

HANDBUCH

BR-DMS.



Dokumentenmanagement für Betriebsräte –
Bedienung, Administration und Technik

Version	1.3.1
Stand	Oktober 2026
Autor	Tim van der Hoven
Kontakt	support@vanderhoven.eu
Lizenz	Open Source · GNU AGPL v3.0

Inhalt

TEIL I – ARBEITEN MIT BR-DMS

1 Einführung	5
1.1 Was ist BR-DMS?	5
1.2 Anmelden	5
1.3 Die Oberfläche	6
1.4 Rollen auf einen Blick	7
2 Dashboard	8
3 Dokumente & Fristen	9
3.1 Eingang	9
3.2 Dokumentenarchiv	10
3.3 Fristen & Fristenkalender	14
3.4 Anhörung als Vorgang (§ 99 / § 102)	15
4 Sitzungen	18
4.1 Der Lebenszyklus einer Sitzung	18
4.2 Sitzung vorbereiten	18
4.3 Sitzung durchführen und protokollieren	20
4.4 Protokoll finalisieren	21
4.5 Beschlussregister	23
4.6 Konstituierende Sitzung und Betriebsversammlung	23
4.7 Gremien und Fremdprotokolle	25
5 Planung & Zusammenarbeit	27
5.1 Aufgaben und Vorhaben	27
5.2 Themen-Backlog	28
5.3 Nachrichten	29
5.4 Kummerkasten	29
5.5 Wahlen (Betriebsrat und JAV)	31
5.6 Kosten des Betriebsrats (§ 40)	34
6 Wissen & Recherche	36
6.1 Wissensarchiv	36
6.2 Ressourcen	36
6.3 Themensammlung	37
6.4 Globale Suche und Gesetzestexte	37
7 Personal	39
7.1 Mitarbeiter	39
7.2 Eingruppierung	40
7.3 Zeitmodelle und Überstunden	42
7.4 Betriebsvereinbarungen	43
7.5 Geschäftsordnung	43
7.6 Schulungen und Qualifikationsmatrix	44
8 Abläufe in der Praxis	45
8.1 Vom Dokument zum Protokoll	45
8.2 Daily Business	46

TEIL II – ADMINISTRATION

9 Einstellungen	48
9.1 Benutzer und Gremium	48
9.2 Zugriff des Admins auf Inhalte	49
9.3 Design	50
9.4 Module	50
9.5 Löschrufen und Erinnerungsmails	51
9.6 Protokoll-Layout	52
9.7 System	53
9.8 Gesetzestexte	54
9.9 Amtsübergabe	55
9.10 Audit-Log	56
10 Rollen & Berechtigungen	57

TEIL III – TECHNIK

11 Architektur & Sicherheit	60
11.1 Aufbau	60
11.2 Sicherheit	60
11.3 Den Server (NAS) absichern	62
12 Installation	66
12.1 Voraussetzungen	66
12.2 Schritt für Schritt	66
12.3 Der Installationsassistent – Frage für Frage	67
12.4 HTTPS-Zertifikat	68
12.5 Die .env von Hand	69
12.6 Watch-Folder	70
12.7 Wenn etwas nicht klappt	70
12.8 Datei-Links im Editor (Windows)	71
13 Betrieb	73
13.1 Updates einspielen	73
13.2 Backup und Wiederherstellung	75
13.3 Demo-Instanz	76
13.4 Demo auf dem Server – das Gremium ausprobieren lassen	77
14 Datenbank	80
14.1 Wichtige Statuswerte	80

AUTOR, LIZENZ & SUPPORT

TEIL I



Arbeiten mit BR-DMS

Alle Funktionen aus Sicht der Betriebsratsmitglieder – vom Dokumenteingang über Sitzungen und Beschlüsse bis zur Personalverwaltung. Die Abbildungen zeigen die Demo-Instanz mit erfundenen Beispieldaten.

KAPITEL 1

Einführung

1.1 Was ist BR-DMS?

BR-DMS ist ein Dokumentenmanagementsystem speziell für Betriebsräte. Es bündelt Sitzungen, Protokolle, Beschlüsse, Fristen und vertrauliche Dokumente in einem System, das vollständig im eigenen Intranet läuft – auf einer NAS, einem eigenen Server oder einer virtuellen Maschine. Eine Cloud-Verbindung ist nicht nötig.

Das System begleitet ein Betriebsratsdokument über seinen ganzen Lebenszyklus: vom Eingang über Kategorisierung und Fristüberwachung, die Behandlung in der Sitzung bis zum rechtssicheren Protokoll – und am Ende die geregelte Löschung nach Ablauf der Aufbewahrungsfrist.

- **Sicher** – Alle Dokumente AES-256-verschlüsselt, Zugriff nach Rollen, lückenloser Audit-Trail
- **Rechtssicher** – Fristen nach § 87, § 99 und § 102 BetrVG, unveränderliche Protokolle mit Zeitstempel
- **Vollständig** – Sitzungen, Beschlussregister, Aufgaben, Wissensarchiv, Personal- und Schulungsverwaltung
- **Anpassbar** – Optionale Module ein- und ausschaltbar, eigenes Logo, eigene Farben
- **Unabhängig** – 100 % self-hosted, keine externen Dienste, Open Source

1.2 Anmelden

BR-DMS wird im Browser geöffnet, z. B. unter <https://<Server>:8443>. Angemeldet wird mit E-Mail-Adresse oder nur dem Teil vor dem @ als Benutzername, dazu das Passwort. „Eingeloggt bleiben“ hält die Anmeldung 24 Stunden, ohne Haken eine Stunde. Nach längerer Inaktivität meldet das System automatisch ab (einstellbar).

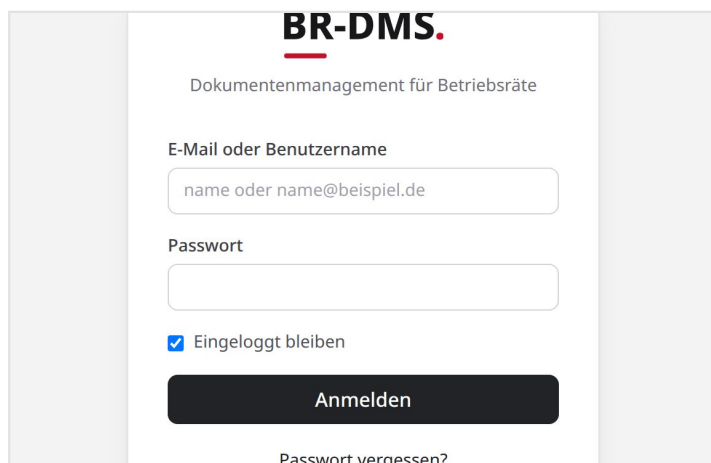


Abb. 1: Anmeldeseite

Passwort vergessen?

Wer sein Passwort vergessen hat, kann über „Passwort vergessen?“ einen Link per E-Mail anfordern. Alternativ setzen Vorsitz oder Admin das Passwort in der Benutzerverwaltung zurück.

Ist die Zwei-Faktor-Anmeldung eingeschaltet (Kapitel 9.7) und für Ihr Konto eingerichtet, fragt BR-DMS

nach dem Passwort zusätzlich nach dem 6-stelligen Code aus Ihrer Authenticator-App. Ohne Handy hilft einer der Wiederherstellungscodes („Handy nicht zur Hand?“). Ist sie für Ihre Rolle Pflicht und noch nicht eingerichtet, führt die Anmeldung einmalig durch die Einrichtung.

Mein Konto

Ein Klick auf Ihren Namen oben in der Seitenleiste öffnet „Mein Konto“ – alles zum eigenen Zugang an einer Stelle, für jede Rolle:

- **Profil** – Name, Rolle, Anmelde-E-Mail und die Adresse für Einladungen. Die Einladungsadresse ändern Sie direkt; die Anmelde-E-Mail nur mit Ihrem Passwort, und die alte Adresse bekommt einen Hinweis
- **Passwort ändern** – alle anderen Sitzungen enden dabei
- **Überall sonst abmelden** – etwa wenn Sie an einem fremden Rechner angemeldet geblieben sind
- **Zwei-Faktor-Anmeldung** – einrichten, neue Wiederherstellungscodes erzeugen oder abschalten (nicht, wenn sie für Ihre Rolle Pflicht ist)
- **Letzte Anmeldungen** – Zeitpunkt, Browser und IP-Adresse; eine fremde Anmeldung fällt so auf

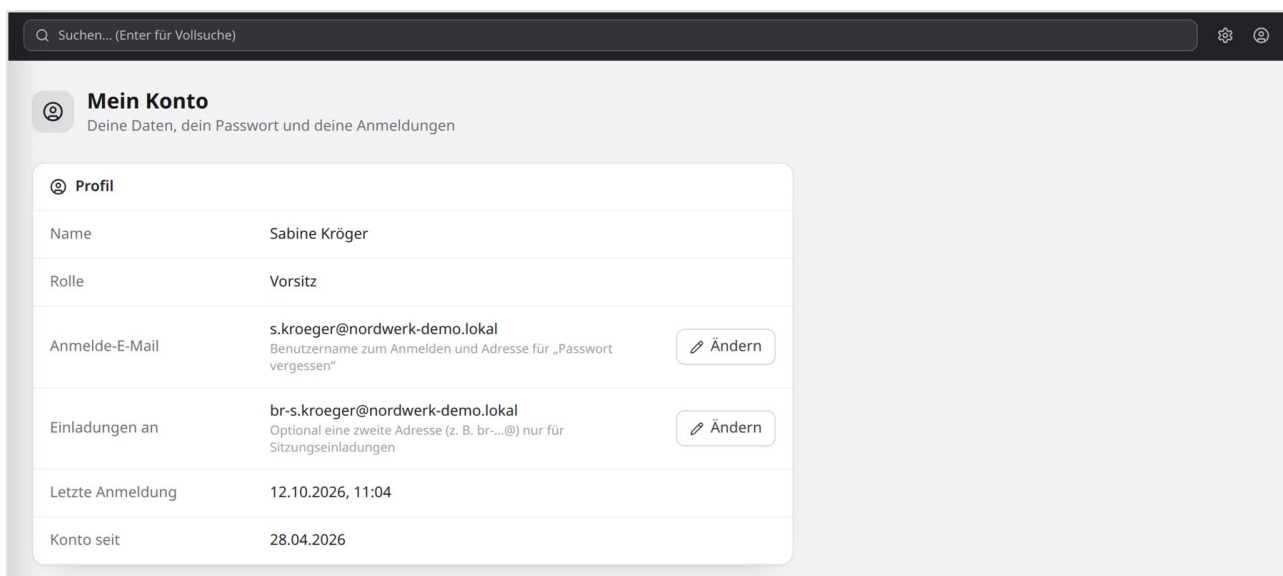


Abb. 2: Mein Konto (Klick auf den eigenen Namen)

1.3 Die Oberfläche

Links befindet sich die Seitenleiste mit allen Bereichen, thematisch gruppiert (Postfach, Sitzungen, Dokumente & Wissen, Planung, Personal, Verwaltung). Jede Gruppe hat zur schnelleren Orientierung einen eigenen farbigen Rand; die Gruppen lassen sich auf- und zuklappen, das merkt sich der Browser. Oben in der Leiste steht Ihr Name. Der Kopfbalken über dem Inhalt enthält die Schnellsuche, das Zahnrad für die Einstellungen und rechts daneben „Abmelden“. Zahlen an den Einträgen zeigen Ungelesenes oder Offenes an.

- **Schnellsuche** – Ab zwei Zeichen erscheinen Treffer aus allen Bereichen; Enter öffnet die ausführliche Suche
- **Benachrichtigungen** – Neue Dokumente, Nachrichten und Aufgaben werden als Hinweis eingeblendet
- **Über BR-DMS** – Ganz unten in der Seitenleiste: Version, Lizenz, Support-Kontakt und „Fehler melden“

1.4 Rollen auf einen Blick

Rolle	Für wen	Kurz gesagt
Vorsitz	Vorsitzende/r	Alles – inkl. Sitzungen fixieren und finalisieren, Benutzer verwalten
Stellvertretung	Stellv. Vorsitzende/r	Wie Vorsitz im Tagesgeschäft
Mitglied	Ordentliche Mitglieder	Dokumente, TOPs, Aufgaben, Personal; keine vertraulichen Dokumente anderer
Ersatzmitglied	Nachrückende	Lesend; bei aktiver Vertretung wie ein Mitglied
JAV	Jugend- und Auszubildendenvertretung	Nur Lesezugriff auf Sitzungen, vertrauliche TOPs ausgeblendet
SBV	Schwerbehindertenvertretung (§ 178 SGB IX)	Wie JAV: nur Sitzungen und Protokolle lesen, ohne vertrauliche TOPs
Admin	Technische Betreuung	Alle Rechte inkl. Module – aber kein Sitzungsmitglied; auf Wunsch ohne Zugriff auf Inhalte (Kapitel 9.2)

Die vollständige Berechtigungsmatrix steht in Kapitel 10.

KAPITEL 2

Dashboard

Das Dashboard ist die Startseite nach dem Login und zeigt nur, was im Alltag zählt: die wichtigsten Punkte auf einen Blick, die eigenen und die übrigen Aufgaben und die nahen Fristen.

Abb. 3: Dashboard: Auf einen Blick, Aufgaben und Fristen

- **Kopfzeile** – Begrüßung und die Zahl ungelesener Dokumente im Eingang
- **Auf einen Blick** – Vier Karten mit farbigem Rand (grün = in Ordnung, gelb = Handlungsbedarf): nächste Sitzung mit Uhrzeit, Ort und Zahl der TOPs; Betriebsvereinbarungen, die in den nächsten 90 Tagen auslaufen oder gekündigt sind; Qualifikationen, die abgelaufen sind oder in 90 Tagen ablaufen, samt nächstem Schulungstermin; Geschlechterquote nach § 15 Abs. 2 BetrVG (Sitze des Minderheitengeschlechts gegen die Mindestsitze aus der Benutzerverwaltung). Ein Klick führt zur jeweiligen Seite; Karten abgeschalteter Module und eine nicht eingetragene Quote werden ausgeblendet
- **Aufgaben** – Oben „Für mich“: alle Ihnen zugewiesenen Aufgaben, nach Fälligkeit sortiert, mit dem Kreis links direkt abhaken. Darunter „Alle anderen“: die Aufgaben der übrigen Mitglieder mit Namen davor; Aufgaben ohne Zuständigkeit stehen dort als „nicht zugewiesen“
- **Fristen** – Kompakt eine Zeile je Frist: überfällige und die der nächsten 14 Tage (höchstens sechs), Resttage farbig (rot ≤ 3 Tage, gelb ≤ 7 Tage); das Häkchen erledigt eine Frist, der Link führt in den Fristenkalender
- **Hinweise** – Erscheinen nur bei Bedarf: Dokumente, die in den nächsten 30 Tagen automatisch gelöscht werden, und fehlerhafte Watch-Folder-Dateien der letzten 7 Tage. Das vollständige Importprotokoll des Watch-Folders steht unter Einstellungen → System

KAPITEL 3

Dokumente & Fristen

3.1 Eingang

Neu eingegangene Dokumente landen zuerst im Eingang – egal ob per Upload oder automatisch über den Watch-Folder (Scanner- oder Netzwerkordner). Hier entscheidet der Vorsitz, was mit jedem Dokument passiert. Ungelesene Einträge sind hervorgehoben.

