DATENSCHUTZ – D10

Stand: Januar 2022

Ihr Ansprechpartner
Ass. iur. Kim Pleines
E-Mail
kim.pleines@saarland.ihk.de
Tel.
(0681) 9520-640
Fax
(0681) 9520-690

Beschäftigtendatenschutz

Unternehmen verarbeiten in der Regel Daten ihrer Arbeitnehmer, um ihre vertraglichen oder gesetzlichen Aufgaben zu erfüllen. Wann dies zulässig ist und welche Vorschriften Arbeitgeber beachten müssen, stellen wir Ihnen nachfolgend dar.

I. Wer ist Beschäftigter nach dem BDSG?

§ 26 Abs. 8 BDSG stellt klar, wer Beschäftigter im Sinne des Datenschutzgesetzes ist. Unter den Begriff fallen u.a. folgende Personen:

1. Arbeitnehmer/innen einschließlich der Leiharbeitnehmer/innen
2. Auszubildende
3. ausgeschiedene Arbeitnehmer/innen
4. Bewerber/innen
5. in anerkannten Werkstätten für behinderte Menschen Beschäftigte und
6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind.

II. Inhalt des § 26 BDSG: Rechtsgrundlagen für den Arbeitgeber

1. Datenverarbeitung zum Zwecke des Beschäftigtenverhältnisses (§ 26 Abs. 1 Satz 1 BDSG)

Nach § 26 Abs. 1 Satz 1 BDSG dürfen personenbezogene Daten von Beschäftigten erhoben werden, wenn dies für die **Begründung**, die **Durchführung** oder die **Beendigung** des Arbeitsverhältnisses erforderlich werden. Dabei dürfen nicht alle Daten erhoben werden, sondern nur solche, die wirklich für das Arbeitsverhältnis erforderlich sind.

Industrie- und Handelskammer des Saarlandes
Postanschrift: IHK Saarland │ 66104 Saarbrücken │ Büroanschrift: Franz-Josef-Röder-Straße 9 │ 66119 Saarbrücken
Tel. 0681/9520-0 │ Fax 0681/9520-888 │ E-Mail: info@saarland.ihk.de │ Internet: www.saarland.ihk.de

Dazu gehören in erster Linie die **Stammdaten,** um die gesetzlichen und vertraglichen Pflichten, die sich etwa aus dem Arbeitsvertrag und den Steuer- oder Sozialgesetzen ergeben, zu erfüllen. Eine Verpflichtung zur Datenerhebung kann sich aber auch aus Tarifvertrag oder einer Betriebsvereinbarung ergeben.

2. Datenverarbeitung zum Zwecke der Aufklärung von Straftaten (§ 26 Abs. 1 Satz 2 BDSG)

Die Daten dürfen zur **Aufdeckung von Straftaten** verarbeitet werden. Voraussetzung ist, dass dokumentierte und tatsächliche Anhaltspunkte den **Verdacht** begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat. Es darf nicht „ins Blaue hinein" ermittelt werden. Es muss immer ein Anfangsverdacht für das Vorliegen einer Straftat bestehen. Die Verarbeitung muss zur Aufdeckung erforderlich und verhältnismäßig sein, d.h. schutzwürdige Interessen des Beschäftigten dürfen nicht überwiegen. Die tatsächlichen Anhaltspunkte hat der Arbeitgeber zu dokumentieren. Unter die Vorschrift fallen **keine präventiven Maßnahmen** - wie etwa die Videoüberwachung von Pausenräumen - zur Verhinderung von Straftaten.

Nicht im Gesetz mit aufgenommen wurde die Datenverarbeitung beim **Verdacht schwerwiegender Pflichtverletzungen.** Eine solche schwerwiegende Pflichtverletzung kann z.B. ein Wettbewerbsverstoß während des laufenden Arbeitsverhältnisses sein. Das BAG hat 2017 (BAG, Urt. v. 29. Juni 2017, 2 AZR 597/16) entschieden, dass eine Datenverarbeitung im Rahmen eines Detektiveinsatzes zulässig ist, wenn die Datenerhebung dazu dient, eine Pflichtverletzung aufzudecken und die Datenverarbeitung verhältnismäßig ist. Auch wenn das Gericht die Regelung aus dem „alten" BDSG angewendet hat, sollte die Rechtsprechung auch auf die Neuregelung übertragbar sein.

3. Datenverarbeitung auf Grundlage einer Einwilligung (§ 26 Abs. 2 BDSG)

Neben dem Arbeitsvertrag kann auch eine Datenverarbeitung aufgrund einer **Einwilligung** erfolgen. Dies betrifft Daten, die nicht aufgrund vertraglicher oder gesetzlicher Rechtsgrundlage erfasst werden.

