Industrie- und Handelskammer
Ostwestfalen zu Bielefeld

Beschäftigtendatenschutz

Merkblatt

Ihr Ansprechpartner:
Christina Meyer
Telefon:
0521 554-215
Fax:
0521 554-420

Stand: 07/2024

Gesamt: 4 Seiten

Der Umgang mit personenbezogenen Daten zukünftiger bzw. bereits beschäftigter Mitarbeiter regelt insbesondere die Datenschutzgrundverordnung (DSGVO) sowie das Bundesdatenschutzgesetz (BDSG). Im Folgenden soll ein Überblick über die wesentlichen Regelungen verschafft werden.

Beschäftigte
Wer gilt eigentlich als Beschäftigter? Beschäftigte im Sinne des Datenschutzrechts sind zunächst alle privatrechtlich verpflichteten Arbeitnehmerinnen und Arbeitnehmer. Darüber hinaus gilt die Beschäftigteneigenschaft von Leiharbeitern auch im Verhältnis zum Entleiher, also nicht nur zum Verleiher. Des Weiteren fallen auch Bewerber, die sich für ein Unternehmen interessieren, unter diese Definition.

Personenbezogene Daten
Personenbezogene Daten sind alle Informationen, die eindeutig einer bestimmten natürlichen Person zugeordnet sind oder diese Zuordnung zumindest mittelbar erfolgen kann. D.h. alle Informationen/Daten, die eine Person identifizierbar machen. Die Informationen können sich sowohl auf persönliche als auch auf sachliche Verhältnisse beziehen. Folgende Angaben sind beispielsweise personenbezogene Daten:

- Name
- Geburtsdatum
- Anschrift
- E-Mail-Adresse
- Telefonnummer
- Beruflicher Werdegang
- Körperliche Merkmale
- Gesundheitsdaten
- Beziehungen
- Religionszugehörigkeit
- Politische Orientierung
- Ethnische Herkunft
- Steuerrechtliche Angaben
- Sozialrechtliche Angaben

Verarbeitung von Beschäftigtendaten
Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, soweit dies für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist.

HINWEIS:
Das Merkblatt enthält nur erste Hinweise und erhebt keinen Anspruch auf Vollständigkeit. Obwohl es mit größtmöglicher Sorgfalt erstellt wurde, kann eine Haftung für die inhaltliche Richtigkeit nicht übernommen werden.

Auch die Verarbeitung von Beschäftigtendaten auf der Grundlage von Kollektivvereinbarungen ist zulässig. Dazu gehören Tarifverträge sowie Betriebs- und Dienstvereinbarungen. Beschäftigtendaten dürfen in diesem Fall ebenso verarbeitet werden, soweit es für die Rechte und Pflichten der Interessenvertretungen der Beschäftigten erforderlich ist.

Beschäftigte können auch freiwillig in eine Datenverarbeitung einwilligen. § 26 Abs. 2 BDSG konkretisiert das Merkmal "freiwillig" dahingehend, dass die Freiwilligkeit im Beschäftigungsverhältnis vom Grad der Abhängigkeit des Beschäftigten sowie den konkreten Umständen der Erteilung abhängig ist. Freiwilligkeit liegt vor, wenn der Beschäftigte einen rechtlichen oder wirtschaftlichen Vorteil erlangt oder der Arbeitgeber und der Beschäftigte gleichgelagerte Interessen verfolgen. Der Beschäftigte muss aber eine echte Wahlmöglichkeit haben, ob er in die Verarbeitung seiner Daten einwilligt. Ihm darf durch Nicht-Erteilung der Einwilligung oder den späteren Widerruf kein Nachteil entstehen. Die Einwilligung selbst hat grundsätzlich schriftlich oder elektronisch zu erfolgen. Die/der Beschäftigte muss auf die jederzeitige Widerrufbarkeit der Einwilligung hingewiesen werden.

Die Verarbeitung besonderer Kategorien personenbezogener Daten, aus denen etwa die ethnische Herkunft, politische Meinungen, religiöse Überzeugungen, der Gesundheitszustand oder die Gewerkschaftszugehörigkeit hervorgehen, ist gem. § 26 Abs. 3 BDSG zulässig, wenn sie für die Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht erforderlich ist.

Die zuvor genannten Regelungen gelten auch, wenn die Daten nicht in einem Dateisystem gespeichert werden.

Es dürfen immer nur die Daten erhoben und verarbeitet werden, die tatsächlich für die personalwirtschaftlichen Belange notwendig sind (Datenminimierungspflicht). Verlässt also ein Mitarbeiter das Unternehmen, so sind dessen Daten, sofern sie nicht aufgrund gesetzlicher Vorgaben aufzubewahren sind, nachweisbar zu löschen. Solche gesetzlichen Aufbewahrungsfristen finden sich beispielsweise im:

- Arbeitsrecht:
  - § 17 Abs. 1 und Abs. 2 MiLoG, Nachweis über Beginn, Ende und Dauer der täglichen Arbeitszeit bei geringfügig Beschäftigten, 2 Jahre
  - § 27 Abs. 5 MuSchG, Unterlagen über Beschäftigungsart und –zeiten werdender Mütter, 2 Jahre
  - § 50 Abs. 2 JArbSchG, alle relevanten Unterlagen nach dem JArbSchG zwei Jahre für die Aufsichtsbehörde
  - § 11 Abs.2 S. 2 BetrAVG, Unterlagen zur Ermittlung der Bemessung des Beitrags zum Pensionssicherungsverein, 6 Jahre