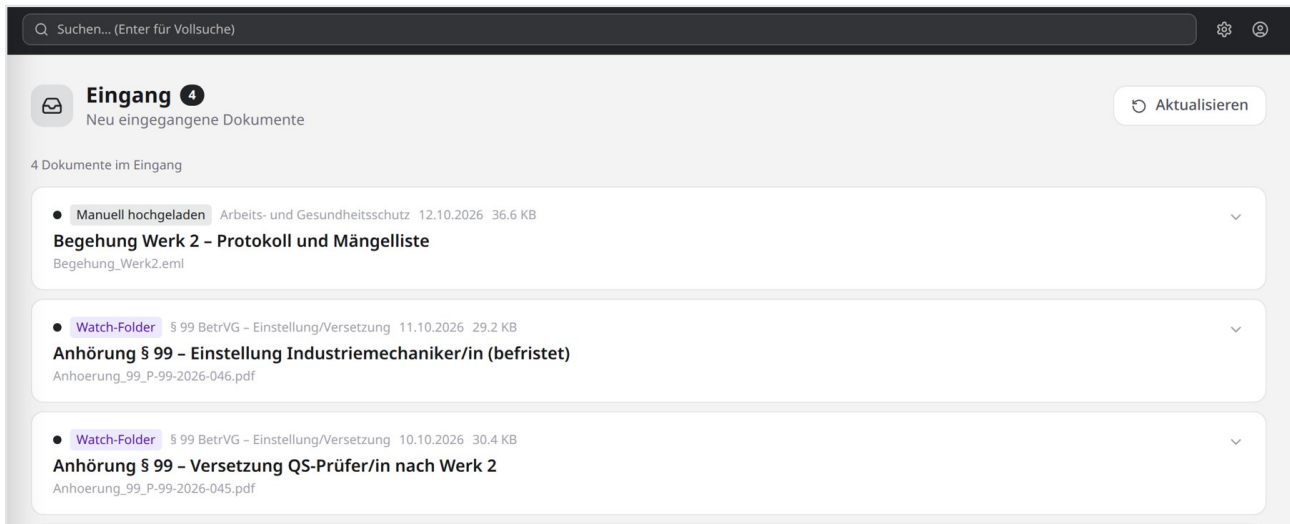


Abb. 4: Eingang mit ungelesenen Anhörungen und Quelle (Watch-Folder / Upload)

Aktionen im Eingang

- **Mit Sitzung verknüpfen** – Einem bestehenden TOP zuordnen oder direkt einen neuen TOP anlegen, auf Wunsch mit Frist
- **Aufgabe erstellen** – Bearbeitung an ein Mitglied übergeben, das Dokument bleibt verknüpft
- **Ins Wissensarchiv** – Inhalt als Wissensseintrag übernehmen
- **Neue Version** – Als neue Fassung eines vorhandenen Dokuments speichern
- **Wiedervorlage** – Datum setzen, an dem das Dokument erneut im Eingang auftaucht
- **Anhörungen** – Stellungnahme, Widerspruch oder Zustimmungsverweigerung entstehen im Vorgang am Dokument (Kapitel 3.4)
- **Download** – Die Originaldatei herunterladen
- **Erledigt** – Das Dokument verlässt den Eingang und liegt nur noch im Dokumentenarchiv

Ein Klick auf einen Eintrag klappt ihn auf: oben die Aktionen als Knopfleiste, darunter die PDF-Vorschau. Jede Aktion öffnet ein kleines Formular direkt unter der Leiste.

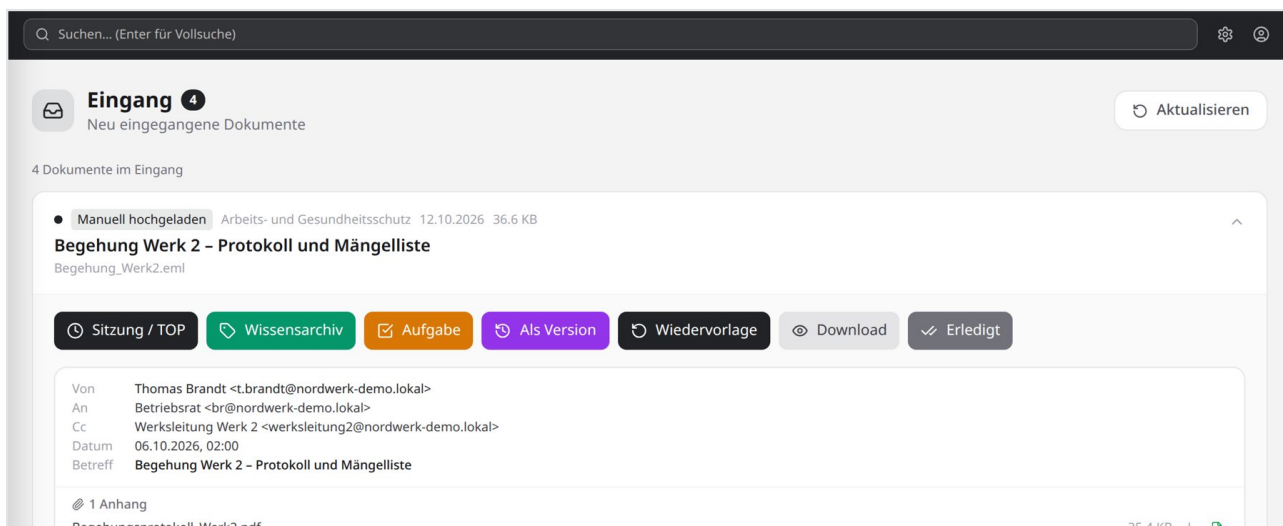


Abb. 5: Aufgeklappter Eintrag mit Aktionsleiste und Vorschau

Der Eingang ist Vorsitz, Stellvertretung und Admin vorbehalten.

3.2 Dokumentenarchiv

Das Archiv enthält alle Dokumente. Über der Liste stehen die Kategorien mit der Zahl ihrer Dokumente – ein Klick filtert. Unter dem Titel steht, in welcher Sitzung und unter welchem TOP das Dokument behandelt wurde; die Vorschau rechts listet alle Sitzungen mit Link. PDFs werden direkt im Browser angezeigt. Jedes Dokument wird beim Speichern verschlüsselt und nur beim Öffnen kurz entschlüsselt.

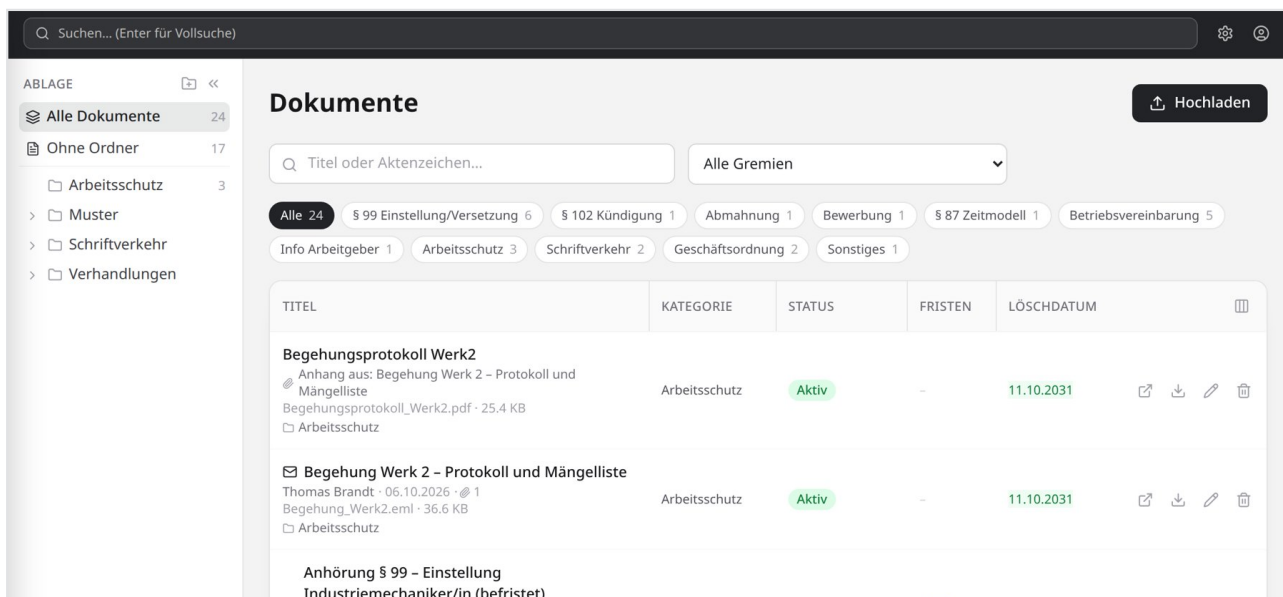


Abb. 6: Dokumentenarchiv mit Kategorie, Fristen und Löschedatum

Funktion	Beschreibung
Upload	PDF, DOCX, DOCM, XLSX und E-Mails (EML, MSG) bis 50 MB, per Klick oder Hineinziehen; bei PDFs und E-Mails wird der Text für die Volltextsuche ausgelesen
Kategorien	Anhörung § 99, Kündigung § 102, Abmahnung, Bewerbung, Bewerbung (Alternativ), Zeitmodell § 87, Betriebsvereinbarung, Information des Arbeitgebers, Arbeits- und Gesundheitsschutz, Schriftverkehr, Protokoll, Sonstiges

Funktion	Beschreibung
Metadaten	Titel, Alias, Tags, Aktenzeichen, Beschreibung, Kennzeichen „vertraulich“
Versionen	Beliebig viele Fassungen mit Änderungsnotiz
Kommentare	Diskussion direkt am Dokument
Löschung	Nach Ablauf der Aufbewahrungsfrist Löschvormerkung, danach endgültige, sichere Löschung
Löschdatum ändern	Im Bearbeiten-Dialog; wechselt die Kategorie, wird das Datum nach deren Regel ab dem Hochladen neu vorgeschlagen. Nur Daten in der Zukunft
Spalten	Grenze zwischen zwei Spalten im Kopf ziehen (feine Linie) – wie in einer Tabellenkalkulation; Reihenfolge durch Ziehen am Spaltennamen ändern, über das Spalten-Symbol rechts ein- und ausblenden. Der Titel nimmt immer den restlichen Platz; reicht er nicht (z. B. bei offener Vorschau), blendet die Liste die unwichtigsten Spalten vorübergehend selbst aus. Alles wird im Browser gemerkt

Ordner

Links neben der Liste steht die Ablage: ein Ordnerbaum wie im Datei-Explorer, z. B. „Schriftverkehr > Geschäftsführung“ oder „Muster > Arbeitsverträge“. Ordner ergänzen die Kategorien, sie ersetzen sie nicht: Die Kategorie sagt, was ein Dokument ist, und steuert Fristen, Aufbewahrung und Abläufe wie die Anhörung. Der Ordner sagt nur, wo es liegt. Jedes Dokument liegt in höchstens einem Ordner.

The screenshot shows the BR-DMS interface. On the left is the 'ABLAGEN' (Storage) sidebar with a folder tree. The main area is titled 'Dokumente' and shows a list of documents under the path 'Alle Dokumente > Schriftverkehr > Geschäftsführung'. The document list has columns for 'TITEL', 'KATEGORIE', 'STATUS', 'FRISTEN', and 'LÖSCHDATUM'. Two documents are visible: 'Antwort GF: Aufstellung Leiharbeit (Eingang per E-Mail)' and 'Schreiben an die GF: Auskunftsverlangen Leiharbeit (§ 80 Abs. 2)'. Both are in the 'Schriftverkehr' category and 'Aktiv' status.

Abb. 7: Ablage mit Ordnerbaum, Pfad und Unterordnern

Aktion	So geht es
Ordner anlegen	Ordner-Plus neben „Ablage“ (oberste Ebene) oder beim Überfahren eines Ordners (Unterordner); Name eingeben, Enter
Umbenennen, löschen	Stift bzw. Papierkorb beim Überfahren. Gelöscht werden nur leere Ordner
Dokument einsortieren	Zeile aus der Liste auf einen Ordner im Baum ziehen – oder im Bearbeiten-Dialog den Ordner wählen. Beim Hochladen ist der gerade geöffnete Ordner vorbelegt

Aktion	So geht es
Ordner verschieben	Ordner im Baum auf einen anderen ziehen; auf „Ohne Ordner“ gezogen, kommt er auf die oberste Ebene
Alle Dokumente	Zeigt wie bisher alles, unabhängig vom Ordner; unter dem Dateinamen steht, in welchem Ordner ein Dokument liegt
Ohne Ordner	Alles, was noch nicht einsortiert ist – etwa neue Dokumente aus dem Watch-Folder
Baum einklappen	« neben „Ablage“ klappt den Baum zu einer schmalen Leiste zusammen (mehr Platz für die Liste); die Ordnerwahl steht dann als Auswahlliste neben der Suche, » klappt ihn wieder auf

Die Suche über der Liste sucht im geöffneten Ordner; ein Klick auf „in allen Dokumenten suchen“ wechselt zu allen. Ordnernamen sehen alle, vertrauliche Dokumente darin nur, wer sie sehen darf. Auf dem Handy ersetzt eine Auswahlliste über der Tabelle den Baum.

E-Mails

E-Mails von außen werden wie jedes andere Dokument abgelegt – als Datei aus dem Mailprogramm: aus Outlook als .msg (Mail auf den Desktop ziehen oder „Speichern unter“), aus Thunderbird und den meisten Webmailern als .eml. Der Titel darf leer bleiben, dann gilt der Betreff. Absender, Empfänger, Text und die Namen der Anhänge sind über die Suche auffindbar.

