN DIE REGELUNGEN DES § 26 BDSG?

Das Gesetz gilt für „Beschäftigte". Das bedeutet im Sinne des Datenschutzes:

- Arbeitnehmerinnen und Arbeitnehmer
- Leiharbeitnehmerinnen und Leiharbeitnehmer (im Verhältnis zum entleihenden Unternehmen)
- Auszubildende
- TeilnehmerInnen an Leistungen zur Teilhabe am Arbeitsleben sowie RehabilitandInnen
- Menschen, die in anerkannten Werkstätten für behinderte Menschen beschäftigt sind,
- Freiwillige nach dem Jugendfreiwilligendienstgesetz oder dem Bundesfreiwilligendienstgesetz
- arbeitnehmerähnliche Personen (z.B. in Heimarbeit Beschäftigte)
- BewerberInnen für ein Beschäftigungsverhältnis
- Personen, deren Beschäftigungsverhältnis beendet ist
- Beamtinnen und Beamte des Bundes, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende (sofern nicht bundes- und landesspezifische Regelungen gelten).

In Kürze: Das Bundesdatenschutzgesetz und die DSGVO gelten für alle Beschäftigungsverhältnisse, einschließlich Leiharbeits- und Ausbildungsverhältnisse; für BewerberInnen und ehemals Beschäftigte. Für Bedienstete und Beschäftigte bei Behörden und öffentlichen Stellen des Bundes, der Länder und der Kommunen, gelten besondere (u.a. beamtenrechtliche) bundes- und landesspezifische Regelungen.

WAS SIND ÜBERHAUPT PERSONENBEZOGENE DATEN?

Personenbezogene Daten sind alle Informationen über eine natürliche Person, die sich der Person **unmittelbar** oder **mittelbar** zuordnen lassen.

- Unmittelbar zuzuordnen ist der Person ihr Name.
- Unmittelbar der Person zuzuordnen kann auch ihre Funktion sein, wenn es zum Beispiel nur eine IT-Leiterin im Unternehmen gibt.
- Mittelbar zuzuordnen ist der Person ihre Personalnummer: Zwar weist die Personalnummer an sich noch nicht auf die konkrete Person hin, der Personenbezug kann jedoch hergestellt werden, wenn bekannt ist, welcher Name zu welcher Personalnummer gehört.
- Mittelbar kann unter bestimmten Umständen auch eine IP-Adresse einer Person zugeordnet werden.

1 https://sds-links.de/v78

Diese Beispiele zeigen, dass vor allem beim mittelbaren Personenbezug der Zusammenhang betrachtet werden muss, wenn es darum geht zu entscheiden, ob es sich um personenbezogene Daten handelt.

Personenbezogene Daten können auch bloße Annahmen und Vermutungen sein. Wenn eine Auskunftei die Kreditwürdigkeit einer Person mit Hilfe eines Score-Wertes berechnet, ist dieser Wert eine Annahme über die Zahlungsfähigkeit oder -bereitschaft des Kunden bzw. über die Ausfallwahrscheinlichkeit des Kredits in der Zukunft. Auch solche Einschätzungen gehören zu den personenbezogenen Daten.

Darüber hinaus gibt es sogenannte „besondere Kategorien personenbezogener Daten“ (Artikel 9 Absatz 1 DSGVO). Das sind Daten, die besonders schutzwürdig sind, weil aus ihnen die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder eine Gewerkschaftszugehörigkeit hervorgehen, sowie genetische und biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben oder der geschlechtlichen Orientierung einer natürlichen Person. Für deren Verarbeitung gibt es besondere Vorschriften.

GILT DIE DSGVO NICHT NUR FÜR DIE AUTOMATISIERTE DATENVERARBEITUNG?

Grundsätzlich gilt die Datenschutz-Grundverordnung für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten. Werden personenbezogene Daten nichtautomatisiert verarbeitet, gilt die DSGVO nur dann, wenn diese in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Ein Dateisystem ist eine strukturierte Sammlung personenbezogener Daten, zum Beispiel alphabetisch geordnete Karteikarten mit Adressen der Beschäftigten.

Personenbezogene Daten im Beschäftigungsverhältnis unterliegen aber immer der DSGVO, unabhängig davon, wie sie verarbeitet (automatisiert/nicht automatisiert) und gespeichert werden (strukturiert/unstrukturiert).

2 https://sds-links.de/jy7 (Artikel 5 Abs.1 Buchstabe b) DSGVO)
3 https://sds-links.de/jy7 (Artikel 5 Abs.2 DSGVO)

Die Verarbeitung von personenbezogenen Daten im Beschäftigungsverhältnis unterliegt immer der DSGVO. Das betrifft auch die besonders geschützten Daten. Unter „Verarbeitung“ versteht man hier jede vorstellbare Handlung: speichern, weitergeben, notieren, sprechen…

DAS PRINZIP DER ZWECKBINDUNG

Das Prinzip der Zweckbindung[2] verlangt, dass Beschäftigtendaten nur für festgelegte, eindeutige und legitime Zwecke erhoben und verarbeitet werden dürfen. Dies muss der Arbeitgeber nachweisen können[3]. In Betriebsvereinbarungen müssen dazu Regelungen getroffen werden, die möglichst konkret, klar und abschließend die Zwecke der Datenverarbeitung festlegen. Allgemeine Beschreibungen sind zu vermeiden.

Beispiel:

Zu allgemein: „Die Datenverarbeitung dient der Urlaubsplanung“
Ausreichend konkret: „Die Unternehmenssoftware „HappyHolidays“ dient der Erfassung und Prüfung der Urlaubsanträge der Beschäftigten auf Basis ihres Urlaubsanspruchs“).

DIE ROLLE DES BETRIEBSRATS

Dem Betriebsrat werden im Zuge seiner Tätigkeit eine Reihe von personenbezogenen Daten, auch solche aus den besonders geschützten Kategorien, bekannt. Ob der Betriebsrat damit eine verantwortliche Stelle im Sinne von Artikel 4 Nr. 7 DSGVO ist oder ob er – wie unter bisherigem Recht – Teil der verantwortlichen Stelle, also des Unternehmens, bleibt, ist derzeit noch umstritten. Damit ist auch offen, ob er der Kontrolle durch den betrieblichen Datenschutzbeauftragten und durch die Aufsichtsbehörden unterliegt.

Unbestritten ist jedoch, dass der Betriebsrat bei seiner Tätigkeit die üblichen gesetzlichen Regelungen der DSGVO befolgen muss.

WICHTIG: Das Schutzniveau von Betriebsvereinbarungen darf nicht geringer sein als das Schutzniveau der DSGVO

DIE DATENSCHUTZBEAUFTRAGTEN

Eine Datenschutzbeauftragte muss benannt werden, wenn in einer Organisation – egal, ob Unternehmen, Behörde oder Sportverein – mindestens 20 Beschäftigte überwiegend mit der Verarbeitung von personenbezogenen Daten befasst sind. Datenschutzbeauftragte werden aufgrund ihrer fachlichen Qualifikation benannt und können angestellt oder selbständig tätig sein.

Verantwortlich für die Einhaltung der Datenschutzbestimmungen ist die Geschäftsleitung. Die Datenschutzbeauftragte berät sie und überwacht die Verarbeitungstätigkeit im Unternehmen. Sie sensibilisiert und schult die Beschäftigten und ist Ansprechperson für die zuständige Datenschutzaufsichtsbehörde. Dabei ist sie zur Verschwiegenheit verpflichtet, wenn ihr Missstände gemeldet werden.

Weil die Datenschutzbeauftragte bei ihrer Tätigkeit weisungsfrei agiert, unterliegt sie einem besonderen Kündigungsschutz und kann während ihrer Tätigkeit und ein Jahr danach nur aus wichtigem Grund gekündigt werden. Das trifft allerdings nur zu, wenn das Unternehmen verpflichtet ist, einen Datenschutzbeauftragten zu benennen; wenn die Benennung freiwillig erfolgt ist, weil weniger als 20 Beschäftigte personenbezogene Daten verarbeiten, entfällt auch der Kündigungsschutz.