Erfolgt die Datenverarbeitung aufgrund einer Einwilligung, muss sie nach § 26 Abs. 2 BDSG **freiwillig** eingeholt werden. Die Einwilligung kann **schriftlich oder elektronisch** eingeholt werden, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

➔**D02** „Einwilligung nach der DSGVO", Kennzahl 2356

Arbeitsverhältnisse sind durch eine gewisse Abhängigkeit vom Arbeitgeber gekennzeichnet. Diese Abhängigkeit könnte der Freiwilligkeit entgegenstehen. Aufgrund des Über-/Unterordnungsverhältnisses sind an die **Einwilligung** deshalb hohe Anforderungen zu stellen, falls eine Verarbeitung von Beschäftigtendaten im Einzelfall hierauf gestützt werden soll.

Die **Freiwilligkeit** der Einwilligung wird vermutet, wenn sich für den Arbeitnehmer ein **rechtlicher oder wirtschaftlicher Vorteil** ergibt. In der Praxis wird sie deshalb überwiegend in Konstellationen möglich sein, die nicht das Arbeitsverhältnis als solches, sondern Zusatzleistungen des Arbeitgebers betreffen. Zulässig sollten Einwilligungen im Rahmen der Erlaubnis der Privatnutzung dienstlicher Fahrzeuge, Telefone oder EDV-Geräte sein.

Wichtig: *Falls Sie auf Ihrer Internetseite Bilder Ihrer Mitarbeiter veröffentlichen wollen, brauchen Sie dazu dessen Einwilligung. Denn: Das Abbilden des Mitarbeiters auf Internetseite ist regelmäßig nicht zur Durchführung des Arbeitsverhältnisses erforderlich. Ein Muster für eine Einwilligung finden Sie am Ende dieses Infoblatts.*

4. Verarbeitung besonderer Kategorien von Daten (§ 26 Abs. 3 BDSG)

Die Verarbeitung „sensibler Daten“ im Rahmen des Arbeitsverhältnisses ist zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist. Darunter fallen insbesondere Angaben zur Religionszugehörigkeit oder zum Schwerbehindertengrad. Beruht die Verarbeitung sensibler Daten auf einer Einwilligung, ist Absatz 2 zu beachten.

5. Datenverarbeitung auf Grundlage von Kollektivvereinbarungen (§ 26 Abs. 4 BDSG)

Die DSGVO ermöglicht ausdrücklich eine Datenverarbeitung aufgrund von Kollektivvereinbarungen im Unternehmen. Bisherige Betriebs- oder Dienstvereinbarungen müssen auf ihre Übereinstimmung mit der DSGVO überprüft werden. Dabei müssen insbesondere die **erhöhten Transparenzpflichten nach Art. 13 und 14 DSGVO**, also die Informationspflichten gegenüber den Mitarbeitern als betroffene Person, erfüllt werden (s. unten).

6. Datentransfer im Konzern

Auch im neuen BDSG fehlt eine Regelung zum Datentransfer innerhalb von Konzernen. Eine Übermittlung von Personaldaten innerhalb eines Konzerns z. B. an die Tochter oder an die Konzernmutter, die die gesamte Personalverwaltung durchführt, kann auf den Erlaubnistatbestand des **Art. 6 Abs. 1 lit. f DSGVO** „Wahrung berechtigter Interessen“ gestützt werden. Der Datentransfer ist aber nur zulässig, soweit nicht die Interessen oder Grundrechte und Grundfreiheiten des Beschäftigten überwiegen (Interessenabwägung). Bei der Übermittlung von Daten in Drittstaaten muss zusätzlich geprüft werden, ob ein angemessenes Datenschutzniveau nach den Mechanismen der Art. 44 ff. DSGVO nachgewiesen werden kann.

III. Informationspflichten gegenüber Beschäftigten

Vor der Verarbeitung der Daten muss der Beschäftigte darüber informiert werden,

- wer die Daten erhebt = Kontaktdaten des Arbeitgebers;
- wer Datenschutzbeauftragter ist = Kontaktdaten des Datenschutzbeauftragten, soweit einer bestellt wurde;

  ➔ **D06** „Betrieblicher Datenschutzbeauftragter“, Kennzahl 2356
- zu welchem Zweck und auf welcher Rechtsgrundlage die Daten verarbeitet werden;
- wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht: welche berechtigten Interessen verfolgt werden;
- an wen die Daten übermittelt werden = z.B. Krankenkasse, Steuerberater;
- wie lange die Daten gespeichert werden;
- welche Recht dem Beschäftigten zustehen = Recht auf Auskunft, Recht auf Berichtigung oder Löschung, Recht auf Einschränkung der Verarbeitung; Recht auf Widerspruch, Recht auf Datenübertragbarkeit, Recht auf Beschwerde bei der Aufsichtsbehörde;
- dass er seine gegebene Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann und
- ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben ist und welche möglichen Folgen die Nichtbereitstellung hätte.