Abb. 8: E-Mail in der Vorschau mit Kopf, Anhängen und Inhalt

Was	So funktioniert es
In der Liste	Briefumschlag vor dem Titel, darunter Absender, Datum und Zahl der Anhänge
Vorschau	Von, An, Cc, Datum und Betreff, darunter die Anhänge und der Inhalt – formatiert oder mit „Nur Text“. Bilder und Inhalte von fremden Servern werden nicht geladen, Skripte nicht ausgeführt: So erfährt der Absender nicht, dass und wann die Mail geöffnet wurde

Was	So funktioniert es
Anhänge	Jeder Anhang lässt sich herunterladen. PDF, Word, Excel und weitergeleitete Mails lassen sich zusätzlich als eigenes Dokument ablegen – beim Hochladen gleich für alle (Haken ist gesetzt) oder später einzeln in der Vorschau
Abgelegte Anhänge	Übernehmen Kategorie, Ordner, Vertraulichkeit und Aktenzeichen der E-Mail und zeigen „Anhang aus: ...“ mit Link zur E-Mail. Sie bekommen keine eigenen Fristen und erscheinen nicht einzeln im Eingang – das gilt für die E-Mail selbst
Original	„Herunterladen“ liefert die unveränderte .eml bzw. .msg, die sich wieder im Mailprogramm öffnen lässt

Vorschau, Bearbeiten und Kommentare

Ein Klick auf eine Zeile öffnet rechts die Vorschau mit dem PDF, den Sitzungen, in denen das Dokument behandelt wurde, und den Versionen. Darüber stehen „Neues Fenster“, „Herunterladen“ und „Bearbeiten“; ein Doppelklick auf die Zeile öffnet das Dokument direkt in einem neuen Fenster.

The screenshot displays the BR-DMS web interface. On the left is a sidebar with a search bar and a folder tree under 'ABLAGE' containing 'Alle Dokumente' (24), 'Ohne Ordner' (17), 'Arbeitsschutz' (3), 'Muster', 'Schriftverkehr', and 'Verhandlungen'. The main area is titled 'Dokumente' and features a search bar, a filter dropdown set to 'Alle Gremien', and a list of document categories with counts: 'Alle 24', '\$ 99 Einstellung/Versetzung 6', '\$ 102 Kündigung 1', 'Abmahnung 1', 'Bewerbung 1', '\$ 87 Zeitmodell 1', 'Betriebsvereinbarung 5', 'Info Arbeitgeber 1', 'Arbeitsschutz 3', 'Schriftverkehr 2', 'Geschäftsordnung 2', and 'Sonstiges 1'. Below this is a table of documents. The first document is 'Begehungsprotokoll Werk2' (Anhang aus: Begehung Werk 2 - Protokoll und Mängelliste, Begehungsprotokoll_Werk2.pdf · 25.4 KB, Arbeitsschutz) with a status of 'Aktiv'. The second document is 'Begehung Werk 2 - Protokoll und Mängelliste' (Thomas Brandt · 06.10.2026 · 1, Begehung_Werk2.eml · 36.6 KB) also with a status of 'Aktiv'. On the right, a preview window for 'Begehungsprotokoll Werk2' is open, showing the PDF content. Above the preview are buttons for 'Neues Fenster', 'Herunterladen', and 'Bearbeiten'. The PDF content includes the header 'NORDWERK MASCHINENBAU GMBH', the title 'Begehungsprotokoll Werk 2 - Lager und Versand', and sections for 'Mängel' and 'Fristen'.

Abb. 9: Vorschau mit „Behandelt in“ und PDF-Ansicht

„Bearbeiten“ ändert Kategorie, Ordner, Titel, Alias, Aktenzeichen, Beschreibung, Löschedatum und die Vertraulichkeit. Unten im selben Fenster steht die Diskussion zum Dokument: Kommentare mit Formatierung, Links und Dokumentverweisen. Der Knopf „Aufgabe“ an einem Kommentar macht daraus direkt eine Aufgabe – mit Titel, Zuständigkeit, Priorität und Fälligkeit.

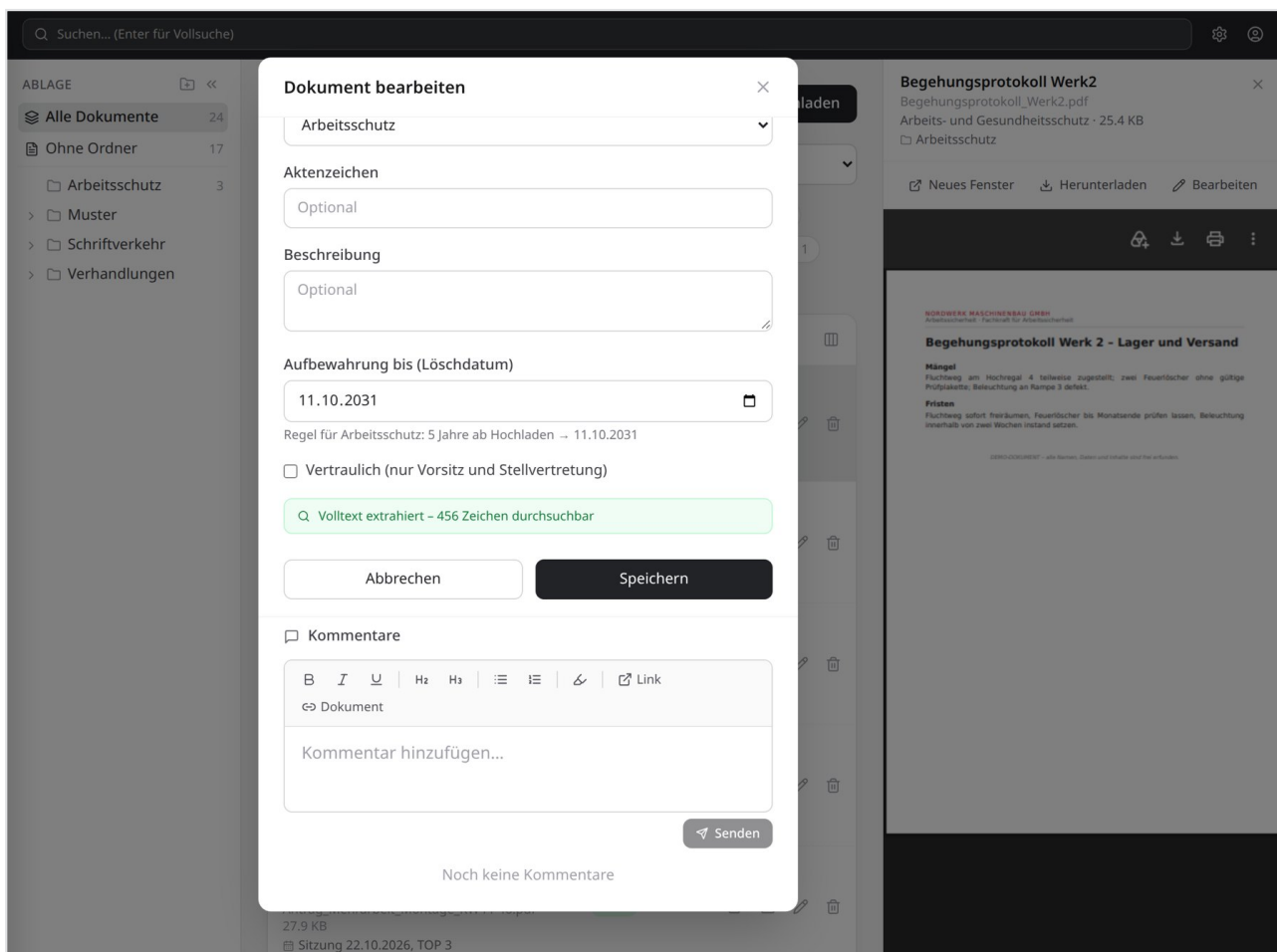


Abb. 10: Bearbeiten-Dialog mit Kommentaren und „Aufgabe“-Knopf

Vertraulichkeit

Vertrauliche Dokumente sehen Mitglieder und Ersatzmitglieder nur, wenn sie sie selbst hochgeladen haben. Vorsitz, Stellvertretung und Admin sehen alle.

3.3 Fristen & Fristenkalender

Für Anhörungen legt BR-DMS die gesetzlichen Fristen automatisch an, sobald ein Dokument der passenden Kategorie eingeht. Zusätzlich können eigene Fristen angelegt werden. Der Fristenkalender zeigt alle Fristen in der Monatsansicht, farblich nach Dringlichkeit; vor Ablauf verschickt das System eine Erinnerung per E-Mail.

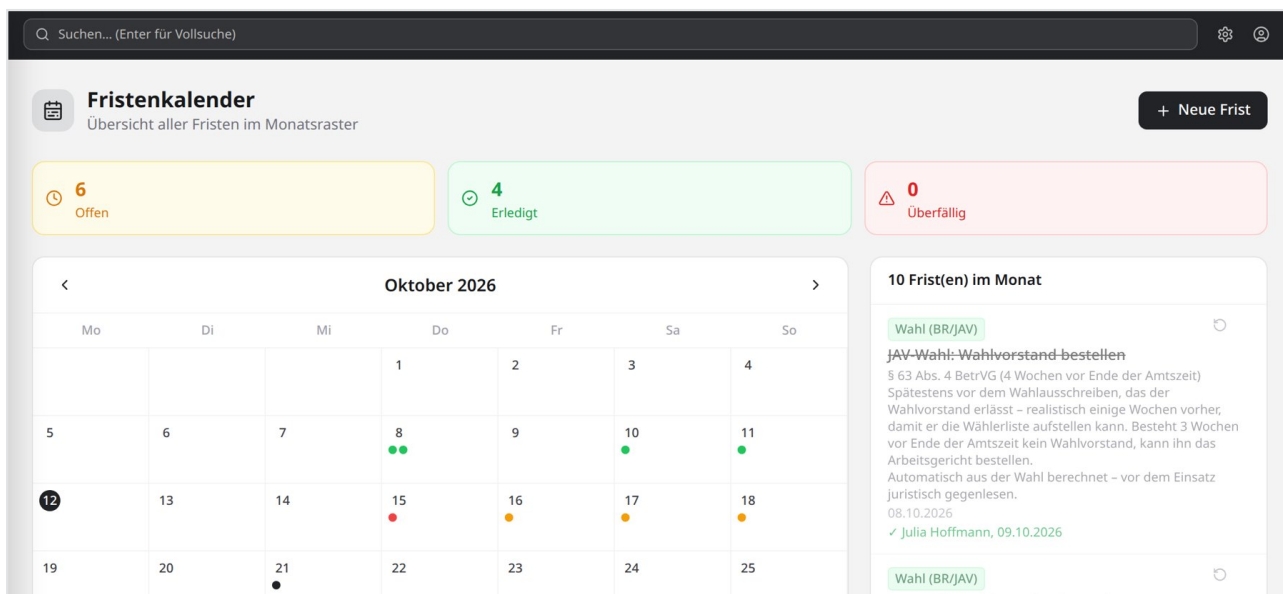


Abb. 11: Fristenkalender in der Monatsansicht

- **Erledigen** – Häkchen an der Frist (im Kalender oder auf dem Dashboard); Name und Datum werden festgehalten, der Pfeil öffnet sie wieder
- **Neue Frist** – Für Termine ohne Dokument, z. B. Wahl, Betriebsversammlung oder eine Erinnerung, mit Bezeichnung und Notiz
- **Bearbeiten** – Stift an der Frist: Bezeichnung, Datum und Notiz ändern; bei Fristen zu einem Dokument nur Datum und Notiz
- **Betriebsversammlung** – Ist im laufenden Quartal noch keine angelegt, erscheint automatisch eine Frist zum Quartalsende (§ 43 Abs. 1 BetrVG); sie erledigt sich mit der ersten Versammlung
- **Überfällig** – Offene Fristen nach ihrem Fälligkeitstag; sie bleiben offen, bis jemand sie erledigt

Fristtyp	Dauer	Rechtsgrundlage
Anhörung § 99 (Einstellung, Versetzung, Eingruppierung)	1 Woche	§ 99 Abs. 3 BetrVG
Anhörung § 102, ordentliche Kündigung	1 Woche	§ 102 Abs. 2 BetrVG
Anhörung § 102, außerordentliche Kündigung	3 Tage	§ 102 Abs. 2 BetrVG
Mitbestimmung § 87 (z. B. Mehrarbeit)	1 Woche	§ 87 BetrVG
Widerspruch	1 Woche	§ 99 / § 102 BetrVG
Betriebsversammlung im Quartal	bis Quartalsende	§ 43 Abs. 1 BetrVG
Individuelle Frist	frei wählbar	–

3.4 Anhörung als Vorgang (§ 99 / § 102)

Jedes Dokument der Kategorie „Anhörung § 99“ oder „Anhörung § 102“ ist zugleich ein Vorgang: vom Eingang über Beratung und Beschluss bis zur Antwort an den Arbeitgeber. In der Vorschau des Dokuments (Kapitel 3.2) steht dafür der Bereich „Vorgang“. Bearbeiten und versenden können Vorsitz, Stellvertretung und Admin.

Vorgang

Eingegangen Beraten Beschlossen Beantwortet

ANHÖRUNG_102_ORDENTLICH – fällig 13.09.2026 ✓

Art der Stellungnahme wählen... ▼

Begründung / weitere Ausführungen...

Speichern Entwurf als PDF

12.10.2026 📅 Als versendet markieren

Behandelt in

📅 20.08.2026 · TOP 3: Anhörung § 102 – Kündigung in der Probezeit

NORDWERK MASCHINENBAU GMBH
Personalabteilung - Az. P-102-2026-007

Anhörung § 102 - Ordentliche Kündigung (Probezeit)

Anhörung des Betriebsrats gemäß § 102 BetrVG
Wir beabsichtigen, das Arbeitsverhältnis mit dem unten genannten Beschäftigten ordentlich innerhalb der Probezeit zu kündigen.

Sozialdaten
Eintritt vor 4 Monaten, 27 Jahre, ledig, keine Unterhaltspflichten, keine Schwerbehinderung.

Kündigungsgründe
Wiederholte unentschuldigte Fehlzeiten trotz Gespräch und schriftlicher Ermahnung.

DEMO-DOKUMENT - alle Namen, Daten und Inhalte sind frei erfunden.

Abb. 12: Vorgang einer Anhörung § 102 mit Widerspruch, Gründen und Entwurf

1

Status

Eingegangen, Beraten, Beschlossen oder Beantwortet – zeigt allen, wo die Anhörung steht. „Beantwortet“ setzt BR-DMS beim Versand selbst.