Wenn eine Beschäftigte zur Datenschutzbeauftragten bestimmt werden soll, darf sie sich nicht selbst beaufsichtigen; daher kommen Mitglieder der Geschäftsleitung oder von Abteilungen, in denen häufig Daten verarbeitet werden, wie IT- oder Personalabteilung, in der Regel nicht in Betracht. Konzerne oder Unternehmensgruppen können eine (einzige) Datenschutzbeauftragte bestellen, wenn diese für die Angehörigen aller Unternehmen gut erreichbar ist.

Beispiel: Freiwillige Bestellung von Datenschutzbeauftragten

Ein Unternehmen hat 20 Beschäftigte, aber davon sind lediglich zehn MitarbeiterInnen mit der Verarbeitung personenbezogener Daten beschäftigt, in dem ihnen Zugriffsrechte auf die Kundendatenbank eingeräumt wurden. In diesem Falle besteht zwar nach BDSG keine Verpflichtung zur Bestellung eines Datenschutzbeauftragten, aber das Unternehmen kann auf freiwilliger Basis eine Datenschutzbeauftragte bestellen. In diesem Falle genießt die Datenschutzbeauftragte allerdings keinen besonderen Kündigungsschutz.

Hinweis: Fällt die Anzahl nur aufgrund von zeitlich begrenzter Kurzarbeit unter 20 Beschäftigte, bleibt es während der Kurzarbeit bei der Pflicht zur Benennung eines Datenschutzbeauftragten.

WANN IST DIE DATENVERARBEITUNG ZULÄSSIG?

Die DSGVO und das BDSG sind Verbotsgesetze mit Erlaubnisvorbehalt. Das bedeutet, dass jede Verarbeitung personenbezogener Daten zunächst unzulässig ist; es sei denn, es gibt einen sogenannten „Erlaubnisgrund", der die Datenverarbeitung erlaubt. Diese Erlaubnisgründe sollen hier kurz dargestellt werden:

DIE DATENVERARBEITUNG IST ERFORDERLICH.

Personenbezogene Daten über Beschäftigte dürfen verarbeitet werden, sofern dies erforderlich ist, um das Arbeitsverhältnis zu begründen, durchzuführen und zu beenden. Weiterhin kann die Datenverarbeitung erforderlich sein, um Pflichten zu erfüllen und/oder Rechte auszuüben, die sich aus Gesetzen, Tarifverträgen und Betriebs- oder Dienstvereinbarungen ergeben. Dabei bedeutet das Merkmal der Erforderlichkeit, dass mit der Datenverarbeitung ein legitimer Zweck verfolgt wird, und dass dieser Zweck ohne diese Datenverarbeitung nicht erreicht werden kann. Auch besonders sensible Daten dürfen verarbeitet werden, wenn dies zur Erfüllung von arbeitsrechtlichen Pflichten oder für den Sozialschutz erforderlich ist.

Beispiel: Durchführung des Arbeitsverhältnisses

In der Personalakte wird die Religionszugehörigkeit (= personenbezogenes Datum) gespeichert (= verarbeitet), weil der Arbeitgeber per Gesetz verpflichtet ist, im Rahmen der Gehaltszahlungen die Kirchensteuer an das Finanzamt abzuführen (= legitimer Zweck). Dies wäre ohne die Verarbeitung des Datums „Religionszugehörigkeit" nicht möglich. Daher ist die Datenverarbeitung erforderlich und damit zulässig.

Beispiel: Daten, die bei der Computernutzung anfallen

Es wird gespeichert, wer sich wann an einem Computersystem anmeldet. Die Anmeldenamen sind im Zusammenhang mit dem Passwort als personenbezogene Daten zu betrachten. Die Datenverarbeitung kann aus Sicherheitsgründen oder zur Dokumentation erforderlich sein (legitimer Zweck). Das Protokollieren aller Tastatureingaben wäre jedoch nicht zulässig, weil damit kein legitimer Zweck verfolgt werden kann; damit fehlt die Erforderlichkeit.

Beispiel: Fahrerlaubnis

Das Unternehmen darf kontrollieren, ob NutzerInnen von Dienstfahrzeugen eine gültige Fahrerlaubnis haben. Es ist aber nicht erforderlich, eine Kopie in der Personalakte zu speichern – vielmehr sollten die Fahrerinnen in regelmäßigen Abständen ihre Fahrerlaubnis im Unternehmen vorzeigen.

Beispiel: Namensschilder

Im Einzelhandel kann das Tragen von Namensschildern der Beschäftigten dazu beitragen, eine kundenfreundliche Atmosphäre zu schaffen. Allerdings ist zu diesem Zweck nicht die Angabe des vollständigen Namens erforderlich, sondern der Nachname kann ausreichend sein.

Beispiel: Zugangskontrollsysteme

Biometrische Daten sind besonders geschützt. Dennoch kann die Verarbeitung erforderlich sein, zum Beispiel wenn der Zugang zu einem Sicherheitsbereich mittels Fingerabdruck- oder Venenscan geregelt werden soll. Dann muss die Erforderlichkeit besonders geprüft werden.

Für die Feststellung der Erforderlichkeit zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes muss stets eine Interessenabwägung stattfinden. Dabei wird das Interesse des Arbeitsgebers an der Datenverarbeitung dem schutzwürdigen Interesse der Beschäftigten gegenüber gestellt, die Daten nicht zu verarbeiten. Die Verarbeitung ist nur dann zulässig, wenn kein Grund zu der Annahme besteht, dass das Interesse der Beschäftigten an dem Ausschluss der Verarbeitung überwiegt.

Für die Verarbeitung besonders geschützter Daten müssen die Interessen von Arbeitgeber und Beschäftigten besonders sorgfältig gegeneinander abgewogen werden, etwa wenn biometrische Kontrollsysteme eingerichtet werden sollen.

Beispiel: Zugangskontrolle mittels Fingerprint

Ein Fingerabdruck ist ein biometrisches Datum und daher besonders geschützt. Wenn der Arbeitgeber ein Zugangskontrollsystem einrichten will, dass auf Fingerabdrücken basiert, muss er im Rahmen der Verhältnismäßigkeit prüfen, welches Interesse überwiegt: Das des Arbeitgebers, den Zugang zu bestimmten Bereichen streng zu kontrollieren, oder das der Beschäftigten, dass ihre Fingerabdrücke nicht verarbeitet werden. Für die Kontrolle des Zugangs zu Sicherheitsbereichen kann die Verarbeitung erforderlich und damit verhältnismäßig sein, für den Zugang zur Kantine eher nicht.

ES LIEGT EINE EINWILLIGUNG VOR.

Die Datenschutz-Grundverordnung regelt, dass die Einwilligung einer betroffenen Person (also derjenigen Menschen, deren personenbezogene Daten verarbeitet werden sollen) die Verarbeitung erlaubt, wenn keine anderen Gründe dagegen sprechen. (Andere Erlaubnisgründe sind zum Beispiel die Erforderlichkeit zur Vertragsdurchführung oder das Vorliegen von entsprechenden gesetzlichen Vorschriften, siehe oben.) Diese Einwilligung muss immer **informiert** und **freiwillig** erfolgen, d.h. die betroffene Person muss wissen, welche Daten in welchem Umfang von wem zu welchem Zweck verarbeitet werden, und es darf ihr kein Nachteil aus einer Ablehnung entstehen.

Diese Aspekte machen es schwierig, in Beschäftigungsverhältnissen mit einer wirksamen Einwilligung zu arbeiten, denn für die allermeisten Menschen ist das Beschäftigungsverhältnis die Grundlage ihrer wirtschaftlichen Existenz. Daher, und wegen der bestehenden Weisungsrechte, bestehen fast immer so unterschiedliche Machtverhältnisse, dass die Freiwilligkeit einer Einwilligung schwer nachzuweisen ist.

Beispiel

In der Bäckerei Hermann treten immer wieder Kassenfehlbeträge auf. Hermann möchte daher die Bäckereifachverkäuferinnen bei ihrer Arbeit per Video überwachen, und bittet diese um ihre Einwilligung. Silke Streusel ist noch in der Probezeit und fürchtet, entlassen zu werden, wenn sie nicht einwilligt.

Das bedeutet jedoch nicht, dass die Datenverarbeitung auf der Grundlage einer Einwilligung im Beschäftigungsverhältnis ausgeschlossen ist. Von einer freiwilligen Einwilligung kann ausgegangen werden, wenn für die Beschäftigten durch die Datenverarbeitung ein rechtlicher oder wirtschaftlicher Vorteil entsteht, oder wenn Arbeitgeber und Beschäftigte übereinstimmende Interessen verfolgen.