Wichtig: *Die Informationen können in einer Kollektivvereinbarung/Betriebsanweisung gegeben werden. Existiert eine solche Vereinbarung nicht, sollten die Angaben in einem Informationsblatt zusammengefasst und dem Mitarbeiter übergeben werden.*

IV. Betroffenenrechte der Beschäftigten: Hinweispflichten des Arbeitgebers

Arbeitgeber müssen ihre Beschäftigten auf deren Rechte hinweisen:

- Recht auf Auskunft, Art. 15,
- Recht auf Berichtigung der Daten, Art. 16,
- Recht auf Löschung von Daten, Art. 17,
- Recht auf Einschränkung der Verarbeitung, Art. 18,
- Recht auf Datenübertragbarkeit, Art. 20.

➔**D05** „Informationspflichten nach der DSGVO“, Kennzahl 2356

Der Arbeitgeber sollte verstärkt mit Auskunftsanfragen rechnen. Um die Personalabteilung nicht über die Maße zu belasten, sollten bereits jetzt Prozesse implementiert werden, um Auskunftsanfragen zügig beantworten zu können. Denn: Die Angaben sind unverzüglich, spätestens innerhalb eines Monats zur Verfügung zu stellen.

Wichtig: *Die Verfahren, bei denen Beschäftigtendaten verarbeitet werden, sind zu dokumentieren =* ***Verzeichnis von Verarbeitungstätigkeiten,*** *Art. 30 DSGVO. Dies gilt nach § 26 Abs. 7 sowohl für Beschäftigtendaten, die in einem Dateisystem gespeichert sind als auch für Daten, die in Papierform verarbeitet werden.*

➔**D11** „Verzeichnis von Verarbeitungstätigkeiten“, Kennzahl 2356

V. Verpflichtung zur Vertraulichkeit und Sensibilisierung der Mitarbeiter

Nach Art. 32 Abs. 4 DSGVO ist das Unternehmen verpflichtet sicherzustellen, dass ihm unterstellte Personen mit Zugang zu personenbezogenen Daten, z. B. die Personalabteilung, die Beschäftigtendaten nur auf Anweisung verarbeiten. Aus diesem Grund ist der **Mitarbeiter zur Vertraulichkeit** zu **verpflichten**.

Die Form dieser Verpflichtungserklärung ist gesetzlich nicht vorgegeben. Aus Nachweisgründen bietet sich die schriftliche oder elektronische Form an. Ein Muster finden Sie auf der letzten Seite.

Die Verpflichtung sollte **am ersten Arbeitstag** vorgenommen werden. Bei Mitarbeitern, die schon länger im Betrieb tätig sind, sollte die Verpflichtung nachgeholt werden. Betriebliche Weisungen können zusätzlich auch in Dienstvereinbarungen festgelegt werden.

Neben der Verpflichtung zur Vertraulichkeit empfiehlt es sich auch, die Mitarbeiter regelmäßig zum Thema Datenschutz zu **schulen** und zu **sensibilisieren**. Dem Mitarbeiter muss klar sein, wie er mit personenbezogenen Daten umgehen soll und wie er z.B. bei Auskunftsanfragen reagieren muss.

VI. Speicherdauer und Aufbewahrungsfristen im Arbeitsverhältnis

Auch im Arbeitsrecht gilt der **Grundsatz der Speicherbegrenzung.** Personenbezogene Daten der Beschäftigten dürfen nur so lange gespeichert werden, wie dies für die Erfüllung einer rechtlichen Verpflichtung erforderlich ist. Sind die Daten nicht mehr erforderlich, sind sie zu löschen.

Aufbewahrungspflichten ergeben sich aus zahlreichen gesetzlichen Regelungen:

- Die Daten sind nicht zu löschen, wenn sie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich sind (Art. 17 Abs. 3 lit. e DSGVO).
- **Bewerberdaten:** sechs Monate ab dem Zeitpunkt der Absage, § 15 Abs. 4 AGG, § 61b Abs. 1 ArbGG.