2

Art wählen

Zustimmung, Zustimmungsverweigerung (§ 99 Abs. 2) oder Widerspruch (§ 102 Abs. 3).

3

Gründe ankreuzen

Bei Verweigerung und Widerspruch die gesetzlichen Gründe (§ 99 Abs. 2 Nr. 1–6 bzw. § 102 Abs. 3 Nr. 1–5) ankreuzen. Unter jedem angekreuzten Grund steht, was die Begründung konkret enthalten muss – darunter den Fall begründen. Mit „Speichern“ sichern.

4

Entwurf als PDF

Zeigt den fertigen Brief mit dem Wasserzeichen „ENTWURF“ zum Gegenlesen. Der Knopf speichert vorher die Eingaben; am Vorgang ändert sich sonst nichts.

5

Als versendet markieren

Mit dem Versanddatum: Versendet wird, was im Formular steht. Der Brief entsteht ohne Wasserzeichen, wird verschlüsselt als „Schriftverkehr“ archiviert, die Fristen des Dokuments gelten als erledigt. Fehlt ein Grund oder ist die Begründung sehr knapp, fragt BR-DMS vorher nach. Danach ausdrucken, unterschreiben und dem Arbeitgeber übergeben.

Konkret begründen

Ein Widerspruch, der nur den Gesetzestext wiederholt („eine Weiterbeschäftigung ist möglich“), ist unbeachtlich: Der Arbeitnehmer kann sich dann nicht auf den Weiterbeschäftigungsanspruch nach § 102 Abs. 5 BetrVG stützen. Deshalb immer konkret werden – bei Nr. 3 etwa die freie Stelle mit Abteilung und Datum.

Schneller geht es aus der Sitzung: Ist das Anhörungsdocument mit einem TOP verknüpft und dort ein Beschluss gefasst, füllt „Stellungnahme erzeugen“ im Mehr-Menü des TOPs (Kapitel 4.3) Art und Text aus dem Beschluss vor. Der Brief nutzt den Briefkopf aus dem Protokoll-Layout (Kapitel 9.6).

Frist und Form

Die Widerspruchsfrist ist kurz: eine Woche bei ordentlicher Kündigung, drei Tage bei außerordentlicher (§ 102 Abs. 2 BetrVG). Ein Widerspruch wirkt nur, wenn er fristgerecht, schriftlich und mit Gründen beim Arbeitgeber eingeht. Die Gründe folgen dem Wortlaut von § 99 Abs. 2 und § 102 Abs. 3 BetrVG, sind aber nicht juristisch geprüft – im Zweifel vor dem Versand rechtlich beraten lassen.

KAPITEL 4

Sitzungen

4.1 Der Lebenszyklus einer Sitzung

Jede Sitzung durchläuft feste Stufen. Jeder Übergang erzeugt eine neue, schreibgeschützte Version – so lässt sich später genau nachvollziehen, was eingeladen und was beschlossen wurde. Die Übergänge lösen Vorsitz oder Stellvertretung aus; sie sind nicht umkehrbar.

Version	Status	Was passiert
1.0	Entwurf	TOPs anlegen, sortieren, Dokumente verknüpfen
1.1	Tagesordnung fixiert	PDF der Tagesordnung entsteht, Einladung geht automatisch an alle Mitglieder
2.0	Protokoll in Bearbeitung	Anwesenheit, Ergebnisse, Beschlüsse und Abstimmungen erfassen
2.1	Protokoll final	Unveränderliches Protokoll-PDF mit Zeitstempel (SHA-256)
–	Abgesagt	Sitzung entfällt, bleibt aber dokumentiert

SITZUNG	DATUM	TYP	STATUS	TOPS	DOKUMENTE	VERSION
KOMMENDE SITZUNGEN (3)						
Ordentliche Betriebsratssitzung am 22.10.2026 Besprechungsraum BR, Verwaltungsgebäude	22.10.2026	Ordentliche Sitzung	Tagesordnung fixiert	5	5	V1.1 – Tagesordnung (Fixiert)
Betriebsversammlung am 05.11.2026 Kantine Werk 1	05.11.2026	Betriebsversammlung	Entwurf	6	–	V1.0 – Einladung (Entwurf)

Abb. 13: Sitzungsliste mit allen Stufen des Lebenszyklus

Die Liste trennt kommende Sitzungen (die nächste zuerst, die heutige zählt dazu) von vergangenen (die jüngste zuerst). Neben der Zahl der TOPs steht, wie viele Dokumente mit der Sitzung verknüpft sind.

4.2 Sitzung vorbereiten

1

Sitzung anlegen

Sitzungen → „Neue Sitzung“: Titel, Datum, Ort und Art angeben (ordentlich, außerordentlich, konstituierend oder Betriebsversammlung). Mit einer Vorlage werden Standard-TOPs gleich mit angelegt; alle aktiven Mitglieder stehen bereits auf der Anwesenheitsliste.

2

Tagesordnung aufbauen

TOPs hinzufügen, per Rich-Text beschreiben, Dokumente anhängen. Die Reihenfolge ändern Sie, indem Sie einen TOP am Punkte-Griff links an die neue Stelle ziehen; die Pfeile rechts verschieben um eine Position. Themen aus dem Themen-Backlog lassen sich direkt als TOP übernehmen. TOPs können als

vertraulich markiert werden.

3 Ladung und Verhinderung

Vor der Sitzung heißt die Anwesenheit „Ladung & Verhinderung“. Meldet sich ein Mitglied ab, wird es auf „Verhindert“ gestellt; BR-DMS schlägt das nächste Ersatzmitglied laut Wahlrang vor. Auf der Anwesenheitsliste steht der Ersatz dann mit „für ...“ in einem eigenen Abschnitt.

4 Tagesordnung fixieren

Vorsitz oder Stellvertretung fixieren die Tagesordnung: Version 1.1 und ihr PDF entstehen, alle Mitglieder erhalten eine Nachricht. Danach sind nur noch Spontan-TOPs möglich.

5 Einladung per E-Mail

In der Karte „Einladung per E-Mail“ verschickt der Vorsitz die Einladung mit der Tagesordnung als PDF an alle Geladenen – an deren Adresse für Einladungen (z. B. br-...), sonst an die Hauptadresse. Wer später nachgeladen wird, bekommt sie mit „An Neue senden“. Jeder Versand wird mit Zeitpunkt, Adresse und Ergebnis protokolliert – das ist der Nachweis der Ladung. JAV und SBV erhalten keine vertraulichen TOPs. Vor dem Senden öffnet sich ein Fenster für einen zusätzlichen Text, etwa den Link zu einem Online-Meeting; er wird beim nächsten Versand für dieselbe Sitzung vorgeschlagen. Jede Einladung bringt den Termin als Datei „Termin.ics“ mit: ein Klick darauf in Outlook oder Thunderbird trägt die Sitzung in den eigenen Kalender ein (zwei Stunden, Erinnerung 15 Minuten vorher). Wird die Einladung nach einer Änderung erneut verschickt, aktualisiert die neue Datei den vorhandenen Termin.

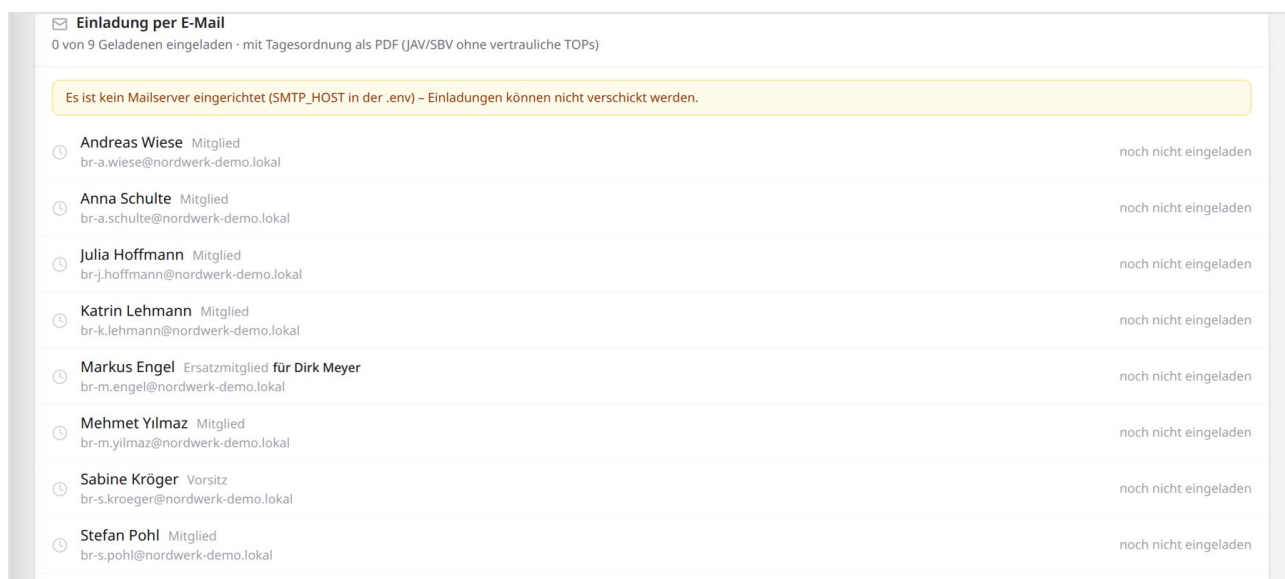


Abb. 14: Karte „Einladung per E-Mail“ mit Versandstatus je Geladenem

Ohne eingerichteten Mailserver weist die Karte darauf hin und der Versand bleibt gesperrt (Kapitel 9.7). Neben jedem Namen steht, ob und wann die Einladung zugestellt wurde.

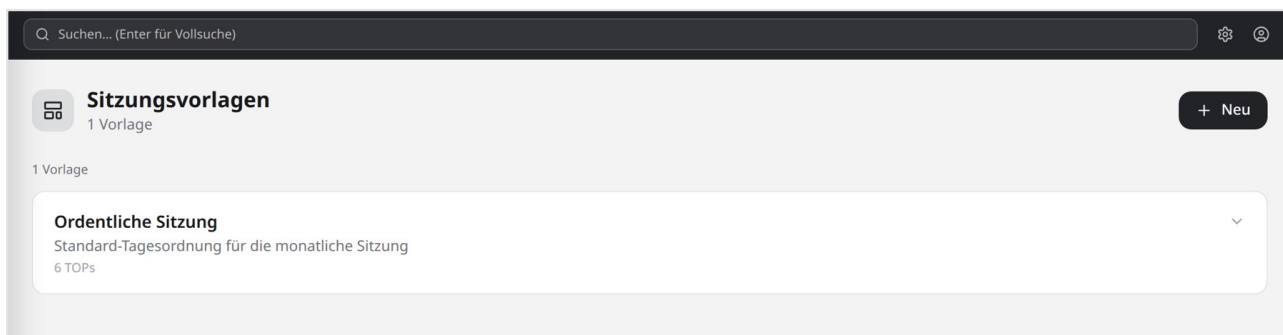


Abb. 15: Sitzungsvorlagen für wiederkehrende Tagesordnungen

4.3 Sitzung durchführen und protokollieren

Mit „Protokoll starten“ wechselt die Sitzung in den Protokollmodus. Zu jedem TOP werden Ergebnis, Beschlüsse und Abstimmungen festgehalten. Die Anwesenheitsliste lässt sich als PDF zum Unterschreiben ausdrucken.

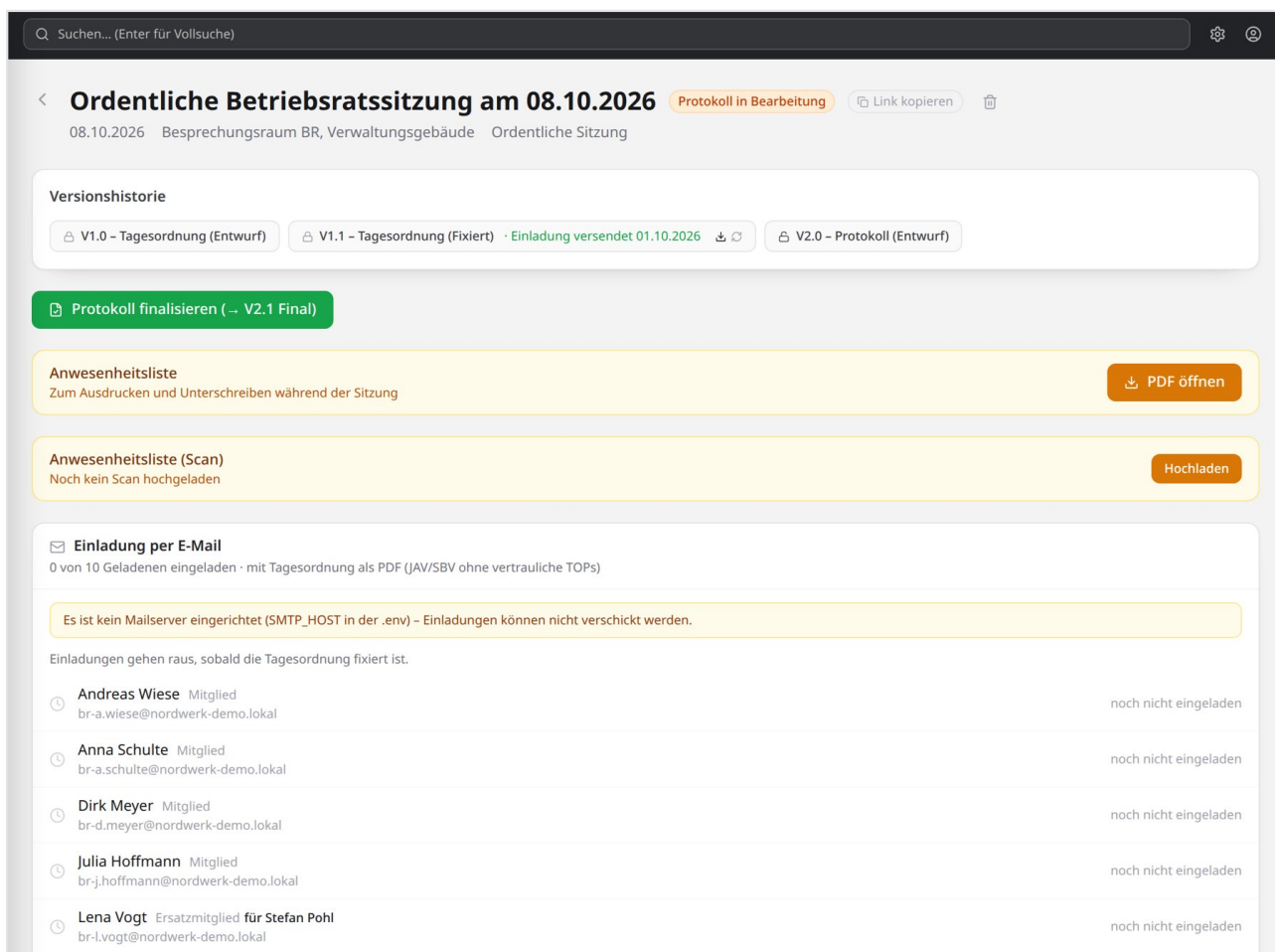


Abb. 16: Sitzung im Protokollmodus mit Editor, Beschluss und Anwesenheitsliste

Der Editor

Beschreibung und Ergebnis eines TOPs werden in einem Editor mit Werkzeugleiste geschrieben. Alles, was hier formatiert ist, erscheint genauso im PDF.