Auch die Verarbeitung besonders sensibler personenbezogener Daten ist mit einer Einwilligung möglich, wenn sich die Einwilligung ausdrücklich auf diese Daten bezieht.

Beispiel

Der Installateurbetrieb Warmwasser stattet seine Installateure mit Mobiltelefonen aus, damit sie währen der Arbeit beim Kunden erreichbar sind, und gestattet die uneingeschränkte private Nutzung. Die Beschäftigten benötigen kein privates Mobiltelefon, dadurch entsteht ihnen ein wirtschaftlicher Vorteil. Daher ist davon auszugehen, dass ihre Einwilligung in die Datenverarbeitung, die ihre private Telefonnutzung betrifft, wirksam erteilt werden kann.

WICHTIG: Die Einwilligung im Arbeitsverhältnis muss grundsätzlich schriftlich erteilt werden. Damit die Einwilligung auch „informiert“ ist, müssen Beschäftigte über Zweck und Umfang der Datenverarbeitung in Kenntnis gesetzt werden; ebenso darüber, dass die Einwilligung jederzeit widerrufen werden kann. Der Widerruf macht die Datenverarbeitung aber nicht rückwirkend unzulässig, sondern nur für die Zukunft.

ES SOLLEN STRAFTATEN AUFGEDECKT WERDEN.

Beschäftigtendaten dürfen verarbeitet werden, wenn dadurch bereits begangene Straftaten aufgedeckt werden sollen. Dazu muss ein begründeter Verdacht gegen bestimmte Beschäftigte dokumentiert sein.

Eine vorsorgliche Datenverarbeitung zur Verhinderung von Straftaten oder zur Aufdeckung von Ordnungswidrigkeiten iist dagegen nicht zulässig.

Nicht gesetzlich geregelt ist, ob eine Datenverarbeitung bei Verdacht auf eine schwerwiegende Pflichtverletzung, die keine Straftat darstellt, in Betracht kommen kann, wie unerlaubte Konkurrenztätigkeit oder das Vortäuschen von Arbeitsunfähigkeit, wenn die Umstände des Einzelfalls berücksichtigt sind.

Auf die auf dem Dienstrechner gespeicherten Daten kann der Arbeitgeber im Einzelfall auch ohne den begründeten Verdacht einer Pflichtverletzung zugreifen. Das betrifft Dateien, die nicht als „privat“ gekennzeichnet sind. Außerdem muss diese Maßnahme offen – also nicht heimlich – erfolgen und der Arbeitgeber muss vorab darauf hingewiesen haben, welche berechtigten Gründe es dafür gibt.

Unklar ist wegen der Transparenzvorgaben der DSGVO ebenfalls, ob eine heimliche Überwachungsmaßnahme grundsätzlich zulässig sein kann (siehe dazu auch den Abschnitt „Videoüberwachung“).

Auf jeden Fall muss an die Zulässigkeit von Überwachungsmaßnahmen zur Aufdeckung schwerer Pflichtverletzungen strenge Maßstäbe angelegt werden; es empfiehlt sich, fachkundigen Rat einzuholen.

UND DIE „BERECHTIGTEN INTERESSEN“?

Wie die Erforderlichkeit und die Einwilligung sind auch die sogenannten „berechtigten Interessen“ nach der DSGVO ein Erlaubnisgrund für die Datenverarbeitung. Ob „berechtigte Interessen“ auch im Rahmen von Beschäftigungsverhältnissen die Datenverarbeitung erlauben, ist im Moment noch umstritten. Daher empfehlen wir, auf die berechtigten Interessen als Erlaubnisgrund zu verzichten, zumal der Arbeitgeber verpflichtet ist, im Streitfall die Rechtmäßigkeit der Datenverarbeitung nachzuweisen.

Die Datenverarbeitung ist unzulässig, wenn dafür kein Erlaubnisgrund vorliegt. Dann kann die zuständige Aufsichtsbehörde hohe Bußgelder verhängen. Das gilt auch bei sogenannten Datenpannen oder -lecks, wenn Daten Unbefugten zur Kenntnis gelangt sind.

BELEHRUNGS-, INFORMATIONS- UND AUSKUNFTSPFLICHTEN

Die Verarbeitung von personenbezogenen Daten im Beschäftigungsverhältnis erfordert vom Arbeitgeber, dass die Beschäftigten über die Datenverarbeitung belehrt und informiert werden. Das betrifft sowohl die Daten, die im Rahmen des Beschäftigungsverhältnisses verarbeitet werden, als auch die Verarbeitung von Daten Dritter, zum Beispiel von Kunden. (Mehr zu allgemeinen Grundsätzen der betrieblichen Datenverarbeitung findet sich in der Broschüre der Stiftung Datenschutz „Datenschutz im Betrieb“.[4])

Zu Dokumentationszwecken sollte dies stets schriftlich erfolgen oder zumindest eine schriftliche Bestätigung über die mündliche Belehrung eingeholt werden.

VERPFLICHTUNG AUF DAS DATENGEHEIMNIS

Beschäftigte, die personenbezogene Daten verarbeiten, sollten auf das Datengeheimnis verpflichtet werden. Das ist zwar in der DSGVO nicht ausdrücklich vorgesehen, aber der Arbeitgeber muss die Rechtmäßigkeit der Datenverarbeitung nachweisen. Ein Muster bietet die bayrische Aufsichtsbehörde auf ihrer Website an.[5]

INFORMATIONSPFLICHTEN GEGENÜBER DEN BESCHÄFTIGTEN

Die DSGVO regelt, dass von der Datenverarbeitung betroffene Personen eine Reihe von Rechten gegenüber der verantwortlichen Stelle ausüben können. Dies gilt auch im Beschäftigtenverhältnis.

Zu den Betroffenenrechten zählen unter anderem der Anspruch auf Information darüber, welche Daten zu welchem Zweck verarbeitet werden und wer – im Falle einer Datenweitergabe – Empfänger dieser Daten ist.

Beispiel

- Verarbeitete Daten: Name, Anschrift, Bankverbindung, Geburtsdatum, Steuerklasse, Zeugnisse, aber auch Arbeitszeiten, Gehaltsdaten, Kranken- oder Urlaubszeiten
- Verarbeitungszwecke: Lohnbuchhaltung, Entgeltauszahlung,
- Erlaubnisgrund: Erforderlichkeit zur Durchführung des Arbeitsverhältnisses
- Empfänger der Datenweitergabe: Krankenversicherung, sonstige Sozialversicherungsträger, Finanzämter

AUSKUNFTSPFLICHTEN GEGENÜBER DEN BESCHÄFTIGTEN

Zu den Betroffenenrechten zählt weiterhin ein Anspruch auf Herausgabe einer Kopie der personenbezogenen Daten, die verarbeitet werden. Dieser Anspruch muss aktiv geltend gemacht werden. Wie weit dieser Anspruch reicht, ist allerdings gesetzlich nicht geregelt und muss im Zweifel gerichtlich für den Einzelfall entschieden werden. Unter Umständen kann die Anfertigung von Kopien mit großem Aufwand verbunden und daher unverhältnismäßig sein, zum Beispiel wenn sich das Unternehmen in der Insolvenz befindet und/oder die Daten sehr umfangreich sind und zeitlich sehr weit zurückreichen.

4 https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_19.pdf
5 https://sds-links.de/dg4

ANWENDUNGEN IN DER BETRIEBLICHEN PRAXIS

HEIMLICHE VIDEOÜBERWACHUNG

Eine heimliche Überwachung ist ein schwerer Eingriff in das allgemeine Persönlichkeitsrecht der Beschäftigten. Aber auch der Arbeitgeber kann sich auf grundrechtlich geschützte Positionen berufen (Eigentumsrecht und Berufsausübungsfreiheit). Derzeit ist umstritten, ob eine heimliche Videoüberwachung unter der Datenschutz-Grundverordnung zulässig ist. Argumente, welche dagegen sprechen, sind das in der DSGVO verankerte Transparenzgebot sowie die fehlende gesetzliche Legitimationsgrundlage, da die heimliche Videoüberwachung im BDSG nicht ausdrücklich genannt wird.

