

Merkblatt

Datenschutzgrundverordnung: Beschäftigtendatenschutz

Ansprechpartner: Referat Recht

Eric Dreuse
Telefon: 0351 2802-194
Fax: 0351 2802-7194
dreuse.eric@dresden.ihk.de

Stand: 2021

Hinweis:

Das Merkblatt wurde sorgfältig erstellt. Dessen ungeachtet können wir keine Gewähr übernehmen und schließen deshalb jede Haftung im Zusammenhang mit der Nutzung des Merkblattes aus. Eventuelle Verweise und Links stellen keine Empfehlung der Kammer dar.

Datenschutzgrundverordnung - Beschäftigtendatenschutz

Vorbemerkungen

Die EU-Datenschutz-Grundverordnung (DSGVO) trifft keine inhaltlichen Regelungen zum Datenschutz im Beschäftigungsverhältnis, sondern überlässt es dem nationalen Gesetzgeber, hierzu Vorschriften zu erlassen. Der deutsche Gesetzgeber hat das innerhalb der Änderung des Bundesdatenschutzgesetzes (BDSG) mit § 26 getan. Dieser lehnt sich weitgehend an den § 32 des noch geltenden BDSG an.

I. Rechtsgrundlagen

Die Geltung der Vorschriften der DSGVO und des BDSG setzt keine IT-gestützte Verarbeitung von Personaldaten voraus; sie gelten auch für in Papierform geführte Personalakten, § 26 Abs. 7 BDSG.

Die Datenverarbeitung ist zulässig, wenn sie zur Entscheidung über die Begründung eines Beschäftigungsverhältnisses (z. B. Bewerberdaten), für seine Durchführung oder Beendigung erforderlich ist. Dazu gehören Pflichten, die sich aus Gesetzen (z. B. Steuer- oder Sozialgesetze), aus Tarifverträgen sowie Betriebs- oder Dienstvereinbarungen ergeben.

Die Verarbeitung besonderer Kategorien von Daten (z. B. Religionszugehörigkeit, Gesundheitsdaten) ist nach der DSGVO nach Art. 9 Abs. 2 Buchstabe b), § 26 Abs. 3 BDSG zulässig.

II. Wer ist Beschäftigter?

Nach § 26 Abs. 8 BDSG umfasst der Begriff auch LeiharbeiterInnen sowie BewerberInnen und ausgeschiedene ArbeitnehmerInnen.

III. Einwilligung

Falls der Arbeitgeber für die Datenverarbeitung eine Einwilligung des Beschäftigten benötigt, muss sie nach § 26 Abs. 2 BDSG in Schriftform eingeholt werden. Die Freiwilligkeit der Einwilligung wird vermutet, wenn sich für den Arbeitnehmer ein rechtlicher oder wirtschaftlicher Vorteil ergibt (z. B. betriebliche Altersversorgung). Der Beschäftigte ist dabei auf die jederzeitige Widerrufsmöglichkeit seiner Einwilligung hinzuweisen. Insofern muss jedes Unternehmen überprüfen, ob bisherige Einwilligungen, die von den Beschäftigten eingeholt wurden, noch gültig sind. Die Anforderungen ergeben sich aus Art. 7 DSGVO. Fehlt es also an dem Hinweis auf das jederzeitige Widerrufsrecht und an der Darstellung des Zwecks der mit der Einwilligung verfolgten Datenverarbeitung, bestehen berechnete Zweifel an der Gültigkeit der alten Einwilligungen nach dem 25.05.2018.

Nach Art. 22 Abs. 2 Buchstabe c) DSGVO bedarf eine automatisierte Entscheidung z. B. in Fällen elektronischer Scoring-Verfahren im Personalbereich einer ausdrücklichen Einwilligung der Beschäftigten.

Die Einwilligungen z. B. zur Verwendung eines Fotos des Beschäftigten im Internet oder zur privaten Nutzung von E-Mail und Internet mit Überprüfungsrecht des Arbeitgebers sollten auf vom Arbeitsvertrag getrennten Dokumenten eingeholt werden, weil sonst bei jedem neuen Einwilligungserfordernis der Arbeitsvertrag geändert werden müsste.

IV. Kollektivvereinbarungen

Bisherige Betriebs- oder Dienstvereinbarungen müssen ebenfalls auf ihre Übereinstimmung mit der DSGVO überprüft werden. Dabei geht es insbesondere um die erhöhten Transparenzpflichten nach Art. 13 und 14 DSGVO, also die Informationspflichten gegenüber der betroffenen Person, hier den Beschäftigten. Die Informationspflichten betreffen insbesondere den genauen Datenkranz, der verarbeitet wird, die Zwecke sowie die Angaben, an wen die Daten übermittelt werden. Davon umfasst ist auch der Hinweis auf etwaige Übermittlungen in Drittstaaten. Die Beschäftigten müssen auch über ihre Rechte nach Art. 12 DSGVO informiert werden:

- Auskunftsrecht, 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.

V. Datentransfer im Konzern

Als Rechtsgrundlage für eine Übermittlung von Personaldaten innerhalb eines Konzerns z. B. an die Tochter oder an die Konzernmutter, die die gesamte Personalverwaltung durchführt, kann auf Art. 6 Abs. 1 Buchstabe f) gestützt werden, wenn die Erforderlichkeit für den Transfer dargelegt werden kann. Damit wäre auch eine Übermittlung von Daten in Drittstaaten zulässig, wenn das angemessene Datenschutzniveau nach den Mechanismen der Art. 44 ff. DSGVO nachgewiesen werden kann.