- **Fett, kursiv, unterstrichen** – auch per Strg+B, Strg+I, Strg+U

- **Überschriften** – zwei Ebenen zum Gliedern längerer TOPs
- Aufzählung und nummerierte Liste
- **Markieren** – Textmarker, etwa um den Beschlusstext hervorzuheben
- **Link** – Weblink setzen oder entfernen
- **Dokument** – Ein Dokument aus dem Archiv suchen und als Verweis einfügen; ein Klick darauf öffnet es

Jeder TOP hat außerdem eigene Kommentare für Rückfragen im Gremium; wie beim Dokument wird ein Kommentar per „Aufgabe“ zur Aufgabe. Über das Menü „...“ am TOP sind weitere Aktionen erreichbar.

Anwesenheit und Ersatzmitglieder

Für jedes Mitglied wird der Status gesetzt: anwesend, entschuldigt oder unentschuldigt abwesend. Fehlt ein Mitglied, schlägt BR-DMS das richtige Ersatzmitglied nach dem Wahlrang vor (§ 25 BetrVG) und warnt, wenn dadurch die Mindestsitze des Minderheitengeschlechts unterschritten würden.

Beschlüsse

Pro TOP können mehrere Beschlüsse erfasst werden – jeweils mit Antragstext, Rechtsgrundlage und Stimmen (Ja, Nein, Enthaltung, nicht teilgenommen). Das Ergebnis berechnet das System. Finalisierte Beschlüsse sind gesperrt und erscheinen im Beschlussregister.

Direkt aus dem TOP heraus

- **Aufgabe erstellen** – Folgeaufgabe mit Bezug zum TOP
- **Ins Wissensarchiv** – Ergebnis als Wissensseintrag festhalten
- **In die Eingruppierung** – Beschlossene Ein- oder Umgruppierung direkt beim Mitarbeiter eintragen
- **Einzelauszug** – Einen TOP als eigenes PDF erzeugen

4.4 Protokoll finalisieren

Ist das Protokoll vollständig, wird es finalisiert (Vorsitz oder Stellvertretung). Version 2.1 wird schreibgeschützt, erhält einen digitalen Zeitstempel und ein PDF mit Briefkopf, Unterschriftenzeilen und allen Abstimmungsergebnissen. Alle Mitglieder werden benachrichtigt.

Suchen... (Enter für Vollsuche)

Ordentliche Betriebsratssitzung am 17.09.2026 Protokoll final Link kopieren

17.09.2026 · Besprechungsraum BR, Verwaltungsgebäude · Ordentliche Sitzung

Versionshistorie

V1.0 – Tagesordnung (Entwurf) · V1.1 – Tagesordnung (Fixiert) · Einladung versendet 10.09.2026 · V2.0 – Protokoll (Entwurf) · Finalisiert 20.09.2026 · V2.1 – Protokoll (Final) · Finalisiert 20.09.2026

Anwesenheitsliste

Zum Ausdrucken und Unterschreiben während der Sitzung PDF öffnen

Unterschriftenseite zum Protokoll – mit Version und Prüfsumme, statt das ganze Protokoll auszudrucken Unterschriftenseite öffnen Sitzungspaket (ZIP)

Anwesenheitsliste (Scan) Hochladen
Noch kein Scan hochgeladen

Protokoll-Unterschriften (Scan) Hochladen
Noch kein Scan hochgeladen

[Eine Datei für beide hochladen](#)

Sitzung abschließen

☒ Protokoll finalisiert
☐ Anwesenheitsliste-Scan hochgeladen
☐ Protokoll-Unterschriften-Scan hochgeladen

Sitzung abschließen

Einladung per E-Mail

0 von 11 Geladenen eingeladen · mit Tagesordnung als PDF (JAV/SBV ohne vertrauliche TOPs)

Es ist kein Mailserver eingerichtet (SMTP_HOST in der .env) – Einladungen können nicht verschickt werden.

Abb. 17: Finales Protokoll mit Versionshistorie und Abstimmungsergebnis

Rechtssicherheit

Nach der Finalisierung lässt sich das Protokoll nicht mehr ändern. Der Zeitstempel (SHA-256 über Inhalt und Zeitpunkt) belegt, dass es seitdem unverändert ist.

In der Versionsliste der Sitzung steht neben jedem PDF ein Knopf „PDF neu generieren“ (Vorsitz, Stellvertretung, Admin). Er erzeugt das PDF einer Version mit dem aktuellen Protokoll-Layout neu – etwa nachdem ein neues Logo hinterlegt wurde (Kapitel 9.6). Der Inhalt der Version ändert sich dabei nicht, nur ihr Aussehen; die gespeicherte PDF-Datei wird ersetzt.

Unterschreiben und Scan hochladen

Zum Unterschreiben reicht eine eigene Unterschriftenseite statt des ganzen Protokolls – sie trägt Version und SHA-256-Prüfsumme, damit sie eindeutig dem finalisierten Stand zugeordnet ist. Die unterschriebene Anwesenheitsliste (geht zu Sitzungsbeginn rum) und die unterschriebene Unterschriftenseite (nach der Finalisierung) werden als Scan zur Sitzung hochgeladen – eine kombinierte Datei darf beide Nachweise auf einmal füllen.

- **Direkt hochladen** – PDF, JPG oder PNG über die Sitzungsseite auswählen
- **Über den Watch-Folder** – Scan in den Unterordner protokoll_scan legen (z. B. Scanner-Ablage); die Datei erscheint im Eingang als „wartender Scan“ und wird dort per Klick der richtigen Sitzung zugeordnet (Kapitel 12.6)

Sitzungspaket und Sitzung abschließen

Sobald das Protokoll final ist, lässt sich das Sitzungspaket als ZIP herunterladen: Tagesordnung bzw. Einladung als PDF, Versandnachweis als CSV, Protokoll bzw. Niederschrift als PDF und – sobald vorhanden – beide Scans. Jede Datei bleibt dabei im Original, nichts wird in ein Sammel-PDF umgewandelt; fehlt ein Teil (z. B. ein Scan steht noch aus), wird er einfach ausgelassen.

Liegen beide Scans vor, lässt sich die Sitzung endgültig abschließen. Eine Checkliste zeigt, was noch fehlt – „Sitzung abschließen“ ist erst aktiv, wenn Anwesenheitsliste- und Protokoll-Unterschriften-Scan hochgeladen sind. Danach wechselt der Status auf „Abgeschlossen“: die Sitzung ist vollständig unveränderlich, auch die Scans lassen sich nicht mehr ersetzen. Downloads (Protokoll, Scans, Sitzungspaket) funktionieren weiterhin.

4.5 Beschlussregister

Das Beschlussregister sammelt alle Beschlüsse sitzungsübergreifend – filterbar nach Zeitraum, Sitzung, Rechtsgrundlage und Ergebnis. So ist auch Jahre später schnell zu finden, wann der Betriebsrat was entschieden hat.

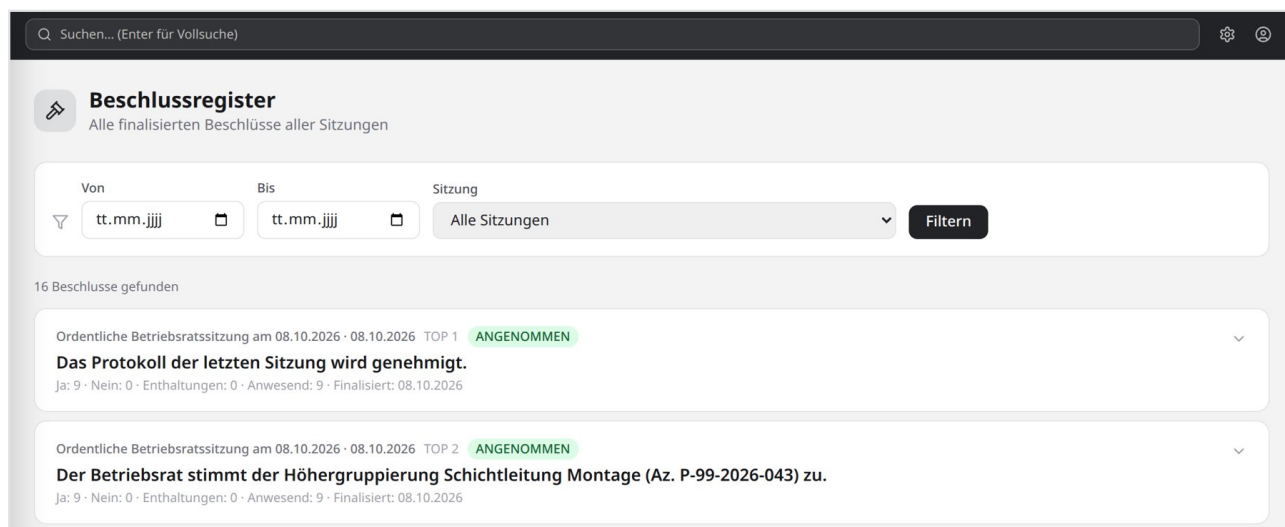


Abb. 18: Beschlussregister über alle Sitzungen

4.6 Konstituierende Sitzung und Betriebsversammlung

Beide Arten nutzen denselben Ablauf von der Tagesordnung bis zum PDF. Wird beim Anlegen keine Vorlage gewählt, bringen sie eine passende Standard-Tagesordnung mit, die sich wie gewohnt anpassen lässt.

Konstituierende Sitzung (§ 29 BetrVG)

Die erste Sitzung nach der Wahl. Die Standard-Tagesordnung enthält Eröffnung durch den Wahlvorstand, Wahl einer Wahlleitung, Wahl von Vorsitz und Stellvertretung (§ 26) und die Bildung des Betriebsausschusses (§ 27). Anwesenheit und Beschlüsse funktionieren wie bei jeder BR-Sitzung.

Betriebsversammlung (§§ 42–46 BetrVG)

Die Standard-Tagesordnung enthält Tätigkeitsbericht des Betriebsrats, Bericht des Arbeitgebers, Fragen aus der Belegschaft und Anträge an den Betriebsrat. Gegenüber einer BR-Sitzung ändert sich:

	BR-Sitzung	Betriebsversammlung
Anwesenheit	Anwesenheitsliste mit Ersatz-Nachrücken	Nur die Teilnehmerzahl
Beschlüsse	Mit Abstimmung	Keine – Anträge an den BR (§ 45) gehen ins Themen-Backlog
Tagesordnungs-PDF	Tagesordnung	Einladung zum Aushang (nicht öffentlich, Teilnahme gilt als Arbeitszeit)
Protokoll-PDF	Protokoll	Niederschrift mit Teilnehmerzahl

- **Fragen aus dem Kummerkasten** – Im Entwurf übernimmt der Knopf über der Tagesordnung ausgewählte Nachrichten ohne Absendernamen als Liste in einen TOP
- **Antrag** – Im Protokollmodus legt der Knopf am TOP einen Antrag der Versammlung als Thema im Backlog an
- **Quartals-Erinnerung** – Ohne Versammlung im laufenden Quartal erscheint eine Frist zum Quartalsende (Kapitel 3.3)

Suchen... (Enter für Vollsuche)

[Betriebsversammlung am 06.08.2026](#) Niederschrift final Link kopieren

06.08.2026 Kantine Werk 1 Betriebsversammlung

Versionshistorie

V1.0 – Einladung (Entwurf)

V1.1 – Einladung (Fixiert) · Einladung ausgehängt 30.07.2026

V2.0 – Niederschrift (Entwurf) · Finalisiert 09.08.2026

V2.1 – Niederschrift (Final) · Finalisiert 09.08.2026

Teilnahme

Bei der Betriebsversammlung gibt es keine Anwesenheitsliste – die Teilnehmerzahl erscheint in der Niederschrift. Weitere Angaben (z. B. Gäste, Arbeitgebervertretung) gehören in die Notizen.

164 Teilnehmende

Unterschriftenseite zur Niederschrift – mit Version und Prüfsumme, statt das ganze Niederschrift auszudrucken

Unterschriftenseite öffnen

Sitzungspaket (ZIP)

Niederschrift-Unterschriften (Scan)

Noch kein Scan hochgeladen

Hochladen

Sitzung abschließen

☒ Protokoll finalisiert

☐ Anwesenheitsliste-Scan hochgeladen

☐ Protokoll-Unterschriften-Scan hochgeladen

Sitzung abschließen

Tagesordnungspunkte (6)

1. **Eröffnung und Begrüßung** Zur Kenntnis

Sabine Kröger eröffnet die Versammlung und begrüßt die Beschäftigten sowie die Geschäftsführung.

Kommentar

Antrag

Ergebnis: Die Versammlung wurde um 9:05 Uhr eröffnet.

Abb. 19: Betriebsversammlung mit Teilnehmerzahl statt Anwesenheitsliste

Eine Betriebsversammlung lässt sich nicht nachträglich in eine BR-Sitzung umwandeln (und umgekehrt), weil Anwesenheitsliste und Beschlüsse sonst verwaist zurückblieben. Im Zweifel neu anlegen.

4.7 Gremien und Fremdprotokolle

Die Seite Gremien verwaltet die anderen Gremien, die der Betriebsrat begleitet – etwa Arbeitsschutzausschuss (§ 11 ASiG), Wirtschaftsausschuss (§§ 106–110), Gesamtbetriebsrat oder JAV/SBV. Der Betriebsrat selbst taucht hier bewusst nicht auf und bleibt wie gewohnt auf der Seite Sitzungen.