- Sozialversicherungsrecht:
  - § 28f Abs. 1 SGB IV, Entgeltunterlagen, bis zu 5 Jahren
  - § 165 Abs. 4 SGB VII, Aufzeichnungen über geleistete Arbeitsstunden von Beschäftigten für die gesetzliche Unfallversicherung, 5 Jahre

- Handelsrecht:
  - § 257 Abs. 4 HGB, Handelsbücher, Jahresabschlüsse und Buchungsunterlagen, 10 Jahre; Handelsbriefe, 6 Jahre

- Steuerrecht:
  - § 41 Abs. 1 S. 9 EStG Lohnkonten bis zum Ablauf des 6. KJ
  - § 147 Abs. 3 AO Handelsbücher, Jahresabschlüsse und Buchungsunterlagen sowie Zollunterlagen, zehn Jahre; Handelsbriefe und sonstige für die Besteuerung bedeutende Unterlagen sechs Jahre, sofern keine kürzeren Aufbewahrungsfristen aus anderen Steuergesetzen zugelassen sind
  - § 14b Abs. 1 UStG Rechnungen, 10 Jahre

Die Daten dürfen auch nur so lange gespeichert werden, bis der Zweck der Verarbeitung erfüllt ist. Beispielsweise dürfen Bewerbungsunterlagen von abgelehnten Bewerbern nur maximal sechs Monate aufbewahrt werden. Es sei denn, es liegt eine Einwilligung des Bewerbers vor, diese weiter vorzuhalten, um beispielsweise bei künftigen Ausschreibungen berücksichtigt zu werden (Bewerberpool).

Eine Verwendung von Daten zu einem anderen als dem ursprünglichen und notwendigen Zweck ist unzulässig. Daher darf ein Unternehmen Mitarbeiterdaten auch nicht einfach an einen Dritten weitergeben, wenn die Weitergabe nicht aufgrund einer gesetzlichen Rechtsgrundlage nach Art. 6 DSGVO erfolgt. Hierunter fällt auch die Einwilligung. (Zweckbindung).

Informationspflichten gegenüber den Beschäftigten
Die betroffenen Beschäftigten müssen bereits zum Zeitpunkt der Erhebung der Daten über den Zweck, die Dauer der Speicherung und gegebenenfalls über die Empfänger der Daten informiert werden. Den Beschäftigten müssen ferner Name und die Kontaktdaten des Verantwortlichen für die Datenverarbeitung bzw. dessen Vertreter mitgeteilt werden. Wenn ein Datenschutzbeauftragter erforderlich ist, müssen auch diese Kontaktdaten mitgeteilt werden. Daneben müssen die Beschäftigten über folgende Rechte informiert werden:

- Recht auf Auskunft: Auf Nachfrage muss Beschäftigten eine umfassende Auskunft über die Daten, die von ihnen gespeichert werden, gegeben werden.
- Recht auf Berichtigung: Wurden von dem Beschäftigten falsche Daten erhoben oder sind diese veraltet, so müssen diese korrigiert werden.
- Recht auf fristgemäße Löschung der verarbeiteten Daten: Beschäftigte können verlangen, dass ihre Daten nach Ablauf der Speicherfrist gelöscht werden.
- Recht auf Einschränkung der Verarbeitung: Werden Daten von Beschäftigten über das erforderliche Maß hinaus verarbeitet, können Beschäftigte eine Einschränkung der Verarbeitung fordern.
- Recht auf Datenübertragbarkeit: Der Mitarbeiter hat das Recht, die ihn betreffenden personenbezogenen Daten, die er dem Arbeitgeber bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten

- Recht auf Beschwerde bei der Aufsichtsbehörde: Sind Beschäftigte der Ansicht, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt, können sie sich bei einer Aufsichtsbehörde beschweren.

Wie die Unternehmen den betroffenen Personen die Informationspflichten mitteilen, steht diesen frei. Eine Möglichkeit wäre, auch innerhalb eines Unternehmens für die Beschäftigten eine Datenschutzerklärung aufzusetzen, die die notwendigen Informationen enthält.

Rechenschaftspflicht
Der Arbeitgeber muss gegenüber Anfragenden die Einhaltung der Datenschutzgrundsätze bei der Verarbeitung personenbezogener Daten nachweisen können. Eine entsprechende Datenschutzerklärung, die den Umgang mit personenbezogenen Daten im Unternehmen beschreibt, kann hierbei die Grundlage bilden. Besonderes Augenmerk sollte hierbei auf Datenminimierung und Speicherbegrenzung gelegt werden.

Sicherheit der Datenverarbeitung
Zum Schutz der Daten müssen bei der Verarbeitung geeignete technische und organisatorische Maßnahmen getroffen werden. Beispielsweise passwortgeschützte Zugriffsmöglichkeiten für einen notwendigen Personenkreis oder andere. Pseudonymisierungs-, Anonymisierungs- und Verschlüsselungsverfahren.

Verzeichnis von Verarbeitungstätigkeiten
Werden personenbezogene Daten verarbeitet, müssen diese in eine geeignete Verzeichnisstruktur eingebettet sein (beschränkte Zugriffsmöglichkeit, Datenportabilität).

Meldung von Datenschutzverstößen
Datenschutzverstöße müssen innerhalb von 72 Stunden nach Bekanntwerden der Aufsichtsbehörde gemeldet werden.

Sanktionen
Ein Verstoß gegen die Bestimmungen des Beschäftigtendatenschutzes kann mit einer Geldbuße bis zu 20 Millionen Euro bzw. bis zu 4% des Jahresumsatzes geahndet werden.