Im Zuge der Interessenabwägung ist nach der bisherigen Rechtsprechung des Bundesarbeitsgerichts eine heimliche Videoüberwachung nur im absoluten Ausnahmefall als letztes Mittel zulässig, wenn ein konkreter Verdacht einer strafbaren Handlung oder einer anderen schwerwiegenden Verfehlung besteht. Durch eine unzulässige Videoüberwachung gewonnene Beweise dürfen nicht gerichtlich verwertet werden.

OFFENE VIDEOÜBERWACHUNG

Nach der Rechtsprechung des Bundesarbeitsgerichts ist auch eine offene Videoüberwachung nur in Ausnahmefällen zulässig. Mitentscheidend ist insbesondere die Intensität des Eingriffs für die Beschäftigten, die von den Bildaufnahmen erfasst sind, und ob die Maßnahme erforderlich ist oder der Zweck auch im Wege einer weniger einschneidenden Maßnahme erreicht werden kann. Zu prüfen ist, ob die Beschäftigten einem ständigen Überwachungsdruck ausgesetzt sind und damit in schwerwiegender Weise in das allgemeine Persönlichkeitsrecht eingegriffen wird und dadurch auch ein Anpassungsdruck erzeugt werden kann. Das ausschlaggebende Kriterium ist hier die Verhältnismäßigkeit.

WICHTIG: Die Intimsphäre muss unter allen Umständen unangetastet bleiben. In Umkleidekabinen oder Sanitärbereichen ist Videoüberwachung grundsätzlich unzulässig. Abgeschlossene Schränke oder Schubladen gehören zwar nicht zur Intimsphäre, dürfen jedoch allenfalls im Beisein der Beschäftigten bzw. gegebenenfalls im Beisein einer Vertrauensperson (Betriebsrat, Datenschutzbeauftragte) geöffnet werden.

Die Videoüberwachung unterliegt hohen formalen Anforderungen, so dass wir empfehlen, solche Maßnahme mit Hilfe spezieller Datenschutz-Expertise zu planen und durchzuführen. Diese Anforderungen umfassen

- das Verzeichnis von Verarbeitungstätigkeiten
- eine Datenschutz-Folgenabschätzung
- die Berücksichtigung des Prinzips „Datenschutz durch Technik“
- die Erfüllung von Informationspflichten gegenüber den Betroffenen
- die Prüfung der zeitlichen Beschränkung der Maßnahmen

Insgesamt muss die Zulässigkeit einer Videoüberwachung pro Betrieb und im Einzelfall bewertet werden. In jedem Fall unterliegt die Videoüberwachung der Mitbestimmung durch den Betriebsrat, wenn vorhanden. In diesem Fall sollte die Durchführung und Auswertung der durch Videoüberwachung erzeugten Aufnahmen in einer Betriebsvereinbarung geregelt werden.

EINSTELLUNGSTESTS

Auch in Bezug auf Einstellungstests im Rahmen eines Personalauswahlverfahrens oder ärztliche Eignungsuntersuchungen gilt der Grundsatz der Erforderlichkeit, wenn kein milderes Mittel zur Verfügung steht. So können beispielsweise ärztliche Bescheinigungen über die gesundheitliche Eignung erforderlich sein, wenn diese Eignung eine wichtige Voraussetzung darstellt, um den Beruf ausüben zu können, (z.B. Lehrer, Pilotin).

Eignungstests (Arbeitsprobe, Leistungstest, Intelligenztest, Assessments,...) müssen nachweisbar geeignet und erforderlich sein, die Eignung des Bewerbers für die vakante Position festzustellen. Allgemeine Intelligenz- oder Persönlichkeitstests zur Erfassung der Gesamtpersönlichkeit des Beschäftigten sind nicht erforderlich und damit unzulässig.

Es muss sich grundsätzlich um einen wissenschaftlich anerkannten Test handeln, der fachkundiger Ausführung bedarf. So müssen psychologische Tests von Psychologen durchgeführt werden, die aufgrund ihrer Schweigepflicht dem Arbeitgeber nur das Gesamtergebnis der Tests übermitteln dürfen (Eignung oder Nichteignung). Das Verfahren muss für die BewerberInnen transparent sein.

Eignungstests im Bewerbungsverfahren auf der Erlaubnisgrundlage der Einwilligung sind zu vermeiden, weil erhebliche Bedenken im Hinblick auf die Freiwilligkeit der Einwilligung naheliegen.

KONZERNINTERNE DATENÜBERMITTLUNG

Sollen personenbezogene Beschäftigtendaten innerhalb eines Konzerns übermittelt werden, ist eine solche Übermittlung grundsätzlich nicht privilegiert; auch hierfür ist eine Rechtsgrundlage notwendig. Innerhalb einer Unternehmensgruppe kann allerdings auch ein berechtigtes Interesse dahingehend bestehen, personenbezogene Daten für interne Verwaltungszwecke zu übermitteln, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten. Hierfür ist eine Interessenabwägung erforderlich. Wird die Datenübermittlung in einer Betriebsvereinbarung geregelt, muss diese rechtmäßig sowie für die Betroffenen nachvollziehbar (transparent) sein und der Zweckbindungsgrundsatz umgesetzt werden.

PRIVATE INTERNETNUTZUNG

Wenn eine Arbeitgeberin die private Internetnutzung am Arbeitsplatz verboten hat, darf sie auch überwachen, ob die MitarbeiterInnen das Verbot einhalten. Allerdings muss der Umfang der Kontrollmaßnahmen verhältnismäßig sein. Eine dauerhafte Überwachung wäre unverhältnismäßig.

Die Arbeitgeberin kann aber Protokolldaten stichprobenartig untersuchen, ohne das ein Personenbezug hergestellt wird. Erst wenn sich darauf Verdachtsmomente ergeben, sollten die identifizierenden Daten wie IP-Adressen herangezogen werden. Die Protokollierung der Internetnutzung durch die Arbeitgeberin bedarf stets der Zustimmung des Betriebsrats.

Ist umgekehrt die Privatnutzung erlaubt, sollten die Beschäftigten im eigenen Interesse prüfen, ob eine schriftliche Vereinbarung mit der Arbeitgeberin zu Inhalt und Umfang der gestatteten Privatnutzung vorliegt, beispielsweise eine Betriebsvereinbarung, und ob diese an Bedingungen geknüpft ist. Wenn die Arbeitgeberin die private Internetnutzung unter bestimmten Bedingungen erlaubt (zum Beispiel zeitlich befristet), benötigt sie die Einwilligung der Beschäftigten, um die Einhaltung der Nutzungsregelungen zu kontrollieren.

ARBEITEN IM HEIMBÜRO

Um das Arbeiten im Heimbüro datenschutzgerecht zu ermöglichen, muss der Arbeitgeber die notwendigen technischen und organisatorischen Maßnahmen bereitstellen und den Beschäftigten in nachvollziehbarer Form erläutern. Die Maßnahmen beziehen sich einerseits auf den Schutz der personenbezogenen Daten, die im häuslichen Umfeld verarbeitet werden, aber andererseits ebenso auf die Wahrung der Intim- und Privatsphäre der MitarbeiterInnen. So sollten bestimmte Videokonferenz-Systeme aufgrund der bekannt gewordenen Sicherheitsproblemen und der unverschlüsselten Speicherung des Inhalts der Gespräche auf den Servern des Anbieters nicht genutzt werden.

Zu beachten ist in diesem Zusammenhang, dass das allgemeine Persönlichkeitsrecht auch das Recht am gesprochenen Wort schützt. Gespräche der Beschäftigten dürfen weder heimlich aufgenommen noch ohne ihre Einwilligung verwertet werden. Dies kann sogar strafrechtlich relevant sein. Die Geschäftsleitung sollte sich bei der

Auswahl geeigneter Werkzeuge von der Datenschutzbeauftragten beraten lassen. Darüber hinaus sollten Beschäftigte beim Einsatz von Videokonferenzsystemen eigenverantwortlich und im eigenen Interesse berücksichtigen, dass Einblicke in ihr häusliches Umfeld möglich sind und etwa beim Teilen ihres Bildschirms darauf achten, ihren Mailaccount für die Zeit ihrer Teilnahme zu deaktivieren, da private Mails über Pop-Up-Fenster für die anderen Teilnehmer sichtbar werden können.