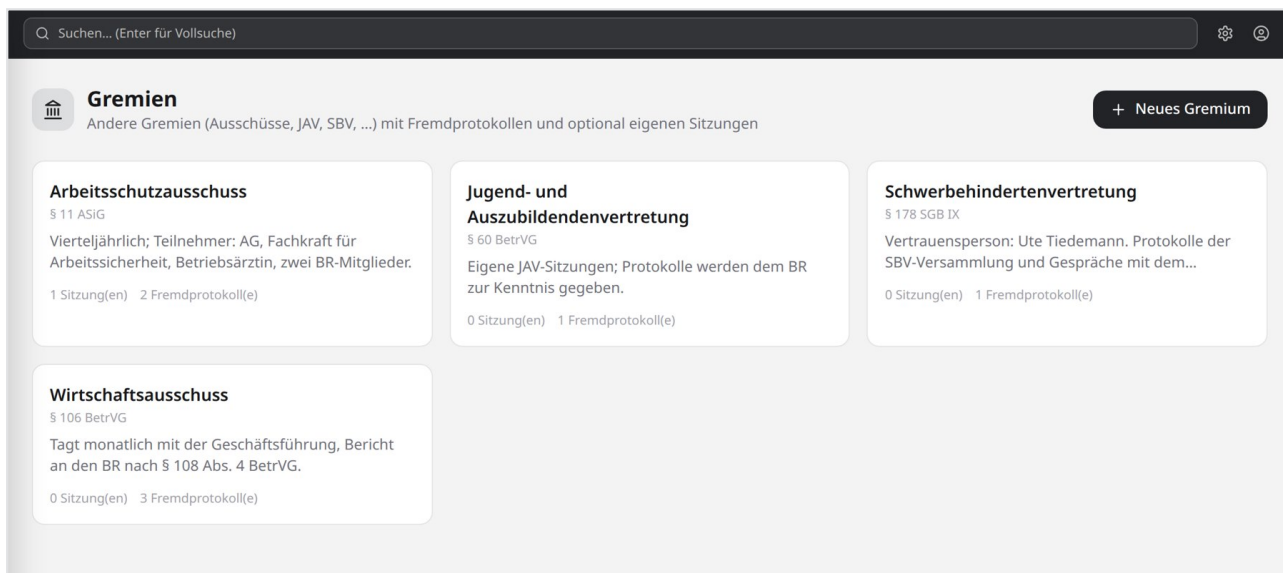


Abb. 20: Gremien-Übersicht mit Fremdprotokollen und Sitzungen

Ein Klick auf eine Karte öffnet das Gremium: oben Rechtsgrundlage und Beschreibung (Stift zum Bearbeiten), darunter die Mitglieder und eine gemeinsame Zeitleiste aus Fremdprotokollen und eigenen Sitzungen des Gremiums, neueste zuerst. Ein Doppelklick öffnet ein Fremdprotokoll in einem neuen Fenster (PDF und Bilder; DOCX wird heruntergeladen). Daneben lässt es sich herunterladen, bearbeiten und löschen; ein Schloss kennzeichnet vertrauliche.

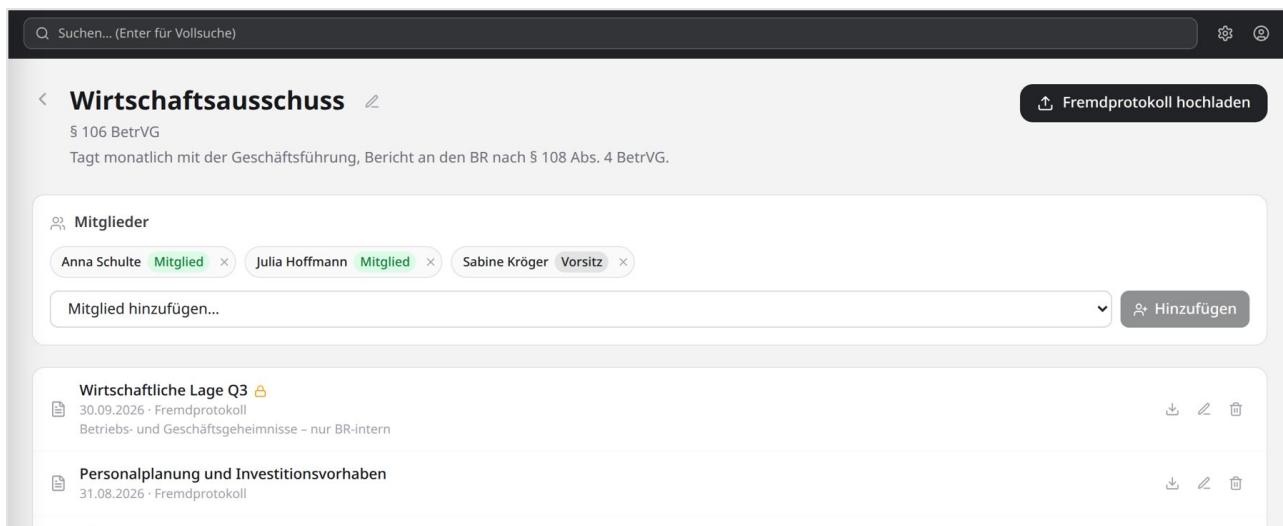


Abb. 21: Gremium mit Mitgliedern und Fremdprotokollen

Fremdprotokoll

Für Gremien, die der Betriebsrat nicht selbst im System führt, wird ein fertiges Protokoll als Fremdprotokoll abgelegt – eine hochgeladene Datei mit Gremium, Datum und Titel, ohne eigene Tagesordnungspunkte oder Anwesenheitsliste. Eine Markierung als vertraulich beschränkt Ansicht und Download auf Vorsitz, Stellvertretung, Admin und die Mitglieder dieses Gremiums – etwa für Wirtschaftsausschuss-Protokolle, die nur dessen Mitglieder sehen sollen. Hochgeladen wird über „Fremdprotokoll hochladen“ – PDF, JPG, PNG oder DOCX, mit Datum, Titel und optionaler Bemerkung.

Mitglieder

Je Gremium lässt sich hinterlegen, wer dazugehört. Führt der Betriebsrat eine Sitzung dieses Gremiums doch im System (Tagesordnung, Protokoll, PDF wie gewohnt – über das Gremium-Feld beim Anlegen einer Sitzung), füllt BR-DMS die Anwesenheit automatisch mit diesen Mitgliedern statt mit allen Betriebsratsmitgliedern vor.

Ohne hinterlegte Mitglieder bleibt die Anwesenheitsliste einer Gremium-Sitzung leer und wird von Hand gepflegt – BR-DMS füllt dann nicht ersatzweise die Betriebsratsmitglieder ein.

Sowohl die Sitzungsliste als auch das Dokumentenarchiv lassen sich nach Gremium filtern; bei Dokumenten, die über einen TOP mit einer Gremium-Sitzung verknüpft sind, erscheint der Gremium-Name zusätzlich direkt bei „Behandelt in“.

KAPITEL 5

Planung & Zusammenarbeit

5.1 Aufgaben und Vorhaben

Aufgaben haben Priorität, Fälligkeit, eine verantwortliche Person und können privat oder für alle sichtbar sein. Größere Vorhaben – etwa eine Wahl, eine Betriebsversammlung oder eine Verhandlungsphase – fassen mehrere Aufgaben über einen Zeitraum zusammen. Vorhaben lassen sich verschachteln und farblich kennzeichnen. Über den Filter oben zeigt die Seite alle Aufgaben, nur die ohne Vorhaben oder die eines bestimmten Vorhabens.

Ansicht	Wofür
Board	Alle Aufgaben als Kanban (Neu, In Bearbeitung, Auf Hold, Erledigt), per Ziehen verschieben; das Vorhaben steht klein an der Karte
Liste	Aufgaben gruppiert nach Vorhaben, dazu die Aufgaben ohne Vorhaben; mit „+“ direkt eine Aufgabe im Vorhaben anlegen
Zeitplan	Vorhaben und ihre Aufgaben als Gantt-Diagramm über die Zeit

Abb. 22: Board mit Aufgaben aus verschiedenen Vorhaben

Suchen... (Enter für Vollsuche)

Aufgaben
14 offene Aufgaben · 3 Vorhaben

Board Liste Zeitplan + Vorhaben + Aufgabe

Alle Vorhaben **Alle** Offen (14) Erledigt

Verhandlungsphase BV Schichtarbeit
Vorhaben 13.08.2026 – 26.11.2026 Thomas Brandt von Thomas Brandt

Noch keine Aufgaben in diesem Vorhaben.

JAV-Wahl 2026 3 offen
Begleitung der JAV-Wahl durch den Betriebsrat. Den Ablauf verantwortet der Wahlvorstand.
Vorhaben 12.09.2026 – 01.12.2026 Finn Albers von Sabine Kröger

Wahlvorstand mit Azubi-Liste unterstützen

Abb. 23: Liste, gruppiert nach Vorhaben

Suchen... (Enter für Vollsuche)

Aufgaben
14 offene Aufgaben · 3 Vorhaben

Board Liste Zeitplan + Vorhaben + Aufgabe

Alle Vorhaben **Alle** Offen (14) Erledigt

VORHABEN Aug. 26 Sept. 26 Okt. 26 Nov. 26 Dez. 26 Jan. 27 Feb. 27 März 27 Apr. 27 Mai 27 Juni

Verhandlungsphase BV ... Verhandlungsphase BV Schichtarbeit

JAV-Wahl 2026 JAV-Wahl 2026

Wahlvorstand mit Azubi-Li...

Konstituierende Sitzung d...

Wahlversammlung/Wahlta...

Abb. 24: Zeitplan der Vorhaben

Wird ein Vorhaben gelöscht, bleiben seine Aufgaben erhalten und stehen danach ohne Vorhaben da.

5.2 Themen-Backlog

Im Themen-Backlog sammelt der Betriebsrat Ideen und Anliegen, bevor sie in eine Sitzung kommen. Ein Klick übernimmt ein Thema als TOP in die nächste Sitzung. Auch Anträge aus der Betriebsversammlung landen hier (Kapitel 4.6).

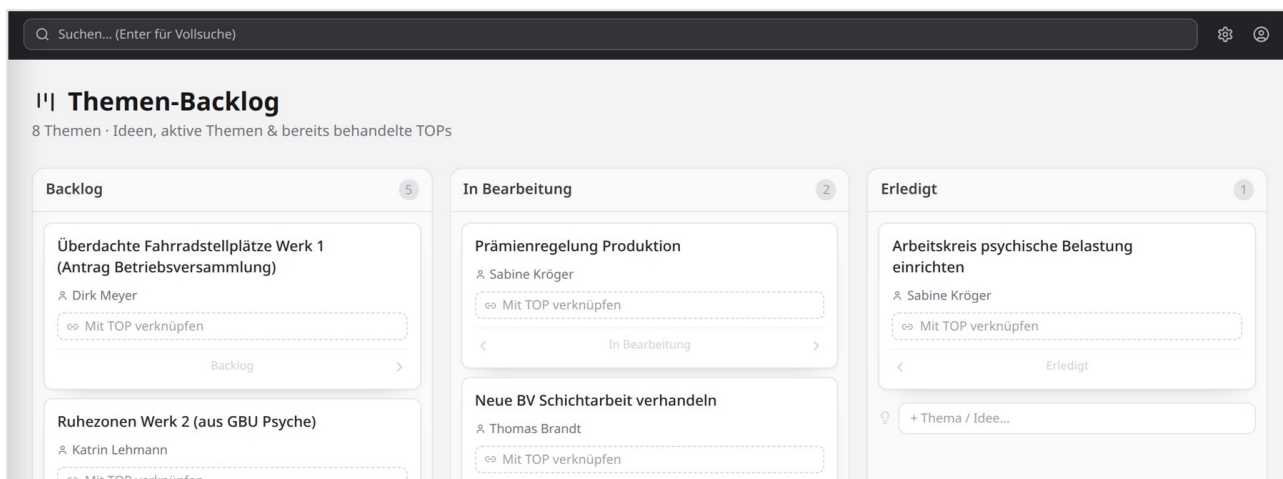


Abb. 25: Themen-Backlog als Kanban-Board

5.3 Nachrichten

Das interne Postfach verbindet die Mitglieder ohne externe Dienste. Nachrichten gehen an einzelne Mitglieder, an alle oder an die Teilnehmer einer Sitzung. Einladungen und Protokolle verschickt das System automatisch, auf Wunsch mit PDF-Anhang.

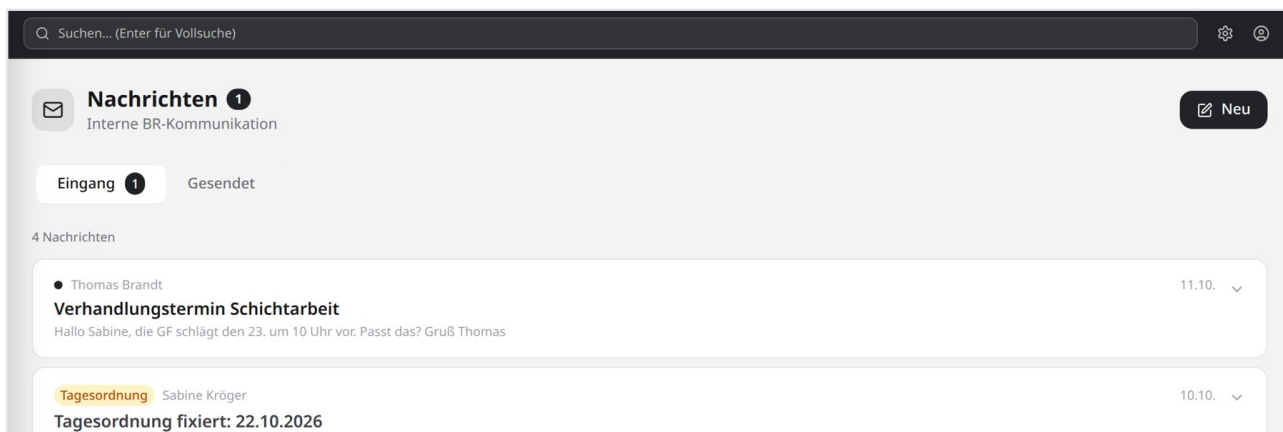


Abb. 26: Postfach mit Systemnachrichten und persönlichen Nachrichten

5.4 Kummerkasten

Der Kummerkasten ist eine öffentliche Seite ohne Anmeldung, über die Beschäftigte dem Betriebsrat Anliegen, Kritik oder Ideen schicken – anonym oder mit Namen. Intern werden die Einträge mit Status und einer nur für den Betriebsrat sichtbaren Notiz bearbeitet. Für die Betriebsversammlung lassen sich Einträge als Fragen in die Tagesordnung übernehmen (Kapitel 4.6).

