



DATENSCHUTZ IM BETRIEBSRATSBÜRO

Whitepaper

Rechtliche Grundlagen
Organisatorische Anforderung
Umgang und Aufbewahrung

AdOrga Solutions

Regina Mühlich
consulting@adorgasolutions.de

Inhalt

1	Rechtliche Grundlagen	2
2	Organisatorische Anforderungen	2
3	Grundsätze für den Umgang mit Mitarbeiterdaten	3
4	Aufbewahrung von Unterlagen (Speicherung)	4
5	Links	4

* Hinweis: Der Übersichtlichkeit wegen werden im Folgenden nur die männlichen Formen verwendet.

© Copyright 2016 Regina Mühlich, AdOrga Solutions | E-Mail: consulting@adogasolutions.de

Dieses Dokument ist auf dem Stand des ersten Tages der Veröffentlichung und kann von Regina Mühlich jederzeit geändert werden.

Die Informationen in diesem Dokument sind ohne jegliche Garantie, ausdrücklich oder implizit, einschließlich ohne Gewährleistung der Eignung für einen bestimmten Zweck.

1 Rechtliche Grundlagen

Der Betriebsrat ist ein von den Beschäftigten gewähltes, unabhängiges Vertretungsorgan. Er repräsentiert die Beschäftigten, ist nicht weisungsgebunden. Der Betriebsrat handelt im eigenen Namen und in eigener Verantwortlichkeit.

Seine Aufgaben nimmt der Betriebsrat nach den Vorschriften des Betriebsverfassungsgesetzes (BetrVG) wahr. Jedes Betriebsratsmitglied hat das sich aus Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG ergebende Recht auf informationelle Selbstbestimmung der durch ihn vertretenen Beschäftigten sowie ihr Grundrecht auf Datenschutz gemäß Bundesdatenschutzgesetz (BDSG) zu achten und zu schützen.

Diese Verpflichtung obliegt dem Betriebsrat zunächst bei der Wahrnehmung der ihm nach § 80 Abs. 1 BetrVG zugewiesenen Aufgaben. Er hat unter anderem darüber zu wachen, dass die zugunsten der Arbeitnehmer geltenden Datenschutzregelungen durchgeführt werden. Der Schutz des Rechts auf freie Entfaltung der Persönlichkeit ist außerdem in § 75 Abs. 2. BetrVG geregelt.

Der Betriebsrat hat in eigener Verantwortung adäquate Datenschutzvorkehrungen zu treffen.

Hier sind besonders die vom Betriebsrat bei seiner Aufgabenwahrnehmung zu berücksichtigenden technischen und organisatorischen Maßnahmen nach § 9 BDSG gemeint. Diese Verpflichtung ist z. B. verletzt, wenn der Betriebsrat duldet, dass Mitglieder private Mobile Devices für die Betriebsrats-tätigkeiten nutzen.

Vom Betriebsrat sind bei seiner Tätigkeit insbesondere die Vorschriften des Bundesdatenschutzgesetzes (BDSG) zu beachten und hier insbesondere die darin verankerten **Grundsätze der Erforderlichkeit, der Zweckbindung, der Datenvermeidung, der Datensparsamkeit und des Transparenzprinzips**. Gemäß dem Grundsatz der Datenvermeidung (§ 3a BDSG) sind z. B. Sitzungsprotokolle (Sitzungsniederschrift gemäß § 34 BetrVG) so zu verfassen, das nicht mehr personenbezogene Daten im Protokoll enthalten sind wie unbedingt erforderlich.

2 Organisatorische Anforderungen

Der Betriebsrat hat beim Umgang mit personenbezogenen (mitarbeiterbezogenen) Daten folgende organisatorische Anforderungen einzuhalten:

- 2.1 Dem Betriebsrat muss ein **separater Büroraum** für seine Tätigkeit zur Verfügung stehen. Zu diesem Raum dürfen nur Betriebsratsmitglieder freien Zugang haben. Dieser Raum ist mit einem speziellen Schloss zu sperren. Der Betriebsrat regelt, wer den Schlüssel hat. Die vom Betriebsrat genutzten Räume sollten nur in Anwesenheit eines Betriebsratsmitgliedes gereinigt werden.
- 2.2 **Unterlagen** mit personenbezogenen (mitarbeiterbezogenen) Daten sind in verschließbaren Behältnissen **aufzubewahren**. Für die Schlüssel ist hier ebenfalls eine Aufbewahrungsregelung zu treffen.
- 2.3 Für die **Vernichtung von Unterlagen** mit personenbezogenen (mitarbeiterbezogenen) Daten, die für die Aufgabenerfüllung nicht mehr erforderlich sind, sollte ein Aktenvernichter und/oder eine

Datentonne in den Räumlichkeiten des Betriebsrates bereitstehen. Die Unterlagen sind in jedem Falle datenschutzkonform zu vernichten.