Im Falle der erlaubten dienstlichen Nutzung von privaten Geräten der Beschäftigten kann der Arbeitgeber außerdem nicht verlangen, auf diesen einen Messengerdienste zu installieren, der auf Kontaktdaten oder das Telefonverzeichnis zugreift. Allerdings ist der Einsatz privater Geräte im Rahmen dienstlicher Nutzung grundsätzlich als kritisch zu bewerten und Arbeitgeber dürfen in keinem Fall Zugriff auf die privaten Daten ihrer Beschäftigten nehmen. MitarbeiterInnen sollten daher bereits im eigenen Interesse private und dienstliche Datenträger trennen und deutlich kennzeichnen. Dies gilt ebenso, wenn der Arbeitgeber im umgekehrten Falle den Beschäftigten die private Nutzung von dienstlichen Geräten erlaubt – hier sollten die Beschäftigten persönliche oder vertrauliche Dateiordner unmissverständlich benennen. Ein zusätzlicher Schutz der Beschäftigten besteht darin, dass ein Arbeitgeber niemals ohne Zustimmung des Betriebsrats ein System einführen darf, welches geeignet ist, das Verhalten der Beschäftigten, zu überwachen und zu protokollieren.

Die Beschäftigten sollten weiterhin mit dem Arbeitgeber klären, in welchen Grenzen sie berufliche Kontakte auf ihren privaten Geräten speichern dürfen. Insgesamt hängen Umfang und Beschränkungen stets vom Schutzbedarf der „dienstlichen“ Daten ab. Wichtig ist, dass auf dem Endgerät der Beschäftigten keine App oder kein Messengerdienst installiert sind, die auf die dienstlichen Kontaktdaten zugreifen.

Mit Blick auf die personenbezogenen Daten von Kunden oder anderen Beschäftigten gilt, dass sensible personenbezogene Daten (z. B. Gesundheitsdaten oder Gewerkschaftszugehörigkeit) auch in einer Notsituation (wie der Corona-Pandemie) nur auf dienstlichen Geräten verarbeitet werden dürfen.

Zu beachten ist: Aktuell gibt es zur Bewältigung der Corona-Pandemie seitens der Aufsichtsbehörden befristete Ausnahmeregelungen zum Einsatz von Videokonferenzen und Messengerdiensten.

FAZIT

Für viele Menschen ist das Beschäftigungsverhältnis die Grundlage ihrer wirtschaftlichen Existenz. In diesem Verhältnis werden zahlreiche, teils sensible, personenbezogene Daten erhoben und verarbeitet. Beschäftigte müssen sich darauf verlassen, dass dies im Einklang mit den gesetzlichen Vorschriften geschieht. Ziel der vorliegenden Handreichung ist es, für den vorschriftsmäßigen Umgang mit personenbezogenen Daten in der betrieblichen Praxis zu sensibilisieren. Dazu haben wir die wichtigsten Begriffe erklärt und typische Situationen erläutert. Wir wollten häufige Fragen beantworten und Unklarheiten auszuräumen. Ob uns das gelungen ist, können Sie beurteilen, wenn Sie die folgenden Fallbeispiele betrachten.

Wir freuen uns auf Ihre Rückmeldungen und Verbesserungsvorschläge:

mail@stiftungdatenschutz.org

BESCHÄFTIGTEN DATENSCHUTZ

FALLBEISPIELE

THEMEN

IM BEWERBUNGSVERFAHREN

Constanze ist Personalleiterin der Spedition „HappyTrans“. Unter welchen Voraussetzungen darf sie personenbezogene Daten über Bewerberinnen und Bewerber erheben und verarbeiten? Zum Bewerbungsverfahren bei „HappyTrans“ gehört ein umfassender Online-Fragebogen.

Personenbezogene Daten einer Bewerberin oder eines Bewerbers dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses erforderlich ist. Die Fragen des Bewerbungsbogens sind stets unter dem Aspekt stellen, ob diese für die Begründung des konkreten Beschäftigungsverhältnisses erforderlich sind.

Darf Constanze in dem Bewerbungsbogen nach einer Schwerbehinderung fragen? Nach einer Schwangerschaft? Oder nach einer Vorstrafe?

Die Frage nach einer Schwerbehinderung stellt einen Eingriff in das allgemeine Persönlichkeitsrecht der Bewerberin oder des Bewerbers dar und verletzt damit das informationelle Selbstbestimmungsrecht. Diese Wertung ergibt sich auch aus dem Allgemeinen Gleichbehandlungsgesetz (AGG). Ziel dieses Gesetzes ist es, Benachteiligungen unter anderem aus Gründen einer Behinderung oder aufgrund des Geschlechts zu verhindern. Der Arbeitgeber darf danach pauschal keine Auskunft darüber verlangen, ob eine Behinderung vorliegt. Constanze könnte allenfalls fragen, ob die Bewerberin oder der Bewerber an gesundheitlichen, seelischen oder anderen Beeinträchtigungen leidet, die der Erfüllung der erwarteten arbeitsvertraglichen Pflichten entgegenstehen, und zwar wenn dies gerade die wesentliche Voraussetzung für den konkreten Arbeitsplatz darstellt.

Aus den gleichen Gründen darf auch nicht nach einer bestehenden oder geplanten Schwangerschaft gefragt werden. Die pauschale Frage nach einer Schwerbehinderung oder nach einer Schwangerschaft ist demnach unzulässig.

Nach Vorstrafen darf bei der Einstellung nur insofern gefragt werden, wie die Art des zu besetzenden Arbeitsplatzes dies erfordert. Künftige Kurierfahrerinnen dürfen also nach Verkehrsdelikten gefragt werden; oder Buchhalter nach Betrugsdelikten.

Ein polizeiliches Führungszeugnis darf ebenfalls nicht pauschal verlangt werden, weil dies auch Vorstrafen enthält, die im Bundeszentralregister bereits getilgt sind und daher nicht mehr angegeben werden müssen.

Zur Jahresmitte hat Constanze die Stelle eines Kuriers besetzt. Sie weiß, dass zum Weihnachtsgeschäft zahlreiche Kuriere gebraucht werden und speichert die Daten der abgelehnten BewerberInnen in einer Datenbank, um sie später anzuschreiben.

Daten von Bewerbern und Bewerberinnen sollten nicht länger als vier Monate gespeichert und danach gelöscht werden. Sofern Arbeitgeber oder Arbeitgeberinnen für zukünftige Stellenbesetzungen Interesse an einer längerfristigen Speicherung haben, muss die freiwillige und informierte Einwilligung der Bewerber und Bewerberinnen eingeholt werden. Ansonsten gilt, dass ein abgelehnter Bewerber/eine abgelehnte Bewerberin nach dem Allgemeinen Gleichbehandlungsgesetz (AGG) zwei Monate Zeit hat, bei einem Verstoß gegen das Benachteiligungsverbot im Rahmen des Auswahlverfahrens einen Schadensersatzanspruch geltend zu machen. Daher können Bewerbungsunterlagen frühestens nach zwei Monaten gelöscht werden, damit Arbeitgeber und Arbeitgeberinnen die Möglichkeit haben, sich gegen mögliche Ansprüche zu verteidigen. In der Praxis ist die zulässige Höchstspeicherfrist von Bewerbeunterlagen noch nicht abschließend geklärt. Aus Gründen der Verhältnismäßigkeit ist eine längere Speicherdauer als vier Monate jedoch nicht erforderlich.

Weil die Tätigkeit als Kurier besondere Zuverlässigkeit erfordert, schaut Constanze sich die Social-Media-Profile ihrer Bewerber an und fragt die Namen mit einer Suchmaschine ab. Außerdem ruft sie frühere Vorgesetzte der BewerberInnen an. Ist das zulässig?

Zum Schutz des Grundrechts auf informationelle Selbstbestimmung sind Daten grundsätzlich beim Bewerber zu erheben. BewerberInnen sollen entscheiden können, was der neue Arbeitgeber über sie erfährt.

Auskünfte beim früheren Arbeitgeber sind daher nur mit Einwilligung und vorheriger Information erlaubt. Seitens der Recherchen in sozialen Netzwerken wie Facebook oder Twitter halten die Datenschutzaufsichtsbehörden für unzulässig ; es sei denn, es handelt sich um berufliche Netzwerken wie etwa XING oder LinkedIn. Eine Ausnahme besteht, wenn die Online-Präsenz der BewerberInnen als Arbeitsproben betrachtet werden können, die direkte Aufschlüsse auf deren berufliche Eignung zulässt, zum Beispiel bei Social Media Managern oder Website-Designern.