BR-DMS.

Kummerkasten

Anliegen, Kritik oder Ideen an den Betriebsrat — anonym möglich, Name ist freiwillig.

Dein Anliegen *

Was möchtest du dem Betriebsrat mitteilen?

Name (optional)

Kannst du frei lassen, wenn du anonym bleiben möchtest

Absenden

Für BR-Mitglieder: Anmelden - BR-DMS - Open Source (AGPL 3.0)

Abb. 27: Öffentliches Formular (ohne Login erreichbar)

Suchen... (Enter für Vollsuche)

Kummerkasten

3 offen · 5 gesamt — eingereicht über die öffentliche Formularseite

Offen (3) Alle

Anonym · 11.10.2026

Mein Vorgesetzter ruft regelmäßig nach Feierabend an. Ist das erlaubt?

Interne Notiz (für den Absender nicht sichtbar)

z.B. wer sich kümmert, Stand der Klärung...

Neu

Anonym · 10.10.2026

Gibt es eine Möglichkeit für ein Jobrad? Andere Firmen in der Gegend haben das auch.

Neu

Abb. 28: Interne Bearbeitung der Kummerkasten-Einträge

Anonymität

Das Formular speichert keine IP-Adresse und keinen Benutzerbezug. Gegen automatisierte Einsendungen schützen eine Mengenbegrenzung und ein unsichtbares Prüffeld.

5.5 Wahlen (Betriebsrat und JAV)

Unter Planung → Wahlen begleitet der Betriebsrat BR- und JAV-Wahlen. Den Ablauf verantwortet der Wahlvorstand; BR-DMS hilft, die Fristen im Blick zu behalten, die Wählerliste vorzubereiten und das Ergebnis zu übernehmen. Der Wahlvorstand braucht keinen eigenen Zugang.

Gegenlesen

Fristen, Altersgrenzen und Sitzzahlen sind aus BetrVG und Wahlordnung abgeleitet, aber nicht juristisch geprüft. Jede Frist nennt ihre Rechtsgrundlage; Empfehlungen ohne gesetzliche Frist sind gelb markiert. Vor dem Einsatz gegenlesen lassen (Gewerkschaft, Schulung des Wahlvorstands).

Wahl anlegen und Fristen

„Neue Wahl“: Art (BR oder JAV), Verfahren (normal oder vereinfacht), Tag der Stimmabgabe bzw. der Wahlversammlung, Ende der Amtszeit und – sobald bekannt – das Datum des Wahlausschreibens. Daraus berechnet BR-DMS die Fristen; sie erscheinen auf der Seite und im Fristenkalender und lassen sich dort abhaken. Ändern sich die Daten, werden die Fristen neu berechnet; Erledigt-Haken bleiben stehen. Optional entsteht ein Vorhaben im Zeitplan für eigene Aufgaben rund um die Wahl.

Schritt	Normales Verfahren	Vereinfachtes Verfahren
Wahlvorstand bestellen	BR 10, JAV 8 Wochen vor Amtszeitende	4 Wochen vor Amtszeitende
Wahlausschreiben	spätestens 6 Wochen vor der Stimmabgabe	Empfehlung: 3 Wochen vor der Versammlung
Einspruch Wählerliste	2 Wochen nach dem Ausschreiben	3 Tage nach dem Ausschreiben
Wahlvorschläge	2 Wochen nach dem Ausschreiben	1 Woche vor der Versammlung
Konstituierende Sitzung (BR)	binnen 1 Woche nach der Wahl	binnen 1 Woche nach der Wahl
Anfechtung	2 Wochen ab Bekanntgabe	2 Wochen ab Bekanntgabe

Suchen... (Enter für Vollsuche)

Wahlen

BR- und JAV-Wahlen begleiten: Fristen nach BetrVG und Wahlordnung im Blick behalten

+ Neue Wahl

⚠

Die Fristen werden aus BetrVG und Wahlordnung berechnet, sind aber **nicht juristisch geprüft**. Bitte vor dem Einsatz gegenlesen lassen (Gewerkschaft, Schulung des Wahlvorstands). Den Ablauf verantwortet der Wahlvorstand – hier behält der Betriebsrat ihn im Blick.

JAV-Wahl 2026

JAV-Wahl

Vereinfachtes Verfahren

Zeitplan

Wahlversammlung am 06.11.2026 · Amtszeit endet 26.11.2026 · Wahlausschreiben vom 08.10.2026

Wahlvorstand: Julia Hoffmann (BR), zwei Auszubildende.

08.10.2026

Wahlvorstand-bestellen

§ 63 Abs. 4 BetrVG (4 Wochen vor Ende der Amtszeit)

⌚ Spätestens vor dem Wahlausschreiben, das der Wahlvorstand erlässt – realistisch einige Wochen vorher, damit er die Wählerliste aufstellen kann. Besteht 3 Wochen vor Ende der Amtszeit kein Wahlvorstand, kann ihn das Arbeitsgericht bestellen.

✓ Julia Hoffmann, 09.10.2026

08.10.2026

Wahlausschreiben-erlassen

§ 36 WO (einstufiges vereinfachtes Verfahren)

⌚ Tatsächliches Datum des Wahlausschreibens.

✓ Julia Hoffmann, 09.10.2026

Abb. 29: Wahl mit berechneten Fristen und Rechtsgrundlagen

Wählerliste und Gremiumsgröße

Der Bereich „Wählerliste & Gremiumsgröße“ ermittelt aus den Mitarbeiterdaten zum Wahltag, wer wahlberechtigt und wählbar ist, wie groß das Gremium wird und wie viele Sitze dem Geschlecht in der Minderheit mindestens zustehen. Er schlägt auch das Verfahren vor. Dafür braucht es Geburtsdatum und Geschlecht der Beschäftigten – am einfachsten per CSV-Import aus der Liste der Personalabteilung (Kapitel 7.1).

	BR-Wahl	JAV-Wahl
Wahlberechtigt	ab 16 (§ 7), Zeitarbeit nach mehr als 3 Monaten	unter 18 oder Auszubildende unter 25 (§ 60)
Wählbar	ab 18, 6 Monate im Betrieb (§ 8)	unter 25 (§ 61), keine BR-Mitglieder
Größe	§ 9	§ 62
Minderheitengeschlecht	§ 15 – ab 3 Sitzen, Höchstzahlverfahren	§ 62 Abs. 3 – ab 3 Sitzen

- **Dual Studierende** – Schalter je JAV-Wahl, ob sie als Auszubildende zählen; ob das zutrifft, hängt vom Vertrag ab
- **Ausschließen** – Personen von Hand aus der Liste nehmen, z. B. leitende Angestellte
- **Bitte prüfen** – Fehlt ein Geburtsdatum, steht die Person in einer Prüfliste statt in der Wählerliste
- **PDF zum Aushang** – Getrennt nach Geschlechtern, alphabetisch, ohne Geburtsdaten
- **CSV für den Wahlvorstand** – Vollständige Liste mit Geburtsdaten

▼ Wählerliste & Gremiumsgröße Vorschlag aus den Mitarbeiterdaten zum Wahltag

Wahlberechtigt
15
 2 w · 13 m

Größe des Gremiums
1 Sitz
 § 62 Abs. 1 BetrVG: 15 Jugendliche und Auszubildende

Minderheitengeschlecht
entfällt
 Erst ab 3 Sitzen und bei echter Minderheit (§ 15 Abs. 2, § 62 Abs. 3)

Verfahren
Vereinfachtes Verfahren
 15 JAV-Wahlberechtigte: vereinfachtes Verfahren ist Pflicht (§ 63 Abs. 4 und 5 BetrVG).

☐ Dual Studierende als Auszubildende zählen (hängt vom Vertrag ab) – 5 dual Studierende zählen nicht mit; eingeschaltet wären es 20 Wahlberechtigte

[PDF zum Aushang](#) [CSV für den Wahlvorstand](#)

Das PDF enthält keine Geburtsdaten (Abdruck zum Aushang). Die CSV mit Geburtsdaten ist nur für den Wahlvorstand bestimmt.

Q Name oder Abteilung filtern

Name	Abteilung	Alter	Geschl.	Art	Wahlbar
Albers, Finn	Ausbildung	18	m	Azubi	ja
Fischer, Sebastian	Ausbildung	19	m	Azubi	ja
Frank, Daniel	Ausbildung	21	m	Azubi	ja
Franke, Piotr	Ausbildung	17	m	Azubi	ja
Keller, Heike	Ausbildung	17	w	Azubi	ja

Abb. 30: Wählerliste mit Gremiumsgröße und Verfahrensvorschlag

Ergebnis übernehmen

Nach der Wahl überträgt „Ergebnis übernehmen“ das Protokoll des Wahlvorstands: die Gewählten in ihrer Rangfolge, erst die Mitglieder, dann die Ersatzmitglieder. Die Position ist der Wahlrang für das Nachrücken (Kapitel 4.3). Die Vorschau zeigt vor dem Speichern, was sich ändert, und warnt etwa, wenn die Mindestsitze unterschritten sind oder danach niemand Vorsitz ist.

- **Konten** – Bestehende Konten werden über den Namen erkannt; für neue Personen eine E-Mail-Adresse angeben. Das neue Konto hat ein Zufallspasswort, das der Vorsitz in der Benutzerverwaltung neu setzt
- **Rollen** – Mitglieder werden Mitglied, Ersatzmitglieder Ersatzmitglied; Vorsitz und Stellvertretung behalten ihre Rolle bis zur konstituierenden Sitzung. Bei der JAV-Wahl erhalten die Gewählten die Rolle JAV
- **Nicht wiedergewählt** – Auf Wunsch deaktivieren; sonst verlieren sie nur ihren Wahlrang
- **Quote** – Minderheitengeschlecht und Mindestsitze landen in den Einstellungen und gelten für das Nachrücken
- **Konstituierende Sitzung** – Wird mit der Standard-Tagesordnung angelegt (Kapitel 4.6)

#	Name	Gewählt als	Stimmen	Geschlecht	E-Mail (nur neue Konten)
1	Sabine Kröger	Mitglied	148	weiblich	
2	Thomas Brandt	Mitglied	139	männlich	
3	Mehmet Yilmaz	Mitglied	130	männlich	
4	Julia Hoffmann	Mitglied	121	weiblich	
5	Andreas Wiese	Mitglied	112	männlich	
6	Katrin Lehmann	Mitglied	103	weiblich	
7	Stefan Pohl	Mitglied	94	männlich	
8	Dirk Meyer	Mitglied	85	männlich	

Abb. 31: Ergebnis übernehmen – Rangfolge, Stimmen und Geschlecht

Das übernommene Ergebnis bleibt an der Wahl stehen – so sind frühere Wahlen jederzeit nachschlagbar.

5.6 Kosten des Betriebsrats (§ 40)

Der Arbeitgeber trägt die erforderlichen Kosten der Betriebsratsarbeit. Unter „Kosten (§ 40)“ (Seitenleiste, Planung) steht dafür eine Jahresübersicht: oben die Summe des Jahres, was noch offen, bezahlt oder abgelehnt ist, darunter die Aufteilung nach Art und alle Posten. Ein Klick auf eine Art zeigt nur deren Posten.

Summe 2026	Offen	Bezahlte	Abgelehnt
9.812,40 € ohne abgelehnte Posten	8.794,40 € beantragt oder zugesagt	1.018,00 €	169,00 € ggf. Beschlussverfahren

Art	Betrag
Schulung (§ 37 Abs. 6/7)	2.380,00 €
Sachverständige (§ 80 Abs. 3)	4.800,00 €
Rechtsanwalt	1.428,00 €
Sachmittel (§ 40 Abs. 2)	1.018,00 €
Reisekosten	186,40 €

DATUM	BEZEICHNUNG	STATUS	BETRAG

Abb. 32: Kostenübersicht mit Summen, Arten und Posten

- **Arten** – Schulung (§ 37 Abs. 6/7), Sachverständige (§ 80 Abs. 3), Rechtsanwalt, Einigungsstelle (§ 76a), Sachmittel (§ 40 Abs. 2), Reisekosten, Sonstiges
- **Status** – Beantragt, Zugesagt, Bezahlte oder Abgelehnt. Abgelehnte Posten zählen nicht zur Summe, bleiben aber sichtbar – etwa als Grundlage für ein Beschlussverfahren
- **Beschluss** – Sachverständige, Anwalt und Schulungen brauchen einen BR-Beschluss; der Posten zeigt auf den Beschluss aus dem Register

- **Rechnung oder Kostenzusage** – als Dokument aus der Ablage verknüpft. Fremde vertrauliche Dokumente erscheinen für Mitglieder nur als „Vertrauliches Dokument“
- **Export** – „PDF“ für die Jahresübersicht zum Ausdrucken, „CSV“ zum Öffnen in Excel

Abb. 33: Posten bearbeiten mit Status, Beschluss und Rechnung

BR-Schulungen kommen von selbst

Schulungstermine werden unter „Schulungen“ gepflegt (Kapitel 7.6). Welche Qualifikationen BR-Schulungen sind, legt der Vorsitz einmal über „BR-Schulungen“ fest – Arbeitsschutz-Schulungen der Belegschaft wie Ersthelfer gehören nicht dazu. Termine dieser Qualifikationen mit Kosten erscheinen dann automatisch. Datum und Betrag kommen aus der Schulung und werden dort geändert; Status, Beschluss und Rechnung pflegt man in der Kostenübersicht. Abgesagte Termine fallen heraus.

Rechte

Sehen dürfen die Übersicht Mitglieder und aktiv vertretende Ersatzmitglieder; eintragen, ändern und löschen Vorsitz und Stellvertretung. Jede Änderung steht im Audit-Log.

KAPITEL 6

Wissen & Recherche

6.1 Wissensarchiv

Das Wissensarchiv hält Erfahrungen und Lösungen für wiederkehrende Fragen fest – jeweils mit Sachverhalt und Lösung, Schlagworten und der Herkunft (manuell oder aus einem Protokoll übernommen). So geht Wissen auch bei einem Wechsel im Gremium nicht verloren.