- 2.4 Bei der **Nutzung von Telefon** (auch Mobilfunkgeräte) und Telefaxgeräten ist darauf zu achten, dass bei den Geräten die Verbindungsdaten nur im datenschutzrechtlich zulässigen Umfang verarbeitet werden.
- 2.5 Für den vom Betriebsrat **genutzten Rechner** (Notebook, Desktop) sind entsprechende technische Vorkehrungen, wie z. B. Firewall, zu treffen. Es muss technisch ausgeschlossen sein (u. a. Zutritts-, Zugriffs-, Zugangskontrolle), dass sich Unbefugte auf die Daten des Betriebsrates Zugriff verschaffen. CD-Laufwerke, Brenner, USB, etc. sind aus Datensicherheitsgründen zu sperren. Aus datenschutzrechtlichen Gründen dürfen private Rechner nicht für die Betriebsratstätigkeit genutzt werden.

3 Grundsätze für den Umgang mit Mitarbeiterdaten

Im Rahmen seiner Tätigkeiten, Aufgaben und (Mitbestimmungs-)Rechte gemäß dem Betriebsverfassungsgesetz wie u. a.

- **soziale Angelegenheiten** (§ 87 Abs. 1 BetrVG),
- **Änderungen der Arbeitsplätze**, der Arbeitsabläufe oder der Arbeitsumgebung, die den gesicherten arbeitswissenschaftlichen Erkenntnissen über die menschengerechte Gestaltung der Arbeit offensichtlich widersprechen und die betroffenen Arbeitnehmer in besonderer Weise belastet werden (§ 91 BetrVG),
- die Einführung und Verwendung von **Personalfragebögen, Beurteilungsgrundsätzen** sowie von persönlichen Angaben in **Formulararbeitsverträgen** (§ 94 BetrVG),
- die Erstellung von **personellen Auswahlrichtlinien** (§ 95 Abs. 1 BetrVG),
- die Einführung von Maßnahmen der **betrieblichen Berufsbildung** aus Anlass der Planung technischer Anlagen, von Arbeitsverfahren und Arbeitsabläufen oder Arbeitsplätzen (§ 97 Abs. 2 BetrVG) sowie sonstigen Maßnahmen der betrieblichen Berufsbildung (§ 98 BetrVG) sowie
- Mitbestimmung bei personellen Einzelmaßnahmen

hat der Betriebsrat regelmäßig Einblick in Unterlagen, die Daten mit Personenbezug enthalten. Dies sind vor allem Unterlagen

- zur Erfüllung der Unterrichtsverpflichtung seitens Arbeitgeber,
- über Einstellungsverfahren informiert und entsprechend beteiligt
- mit denen der Betriebsrat sein Recht zur Einsichtnahme in listenmäßig aufgeführte Personaldaten wahrnimmt

Insbesondere in diesem Zusammenhang sind entsprechende Regelungen zu treffen und datenschutzrechtliche Anforderungen zu beachten.

4 Aufbewahrung von Unterlagen (Speicherung)

- 4.1 Die **Aufbewahrung von Unterlagen mit Beschäftigtendaten**, die dem Betriebsrat anlässlich seiner Beteiligung an einer bestimmten Maßnahme vom Arbeitgeber erhält, stellt eine Speicherung von personenbezogenen Daten i. S. des § 32 BDSG. Die Speicherung ist gesetzlich nur solange erlaubt, wie der Betriebsrat die Daten den Beschäftigten für die Aufgabe benötigt (§ 31 BDSG). Das bedeutet, dass die Unterlagen, wenn Sie nicht mehr erforderlich sind, zu löschen sind.
- 4.2 **Sonstige Unterlagen**, die personenbezogene Daten enthalten, hierzu zählen z. B. Sitzungsprotokolle und Niederschriften, sind für die Dauer der Amtszeit des Betriebsrats im Betriebsratsbüro aufzubewahren und spätestens nach Ablauf einer weiteren Amtszeit zu löschen (zu vernichten).
- 4.3 **Einladungen mit Tagesordnungen** sind am Ende der Sitzung von den Teilnehmern zu vernichten oder, am besten, zurückzugeben. Ein entsprechender Hinweis sollte auf der Einladung erfolgen. Vom Betriebsrat in Datenverarbeitungssystemen gespeicherte Daten sind regelmäßig auf ihre weitere Erforderlichkeit zu prüfen (Zweckbindung).

5 Links

Bundesdatenschutzgesetz <https://dejure.org/gesetze/BDSG>
Betriebsverfassungsgesetz <https://dejure.org/gesetze/BetrVG>

§ 31 BDSG besondere Zweckbindung <https://dejure.org/gesetze/BDSG/31.html>

§ 32 BDSG Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses
<https://dejure.org/gesetze/BDSG/32.html>

§ 75 BetrVG Grundsätze für die Behandlung der Betriebsangehörigen
<https://dejure.org/gesetze/BetrVG/75.html>

§ 87 BetrVG Mitbestimmungsrechte <https://dejure.org/gesetze/BetrVG/87.html>

§ 91 BetrVG Mitbestimmungsrechte <https://dejure.org/gesetze/BetrVG/91.html>