Die Informationsbeschaffung durch allgemein zugängliche Quellen ist zulässig, wenn sie für die Einstellungsentscheidung erforderlich ist und ausschließlich Informationen betrifft, die vom Fragerecht umfasst sind. Über die Quelle der Daten und die Rechtsgrundlage der Verarbeitung müssen die Bewerberinnen und Bewerber innerhalb eines Monats informiert werden.

Allerdings wird dies in der Rechtspraxis auch unter Anwendung der DSGVO nicht einheitlich bewertet, so dass sich hier eine gesetzliche Klarstellung empfehlen würde.

Aus Gründen der Effizienz möchte Constanze gern die Auswahlgespräche per Skype Video-Telefonat über das Internet führen. Wie ist dies zu beurteilen?

Die Aufsichtsbehörden empfehlen, die schutzwürdigen Belange der Bewerberinnen und Bewerber zu berücksichtigen und auf Video-Telefonate zugunsten persönlicher Auswahlgespräche zu verzichten. Dennoch kann ein solches Video-Telefonat zulässig sein, wenn die Betroffenen dies selbst wünschen. Dann kann von einer freiwillig erteilten Einwilligung ausgegangen werden, wenn die Betroffenen über den Verwendungszweck und die Weitergabe der Daten durch den Diensteanbieter informiert werden. (Skype zum Beispiel speichert bis zu 90 Tage lang die Chat-Protokolle auf den Servern des Mutterkonzerns Microsoft in den USA.) Die Aufsichtsbehörden haben zwar für die Zeit der Corona-Pandemie befristete Ausnahmeregelungen zum Einsatz von Messenger- und Videokonferenzsystemen veröffentlicht. Dennoch gilt, dass nach wie vor der Datenschutz beachtet werden muss. Es sollte daher vorrangig geprüft werden, ob alternativ eine Telefonkonferenz in Betracht kommt, wenn bei mehr als zwei Beteiligten keine Ende-zu-Ende-Verschlüsselung der Kommunikation möglich ist. Ansonsten sollten Anbieter von Videokonferenzsystemen mit Sitz in der EU oder der Schweiz gewählt werden, wenn innerhalb der Onlinesitzung sensible Daten besprochen werden sollen.

Die Aufzeichnung von Auswahlgesprächen ist dagegen ein deutlich schwererer Eingriff in das Selbstbestimmungsrecht der BewerberInnen. Eine Zulässigkeit wird daher von den Aufsichtsbehörden grundsätzlich verneint. Dies ist vor allem auch vor dem Hintergrund der bereits besprochenen Schwierigkeit zu sehen, im Arbeitsverhältnis eine freiwillige Einwilligung, in diesem Falle eine Einwilligung in die Aufzeichnung, einzuholen.

Ferdinand ist Eigentümer der Firma „HappyTrans“ und fordert Constanze auf, bei sämtlichen Einstellungen routinemäßig einen Drogentest durchführen zu lassen. Er verweist darauf, dass er „keine Straftäter“ in seinem Betrieb beschäftigen wolle. Was wird Constanze ihm antworten?

Drogentests sind grundsätzlich nur zulässig, wenn die Betroffenen wirksam schriftlich eingewilligt haben – wobei auf die Probleme einer wirksamen Einwilligung durch die Beschäftigten bereits hingewiesen wurde. Außerdem müssen sie für die Besetzung der konkreten Stelle erforderlich und geeignet sein. Der Test muss darauf gerichtet sein, eine Alkohol-oder Drogenabhängigkeit nachzuweisen; es darf nicht lediglich darum gehen, den Alkohol-oder Drogenkonsum zu ermitteln. Arbeitsplatzrelevantes Verhalten liegt allerdings nur vor, wenn die Beschäftigten durch ein abhängigkeitsbedingtes Fehlverhalten sich selbst, Leben und Gesundheit Dritter oder bedeutende Sachwerte des Unternehmens gefährden könnte.

PERSONALVERWALTUNG

Malermeister Schwarz beschäftigt zwei Angestellte, für die er jeweils handschriftliche Ordner mit ihren Stammdaten angelegt hat. Auf einem Zettel notiert er, dass Hassan eine Woche wegen Schnupfen krankgeschrieben ist und Henriette schon wieder an einem Montag zu spät im Betrieb erscheint. Bei der Einstellung der Aushilfe Herbert ergänzt er beim Anlegen des Personalordners handschriftlich, dass Herbert evangelisch ist. Darf er das?

Die Anwendbarkeit der Vorschriften der DSGVO und des BDSG setzt im Beschäftigtenverhältnis keine automatisierte bzw. IT-gestützte Verarbeitung von Personaldaten voraus. Auch Daten auf Papier unterliegen der DSGVO und dem BDSG.

Die Verarbeitung besonders sensibler Kategorien von Daten (z. B. Religionszugehörigkeit, Gesundheitsdaten) kann zur Erfüllung der Pflichten aus dem Arbeitsrecht oder des Sozialschutzes erforderlich sein. In diesem Falle braucht die Verarbeitung dieser sensiblen Daten keine Einwilligung der Beschäftigten; es sei denn, das Interesse des Beschäftigten an dem Ausschluss der Verarbeitung überwiegt. Zu berücksichtigen ist dabei, dass Angaben zur Religionszugehörigkeit nur für die Abführung von Kirchensteuer erhoben und genutzt werden dürfen.

Bei einer längerfristigen Speicherung von Beschäftigtendaten, etwa beim Führen von Personalakten, gelten die Maßstäbe der Erforderlichkeit sowie der Verhältnismäßigkeit. Informationen zur Identität der Beschäftigten sind erforderlich (Name, Anschrift, Alter, Geschlecht, Familienstand, Schulabschluss und Ausbildung). Für die Beurteilung ist wesentlich, ob die langfristig gespeicherten Daten die Persönlichkeitsrechte der Beschäftigten beeinträchtigen. Eine Speicherung von Informationen zu konkreten Krankheitsgründen oder Notizen des Arbeitgebers über die Leistungen oder Nichtleistungen der Beschäftigten können einen Eingriff in das Persönlichkeitsrecht des Arbeitnehmers begründen. Eine Abmahnung hingegen darf als Dokumentation eines Fehlverhaltens in der Personalakte geführt werden. Von besonderer Bedeutung ist außerdem der Zugriffschutz für die gespeicherten Daten. So gilt für ärztliche Gutachten, Gesundheitszeugnisse, etc., dass diese in verschlossenen Umschlägen zur Personalakte zu nehmen sind.

Ausblick: Aufgrund der Einführung einer digitalen Arbeitsunfähigkeitsbescheinigung entfällt zukünftig die Verpflichtung zur Vorlage einer Arbeitsunfähigkeitsbescheinigung, da der Arbeitgeber diese ab dem Jahre 2021 bei den Krankenkassen digital abrufen kann. Die Beschäftigten müssen jedoch nach wie vor ihre Arbeitsunfähigkeit dem Arbeitgeber melden und benötigen eine ärztliche Feststellung.

Ayse hat ihr Ausbildungsverhältnis bei der Deutschen Röhren AG begonnen. Kurz darauf bekommt sie Post von der „V.Traut"-Versicherung, welche dem gleichen Konzernverbund angehört. Das Versicherungsunternehmen bietet ihr 30% Rabatt an, wenn sie dort eine private Unfallversicherung abschließt. Auf Nachfrage bei ihrem Chef erhält Ayse die Auskunft, dass der Betriebsrat der Deutschen Röhren AG der Übermittlung ihrer Daten an die „V.Traut"-Versicherung zugestimmt hat. Außerdem sei die Datenweitergabe innerhalb des Konzernverbundes unkritisch. Die datenschutzfreundliche Ayse hat dennoch Bedenken. Zu Recht?

Auszubildende fallen unter den Begriff der „Beschäftigten", daher ist hier die Datenschutz-Grundverordnung anzuwenden. Auch innerhalb eines Konzerns ist jedes rechtlich selbstständige Unternehmen im datenschutzrechtlichen Sinne „Dritter". Daher ist für die Datenweitergabe eine Rechtsgrundlage erforderlich.