VI. Datenschutz-Folgenabschätzung

Da zur Erfüllung z. B. der Verpflichtung zur Abführung der Kirchensteuer die Religionszugehörigkeit erfasst werden muss, muss für die Verarbeitung der Personalstammdaten eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO durchgeführt werden. Das gilt auch wegen der Verarbeitung von Gesundheitsdaten (z. B. Krankmeldungen, betriebliches Wiedereingliederungsmanagement) oder automatisierte Personalentscheidungen.

VII. Prüfschema für Betriebsvereinbarungen

1. Anforderungen nach DSGVO

Für Betroffene muss klar erkennbar sein, welche sie betreffenden personenbezogene Daten verarbeitet bzw. in welchem Umfang personenbezogene Daten gegenwärtig oder künftig verarbeitet werden, insbesondere muss deutlich werden:

- die Identität des Verantwortlichen
- die Zwecke der Verarbeitung
- die Informationen, die eine faire und transparente Verarbeitung gewährleisten
- das Recht, eine Bestätigung und Auskunft darüber zu erhalten, welche personenbezogene Daten verarbeitet werden
- die Aufklärung über Risiken, Rechte, Garantien hinsichtlich der Datenverarbeitung
- die Aufklärung darüber, wie Rechte geltend gemacht werden können.

Außerdem müssen die Grundsätze nach Art. 5 DSGVO ihren Niederschlag finden.

Die Verarbeitung muss auf rechtmäßige Weise, nach Treu und Glauben in einer nachvollziehbaren Weise nur für einen festgelegten zu einem eindeutigen und legitimen Zweck erfolgen.

Dies galt auch schon nach bisherigem Recht.

Neu: Die DSGVO erfordert darüber hinaus angemessene und besondere Maßnahmen im Hinblick auf die Transparenz der Verarbeitung oder über eingesetzte Arbeitsmittel.

Zu beachten:

- die Identifizierung des Arbeitnehmers darf nur so lange möglich sein, wie es für den Zweck der Verarbeitung erforderlich ist,
- die Speicherfristen sind auf das unbedingt erforderliche Mindestmaß beschränken.

2. Prüfschema für bestehende Betriebsvereinbarungen

a) Werden auf Grundlage der Betriebsvereinbarung personenbezogene Daten verarbeitet?

b) Enthält die Betriebsvereinbarung Angaben zu den Grundprinzipien nach Art. 5 DSGVO?

aa) Rechtmäßigkeit (= Erlaubnistatbestände vorhanden?)

Verarbeitung rechtmäßig, nach Treu und Glauben und in nachvollziehbarer Weise? vgl. Art. 6 I a-f DSGVO, EG 39 und Art. 12 ff. DSGVO

bb) Zweckbindungsgrundsatz

Zweck deutlich vereinbart (konkret & detailliert)?

Falls Verarbeitung zu anderem Zweck erfolgt: Vereinbarkeit mit altem Zweck?

cc) Datenminimierung

Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke erforderliche Maß beschränkt?

Sind Strategien und Maßnahmen getroffen (Pseudonymisierung, techn. Vorrichtungen)?

- dd) Datenrichtigkeit
Wurden Maßnahmen getroffen, um zu gewährleisten, dass personenbezogene Daten, die hinsichtlich des Zwecks ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden?
Dienstvereinbarung sollte Regelungen zu Korrekturprozessen enthalten.
- ee) Speicherbegrenzung
Sind klare Regelungen zu Speicherdauer von personenbezogenen Daten in Dienstvereinbarung getroffen?
- ff) Integrität und Vertraulichkeit
Sind technisch-organisatorischen Maßnahmen vorhanden, um den Schutz vor unbefugter, unrechtmäßiger Verarbeitung sowie vor Schädigung, Zerstörung oder Verlust zu gewährleisten?
Ist die Verarbeitung besonderer Datenkategorien (z. B. Religionszugehörigkeit, Gesundheitsdaten, biometrische Daten) ausreichend gesichert?

3. Werden besondere Kategorien personenbezogener Daten verarbeitet?

Dann Art. 9 DSGVO beachten. Besonders relevant bei: Zutrittssystemen mit biometrischer Datenverarbeitung, Einsatz von elektronischen Personalakten, Ausgestaltung des BEM, Durchführung von Assessmentcentern mit elektronischer Datenverarbeitung der Bewerberdaten.

4. Sind Maßnahmen getroffen worden, um die Informationspflichten zu erfüllen?

Der Arbeitgeber muss Angaben machen zu: Name des Verantwortlichen, seines Vertreters, des betrieblichen Datenschutzbeauftragten, den Zweck sowie die Rechtsgrundlage der Verarbeitung, Speicherfristen, Betroffenenrechte, Empfänger der Daten, Beschwerderechte und Rechtsbehelfe, Datenverarbeitung im Drittland.

5. Sind Maßnahmen getroffen worden, um die Betroffenenrechte zu berücksichtigen?

Sind die Angaben zu den Betroffenenrechten nach Art. 15 sowie Mitteilungen nach Art. 16 ff. DSGVO enthalten?

Die umfangreichen Angaben sollten als Anhang zum Arbeitsvertrag oder in der Betriebsvereinbarung abgebildet werden.

Praxistipp:

Eine Alternative zur Änderung aller Betriebsvereinbarungen könnte der Abschluss einer „Dach“-Betriebsvereinbarung sein, in der ausschließlich datenschutzrechtliche Aspekte geregelt werden und die Bezug nimmt auf die speziellen Vereinbarungen z. B. zur Arbeitszeit usw. Zumindest könnte aber eine schriftliche allgemeine Information der Beschäftigten darüber erfolgen, welche Daten für welche Zwecke in dem Unternehmen verarbeitet werden.