  Praxistipp: *Wenn Sie die Bewerber-Daten länger aufbewahren möchten, holen Sie die Einwilligung des Bewerbers ein, die Unterlagen beim nächsten Bewerbungslauf zu berücksichtigen.*

- **Dokumentation der Arbeitszeit:** mindestens zwei Jahre (Regelungen in ArbZG, JArbSchG, MiLoG, AentG, MuSchG).
- **Unterlagen über Arbeitsunfälle:** drei Jahre ab bindender Feststellung der Leistungspflicht, § 113 SGB VII.
- **Ansprüche auf regelmäßig wiederkehrende Leistungen der betrieblichen Altersversorgung:** drei Jahre, § 18a S. 2 BetrAVG.
- **Anspruch auf Leistungen der betrieblichen Altersversorgung:** 30 Jahre, § 18a S. 1 BetrAVG.
- **Unterlagen mit steuerrechtlicher Relevanz:** sechs bzw. zehn Jahre, § 257 HGB, §147 AO.
- **Entgelt-Abrechnungsunterlagen:** sechs Jahre, § 28f SGB IV, § 147 AO
- **Lohnkonten:** sechs Jahre, § 41 Abs. 1 S. 9 EStG.

Anlage 1

Einwilligung Mitarbeiterfotos

Wir, [Name des Unternehmens], veröffentlichen auf unserer Internetseite www…...de unsere Mitarbeiter mit Foto, Name, Vorname und Kontaktdaten, um so für unsere Kunden einen ersten persönlichen Eindruck und einen größtmöglichen Service zu leisten.

Für die Veröffentlichung Ihres Fotos und Ihrer Daten benötigen wir eine schriftliche Einwilligung von Ihnen. Wir verwenden Ihr Foto nur zu dem oben genannten Zweck.

Ich, _____(Vorname, Name),

bin damit einverstanden, dass mein Foto für die oben genannten Zweck benutzt und veröffentlicht wird. Soweit sich aus meinem Foto Hinweise auf meine ethnische Herkunft, Religion oder Gesundheit ergeben, bezieht sich meine Einwilligung auch auf diese Angaben. Mir ist bekannt, dass Informationen im Internet weltweit zugänglich sind. Sie können mit Suchmaschinen gefunden und mit anderen Informationen verknüpft werden, woraus sich unter Umständen Persönlichkeitsprofile über mich erstellen lassen. Mir ist auch bekannt, dass ins Internet gestellte Informationen, einschließlich Fotos, problemlos kopiert und weiterverbreitet werden können.

Es steht mir frei, ob ich der Veröffentlichung meiner Fotos zustimme oder nicht. Diese Einwilligung ist freiwillig. Ich kann sie ohne Angabe von Gründen verweigern, ohne dass ich deswegen Nachteile zu befürchten hätte. Die Einwilligung kann jederzeit widerrufen werden. Der Widerruf ist zu richten per Mail an […] oder per Telefon an […]. Mein Foto wird dann unverzüglich aus dem Internetangebot entfernt.

Ort, Datum

Unterschrift

Anlage 2

Verpflichtungserklärung zur Wahrung der Vertraulichkeit bei der Verarbeitung personenbezogener Daten

.....
Name der verantwortlichen Stelle

Sehr geehrte(r) Frau/Herr.....

aufgrund Ihrer Aufgabenstellung verpflichte ich Sie auf die Wahrung der Vertraulichkeit personenbezogener Daten nach Art. 5 Abs. 1 f, Art. 32 Abs. 4 Datenschutz-Grundverordnung (DSGVO), zu denen Sie im Rahmen Ihrer Tätigkeit Zugang erhalten oder Kenntnis erlangen. Es ist Ihnen untersagt, unbefugt personenbezogene Daten zu verarbeiten.

Diese Verpflichtung besteht auch nach Beendigung Ihrer Tätigkeit fort.

Verstöße gegen die Vertraulichkeit können nach Art. 83 Abs. 4 DSGVO, §§ 42, 43 BDSG sowie nach anderen Strafvorschriften mit Freiheits- oder Geldstrafe geahndet werden.

In der Verletzung der Vertraulichkeit kann zugleich eine Verletzung arbeits- oder dienstrechtlicher Schweigepflichten liegen.

Eine unterschriebene Zweitschrift dieses Schreibens reichen Sie bitte an die Personalabteilung zurück.

....
Ort, Datum Unterschrift der verantwortlichen Stelle

*Diese Erklärung kann auf die Wahrung des Fernmeldegeheimnisses nach § 88 TKG (bei Mitwirkung an geschäftsmäßiger Telekommunikation) und allgemein auf die Wahrung von Betriebs- und Geschäftsgeheimnissen sowie Berufsgeheimnissen erweitert werden, Häufig ist die Verschwiegenheitsverpflichtung bei allgemeinen Betriebs- und Geschäftsgeheimnissen bereits im Arbeitsvertrag geregelt.