Denkbar wäre, dass ein berechtigtes Interesse besteht, personenbezogene Daten für interne Verwaltungszwecke zu übermitteln. Bei Ayse und der „V.Traut"-Versicherung trifft dies jedoch nicht zu, weil es sich nicht um Verwaltungszwecke, die für die Durchführung des Ausbildungsverhältnisses erforderlich sind, handelt, sondern um Kundenwerbung.

Auch ein berechtigtes Interesse der „V.Traut" an der Kundenwerbung ist auszuschließen, weil eine Interessenabwägung ergeben müsste, dass Ayses Interesse daran überwiegt, dass ihre Daten nicht ohne ihr ausdrückliches Einverständnis weitergegeben werden.

Zudem muss der Betriebsrat die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer schützen und fördern. Im geschilderten Fall würde dagegen zusätzlich ein Eingriff in das Persönlichkeitsrecht der Beschäftigten vorliegen. Die Zustimmung des Betriebsrats ist hier daher unwirksam, weil der Betriebsrat gar nicht zuständig ist. Eine entsprechende Betriebsvereinbarung wäre nichtig.

Rinku ist in der Personalabteilung eines großen Getränkefachhandels beschäftigt und hat Zugriff auf die unterschiedlichen Beschäftigtendaten. Darf seine Arbeitgeberin seine Zugriffe auf die Beschäftigtendatenbank protokollieren? Rinku hat die Befürchtung, dass seine Arbeitgeberin nachprüft, welche Zeitdauer er für die einzelne Fallbearbeitung benötigt und unterstellen könnte, dass er nicht effizient arbeitet.

Der Umgang mit Protokolldaten kann in der Praxis eine Herausforderung darstellen, da einerseits die Dokumentation sowohl aus revisionsrechtlichen als auch aus datenschutzrechtlichen Gründen erforderlich sein kann, andererseits aber die Gefahr einer Leistungs- und Verhaltenskontrolle von Beschäftigten besteht. Zu berücksichtigen ist, dass jeder Verantwortliche, z.B. ein Arbeitgeber, die datenschutzkonforme Verarbeitung nachweisen muss. So kann damit der Nachweis der Umsetzung der gesetzlichen Datenschutzanforderungen im Sinne einer technisch-organisatorischen Maßnahme verbunden sein. Insbesondere wenn es sich um Zugriffsmöglichkeiten der Beschäftigten auf sensible Daten von Kunden oder Kollegen handelt, kann ein Bedarf an einer Protokollierung bestehen – beispielsweise auch zur Dokumentation, dass keine unberechtigten Zugriffe auf personenbezogene Daten erfolgen. Die Protokollierung ist also eine wichtige Maßnahme, um später überhaupt beurteilen zu können, ob die (bereits zurückliegende) Datenverarbeitung aus datenschutzrechtlicher Sicht rechtmäßig war. Allerdings müssen im Vorfeld die Zwecke der Auswertung detailliert beschrieben werden (etwa der durch konkrete Tatsachen begründete Verdacht einer Straftat). Ebenso muss der Zugriff auf die Protokolldaten datenschutzrechtlichen Anforderungen genügen und erfordert ein detailliertes Berechtigungskonzept. Dies bedeutet, dass die Zwecke der Auswertung klar definiert werden müssen und die Auswertung selbst nur von Personen vorgenommen werden darf, die hierzu befugt sind. Es müssen außerdem Löschungsfristen für die aufgezeichneten Daten bzw. die Protokolldaten definiert sein. Gegebenenfalls müssen die Protokolldaten nach dem Stand der Technik verschlüsselt werden. Die Definition des Zwecks darf nicht allgemein und pauschal, etwa zum Zwecke der „IT-Sicherheit" definiert

sein. Soll eine Auswertung erfolgen, muss vielmehr ein konkreter Verdacht vorliegen. Eine Überwachung ins Blaue hinein ist unzulässig. Es ist sicherzustellen, dass eine Verhaltens- und Leistungskontrolle ausgeschlossen ist. Daher können (im ersten Schritt) ebenso nicht-personenbezogene Auswertungen und Stichproben ausreichend sein. Außerdem ist der Betriebsrat einzubinden – vorausgesetzt, dass ein solcher im Betrieb vorhanden ist.

Konrad Controletti, der Inhaber einer Hausgerätereparaturwerkstatt, möchte sein Außendienstteam besser im Blick haben. Daher lässt er sämtliche Dienstfahrzeuge mit einem Ortungssystem ausstatten. Ist dies unter datenschutzrechtlichen Gesichtspunkten zulässig?

Nein. Die umfassende und anlasslose Überwachung von Arbeitnehmerinnen und Arbeitnehmern ist unzulässig.

Ändert sich etwas, wenn Konrad Controletti die Fahrzeuge vor Diebstahl schützen möchte und das Ortungssystem dazu dienen soll, Mitarbeiter- und Fahrzeugeinsätze besser zu koordinieren?

Die Verarbeitung der Ortungsdaten muss für die Durchführung des Beschäftigungsverhältnisses erforderlich sein. Ob „berechtigte Interessen“ als Erlaubnisgrund für die Datenverarbeitung im Beschäftigungsverhältnis in Betracht kommen, ist derzeit noch umstritten. Auf jeden Fall unterliegt eine solche Maßnahme der Mitbestimmung des Betriebsrats. Es ist außerdem zu beachten, dass beim Einsatz von Ortungssystemen, wie z.B. GPS, Informationspflichten gegenüber den Beschäftigten zu erfüllen sind. Die Verwendung eines solches Systems muss transparent sein. Hierzu wird ebenso vertreten, dass auch der Anruf auf dem Mobiltelefon der Beschäftigten ausreichend sein kann, um den Aufenthaltsort zu ermitteln: So hat das Verwaltungsgericht Lüneburg bezogen auf ein Gebäudereinigungsunternehmen entschieden, dass die ständige Erfassung der Fahrzeugposition weder als Diebstahlprävention noch für die Koordinierung der Arbeitseinsätze geeignet oder erforderlich ist. Als milderes Mittel für die Einsatzkontrolle stünde der Kontakt zu den Mitarbeitern per Mobiltelefon zur Verfügung. Allerdings könnte diese Beurteilung in anderen Branchen, zum Beispiel im Transportgewerbe, anders ausfallen.

Die Deutsche Röhren AG ist ein besonders kundenorientiertes Unternehmen möchte auf ihrer Unternehmenswebseite die Fotos und Kontaktdaten (Name, dienstliche Telefonnummer, dienstliche E-Mail-Adresse, Funktion) ihrer AbteilungsleiterInnen veröffentlichen.

Die Veröffentlichung der Kontaktdaten von Arbeitnehmern und Arbeitnehmerinnen, die im Rahmen ihrer Aufgaben für den Außenkontakt verantwortlich sind, ist auch ohne deren Einwilligung zulässig. Die Beschäftigten müssen darüber informiert werden. Die Veröffentlichung der Fotos ist jedoch davon nicht gedeckt.

Das Sommerfest der Firma „HappyTrans“ war wieder ein großer Erfolg. Social Media Manager Denis hat viele Fotos gemacht, und fragt seine Chefin, ober er eine Auswahl auf der Website und bei Facebook veröffentlichen darf.

Bildnisse dürfen nur mit Einwilligung des Betroffenen veröffentlicht werden. Möchte ein Arbeitgeber daher Fotos seiner Beschäftigten auf der Webseite veröffentlichen, muss er zuvor deren Einwilligung einholen. Die Einwilligung muss informiert und freiwillig sein. „Informiert“ bedeutet hier, dass die Betroffenen wissen müssen, wo, in welchem Kontext und für wie lange die Fotos veröffentlicht werden sollen, und dass sie ihre Einwilligung jederzeit widerrufen können. „Freiwillig“ bedeutet, dass den Betroffenen keinen negativen Konsequenzen drohen, falls sie ihre Einwilligung in die Veröffentlichung verweigern. Die Einwilligung sollte schriftlich eingeholt werden; der Arbeitgeber unterliegt den Informationspflichten der DSGVO.[6]

Dies gilt allerdings nur, wenn die Personen auf den Fotos erkennbar sind.

6 https://sds-links.de/xhp

NUTZUNG VON INFORMATIONS- UND KOMMUNIKATIONSTECHNIK

Konrad Controletti möchte gern die Telefonate seiner Arbeitnehmer ohne deren Wissen mithören. Wie ist dies rechtlich zu bewerten?

Strafrechtlich relevant ist lediglich das Aufnehmen des nicht-öffentlich gesprochenen Wortes oder die Zugänglichmachung an Dritte. Das reine Mithören ist strafrechtlich nicht relevant (zumindest nicht bei handelsüblichen bzw. gebräuchlichen Mithörvorrichtungen in privaten oder geschäftlichen Telefonanlagen). Zu berücksichtigen ist dennoch das Persönlichkeitsrecht der Beschäftigten: Das Recht am gesprochenen Wort ist geschützt und es liegt ein Eingriff in das Persönlichkeitsrecht der Beschäftigten vor, wenn der Arbeitgeber die Vertraulichkeit der Kommunikation verletzt. Dies gilt unabhängig davon, ob es sich um private oder geschäftliche Kommunikation handelt.

Außerdem ist Controletti der Auffassung, dass er die Mails seiner Mitarbeiter und Mitarbeiterinnen jederzeit lesen darf, sofern es sich um betriebliche Kommunikation handelt. Die IT-Azubis Hakan und Charlotte haben Bedenken und weisen darauf hin, dass dies in einer Betriebsvereinbarung geregelt werden müsse.

Hier wird vertreten, dass der dienstlich bereitgestellte Mail-Account zu den Betriebsmitteln zählt, über die der Arbeitgeber entscheidet und die seinem Direktionsrecht unterliegen. Er kann daher die private Nutzung verbieten und bei dienstlicher Kommunikation jederzeit Einsicht verlangen bzw. sich diese zeigen lassen, sofern nicht die Korrespondenz mit betrieblichen Vertrauensstellen (z.B. Betriebsrat, Betriebsarzt) betroffen ist. In der Praxis ist allerdings zu berücksichtigen, dass Mails, selbst wenn diese aus dienstlichem Interesse verfasst sind, mit dem formalen Schriftverkehr nicht gleichgesetzt werden können. Die Kommunikation per Mail ist regelmäßig weniger formal. Insgesamt darf der Inhalt von E-Mails vom Arbeitgeber nicht weiter zur Kenntnis genommen werden, wenn diese erkennbar privat sind. Eine andere Bewertung kann sich allenfalls im Rahmen von zulässigen Missbrauchskontrollen ergeben.

Wie ist die rechtliche Situation zu bewerten, wenn Konrad Controletti ein elektronische Zeiterfassung mittels Fingerabdruck einführt? Hakan und Charlotte verweisen wiederum auf eine fehlende Kollektivvereinbarung und eine freiwillige Einwilligung der Beschäftigten.

Bei einem Fingerabdruck handelt es sich biometrische Daten und um besondere Kategorien personenbezogener Daten, deren Verarbeitung grundsätzlich verboten ist. Etwas anderes gilt, wenn eine gesetzlich geregelte Ausnahme vorliegt, wie etwa eine (freiwillige) Einwilligung. Zu berücksichtigen ist, dass die Verarbeitung eines Fingerabdrucks die Privatsphäre und damit das Recht auf informationelle Selbstbestimmung im besonderen Maße verletzen kann und somit auch besonders hohe Anforderungen an die Rechtmäßigkeit zu stellen sind.

Sofern keine Einwilligung vorliegt, muss die Verarbeitung erforderlich sein, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben kann. Im Rahmen der damit verbundenen Verhältnismäßigkeitsprüfung muss der Arbeitgeber daher prüfen, ob dass das schutzwürdige Interesse der betroffenen Personen (der Beschäftigten) an dem Ausschluss der Verarbeitung überwiegt. Damit ist auch die kritische Prüfung verbunden, ob im betrieblichen Alltag ein anderes, gleich wirksames Verfahren eingeführt werden kann, das weniger gravierend in das Persönlichkeitsrecht eingreift. Dies ist stets Frage des Einzelfalls und muss vom Arbeitgeber entsprechend dargelegt werden. Dazu kann die Prüfung und Begründung gehören, aus welchen Gründen kein manuelles Zeiterfassungsverfahren in Betracht kommt oder ob besondere Gründe vorliegen, die ein Fingerprintverfahren aus Missbrauchsgesichtspunkten erforderlich machen. Dabei muss in die Abwägung ebenso einbezogen werden, welchen Zweck das biometrische Verfahren verfolgt. Hierzu wird die Auffassung vertreten, dass biometrische Daten zwar zur Kontrolle beim Eintritt in Sicherheitsbereiche, nicht jedoch im Rahmen der Arbeitszeit-

erfassung verarbeitet werden können (siehe auch die Entscheidung des Arbeitsgerichts Berlin vom 19.10.2019, AZ 29 Ca 5451/19).

Bei „HappyTrans“ sollen künftig die Beschäftigten WhatsApp auf den dienstlichen Telefonen nutzten. Das ist doch unproblematisch, das nutzen ja ohnehin alle privat?

WhatsApp teilt in seiner Nutzungsrichtlinie mit:

„Im Einklang mit geltenden Gesetzen stellst du uns regelmäßig die Telefonnummern in deinem Mobiltelefon-Adressbuch zur Verfügung, darunter sowohl die Nummern von Nutzern unserer Dienste als auch die von deinen sonstigen Kontakten.“

Allerdings: Die Personen, deren Kontaktdaten in den Adressbüchern gespeichert sind, haben keine Erlaubnis dafür erteilt, dass ihre Kontaktdaten an WhatsApp weitergegeben werden und auf Servern außerhalb Europas gespeichert werden dürfen. Darüber hinaus erhält WhatsApp Kenntnis von den Metadaten (Zeitpunkt und Dauer der Kommunikation, IP-Adresse, Geräte-ID, etc.), die Rückschlüsse auf die Beteiligten zulassen und Profilerstellung zulassen. Zudem ist die dauerhafte Verschlüsselung der Text- und Bilddaten fraglich. Eine datenschutzkonforme Nutzung von WhatsApp ohne Übertragung von Telefonnummern ist nur bei dauerhafter Deaktivierung des Zugriffs auf die Kontakte direkt nach der Installation möglich. Die deutschen Aufsichtsbehörden weisen darauf hin, dass der Einsatz von WhatsApp durch Unternehmen zur betrieblichen Kommunikation gegen die Datenschutz-Grundverordnung verstößt. Auf die Nutzung von WhatsApp sollte im betrieblichen Kontext verzichtet werden, zumal sichere, datenschutzkonforme Alternativen wie Threema, Signal oder Wire zur Verfügung stehen. Die private Nutzung fällt jedoch nicht unter das Datenschutzrecht.

WEITERE INFORMATIONSMATERIALIEN

Alle Beschäftigten sollten sich mit den Kernpflichten des Datenschutzes auskennen. Daher liegen unsere Broschüren für den Einsatz in Unternehmen, Praxen, Vereinen und anderen Organisationen vollständig überarbeitet und an die Anforderungen der EU-Datenschutz-Grundverordnung angepasst vor.

„Datenschutz im Betrieb – Eine Handreichung für Beschäftigte“ soll die notwendigen Hintergründe vermitteln und praxisnah die gesetzlich vorgeschriebenen Informationen darstellen. Die Broschüre umfasst 40 Seiten im DIN A5-Format.

„Datenschutz ganz kurz“ fasst die allerwichtigsten Punkte kurz und knapp zusammen. Für alle, die sich kompakt und praktisch über die Anforderungen des betrieblichen Datenschutzes informieren wollen, auf 20 Seiten im Format DIN lang.

„Das neue Recht auf Datenportabilität“: Mit Inkrafttreten der EU-Datenschutz-Grundverordnung bekam erstmals jede Person das „Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten“. Für die Anbieter von datenverarbeitenden Diensten wird es damit erforderlich, personenbezogene Daten so vorzuhalten, dass diese in einem gängigen Format „mitgenommen“ werden können. Was dies in der Praxis bedeutet, haben wir in zwei Broschüren zusammengetragen.

https://stiftungdatenschutz.org/themen/datenschutz-im-betrieb/

https://stiftungdatenschutz.org/themen/datenportabilitaet/

STICHWORTVERZEICHNIS

IMPRESSUM

Herausgeber
Stiftung Datenschutz

Autorinnen
Prof. Dr. Anne Riechert
Antje Simon, M.A.

Version
2.0, Stand Juli 2020