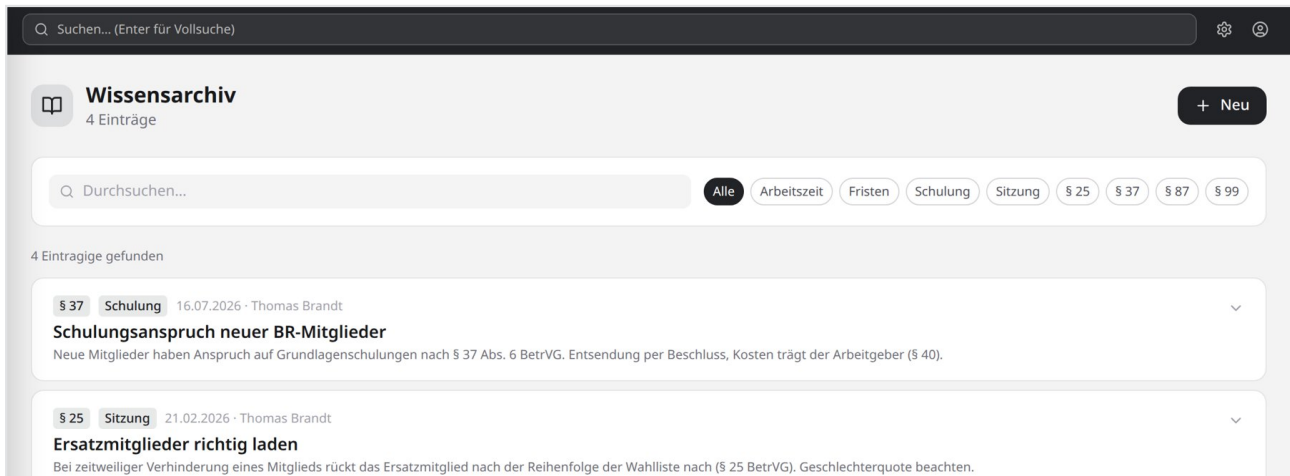


Abb. 34: Wissensarchiv mit Schlagworten

6.2 Ressourcen

Eine gepflegte Linksammlung zu Gesetzen, Behörden, Vorlagen und Werkzeugen, mit Kategorien und Schlagworten. Das Symbol der Zielseite wird automatisch geladen.

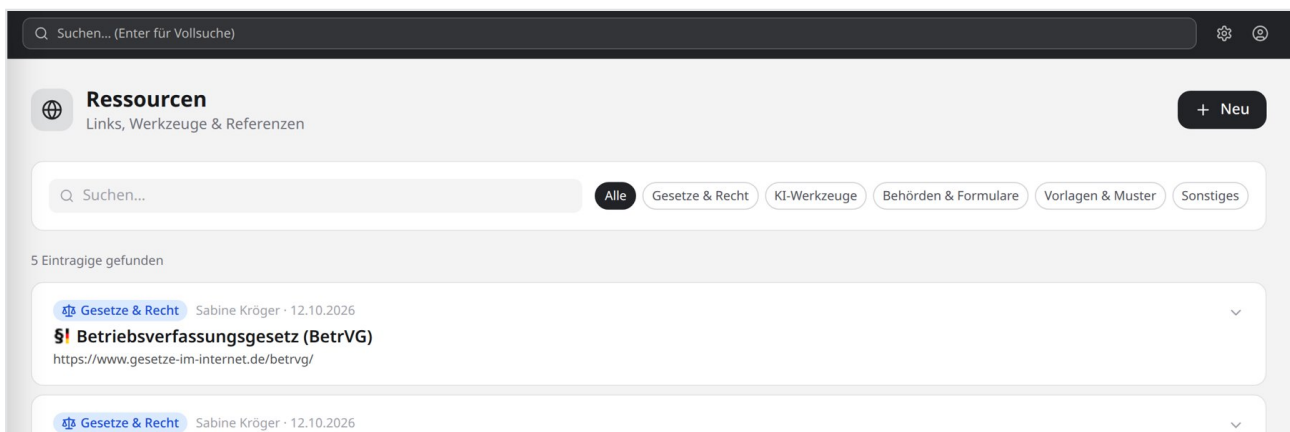


Abb. 35: Ressourcen nach Kategorien

6.3 Themensammlung

Die Themensammlung bereitet Sitzungsergebnisse für die Belegschaft auf – für einen Aushang oder einen Newsletter. Sie sammelt alle TOPs aus protokollierten Sitzungen eines Zeitraums, deren Titel ein Stichwort enthält (Standard: „öffentlich“), und zeigt deren Ergebnis-Text. Am einfachsten bekommt jede Sitzung einen TOP wie „Öffentlichkeitsarbeit – Aushang an die Belegschaft“, in dessen Ergebnis der Text für die Belegschaft steht – ohne Namen und Vertrauliches.

Abb. 36: Themensammlung mit zwei Aushangtexten

- Zeitraum und Stichwort wählen, dann „Themen laden“
- **Drucken** – Die Zusammenstellung direkt ausdrucken, z. B. fürs Schwarze Brett
- **HTML herunterladen** – Fertig formatierte Datei, etwa zum Einfügen in einen Newsletter oder ins Intranet

6.4 Globale Suche und Gesetzestexte

Die Suche durchsucht alle Bereiche gleichzeitig – Dokumente samt PDF-Volltext, Sitzungen, TOPs und Beschlüsse, Aufgaben, Wissensarchiv, Ressourcen, Betriebsvereinbarungen, Schulungen, Mitarbeiter und Gesetzestexte – und gruppiert die Treffer nach Bereich.

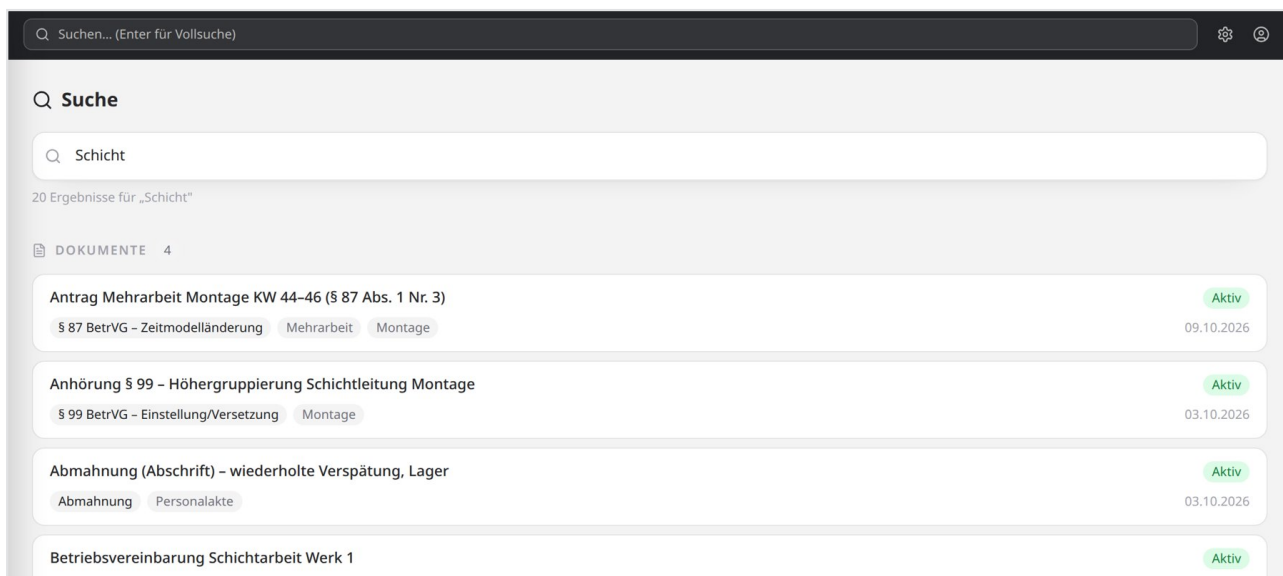


Abb. 37: Suchergebnisse nach Bereichen gruppiert

Die Gesetzestexte (BetrVG, KSchG, ArbSchG, SGB IX, BUrlG, ArbZG) werden monatlich automatisch aktualisiert (Kapitel 9.8). Ein Klick auf einen Paragraphen – in der Suche oder in der Schnellsuche oben links – öffnet den Volltext als Fenster direkt in der Anwendung, ohne Internetverbindung.

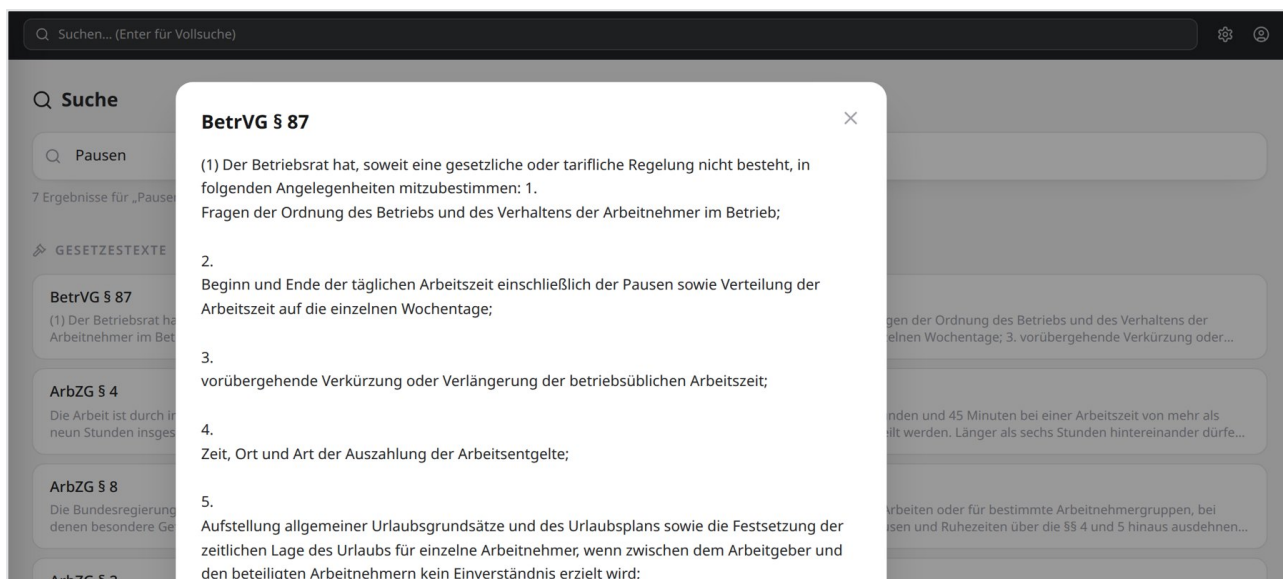


Abb. 38: Paragraph als Fenster: § 87 BetrVG aus der Suche nach „Pausen“

KAPITEL 7

Personal

Die Personalverwaltung bildet die gesamte Belegschaft ab – unabhängig davon, wer einen Zugang zu BR-DMS hat. Sie ist ein optionales Modul und lässt sich abschalten (Kapitel 9.4).

7.1 Mitarbeiter

Stammdaten mit Personalnummer, Abteilung, Standort, Ein- und Austritt sowie Beschäftigungsart (Mitarbeiter, Azubi, Student, dual Studierende, Zeitarbeit). Für Wahlen kommen Geburtsdatum und Geschlecht hinzu (Kapitel 5.5). Die Übersicht zeigt Kennzahlen und die Verteilung nach Standort.

CSV-Import

Der Import liest eine CSV-Datei (Semikolon oder Komma) mit Kopfzeile und zeigt vor dem Speichern eine Vorschau. Pflicht sind nur Nachname und Vorname, die Reihenfolge der Spalten ist egal: PNR, Nachname, Vorname, Abteilung, Eintritt, Austritt, Standort, Geburtsdatum, Geschlecht (oder Anrede). Vorhandene Mitarbeiter werden über die PNR erkannt und ergänzt; Geburtsdatum und Geschlecht aus der Liste der Personalabteilung ersetzen abweichende Werte, die Vorschau meldet jede Korrektur. Ungültige Daten werden mit Zeilennummer abgelehnt.

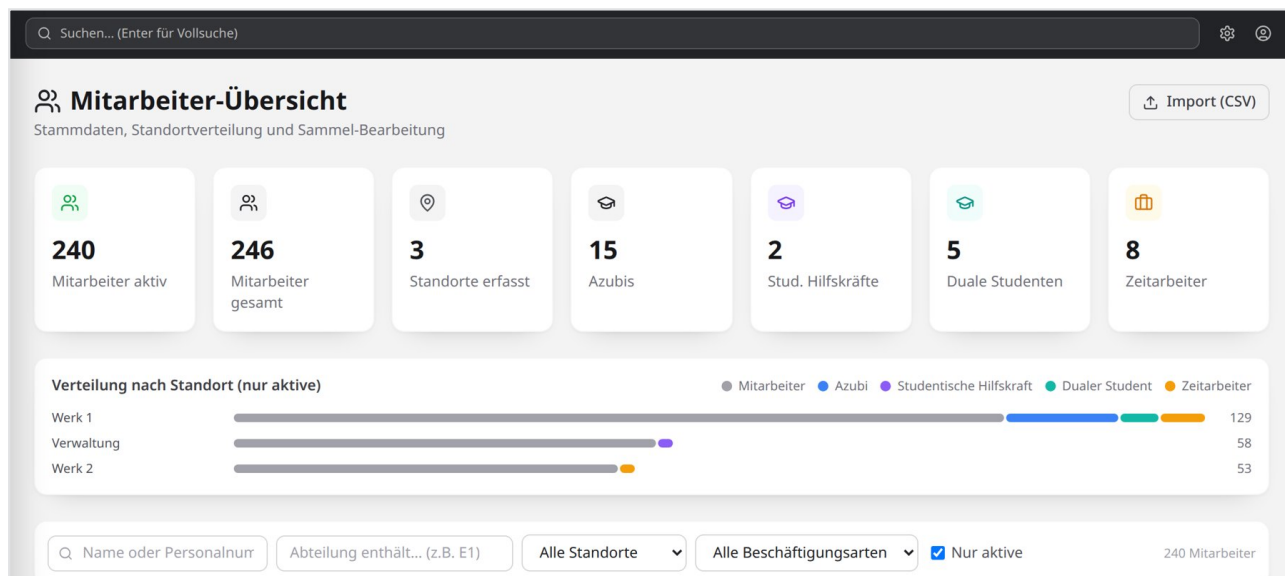


Abb. 39: Mitarbeiterübersicht mit Kennzahlen

Filtern, bearbeiten und Standort für viele setzen

Die Liste lässt sich nach Name oder Personalnummer, Abteilung, Standort und Beschäftigungsart filtern; „Nur aktive“ blendet Ausgetretene aus. Der Stift am Ende einer Zeile öffnet die Stammdaten zum Bearbeiten. Über die Kästchen vor den Namen werden mehrere Mitarbeiter markiert – das Kästchen im Tabellenkopf wählt alle gefilterten. Dann erscheint eine Leiste, in der ein Standort eingetragen und mit „Standort übernehmen“ für alle Markierten gesetzt wird.

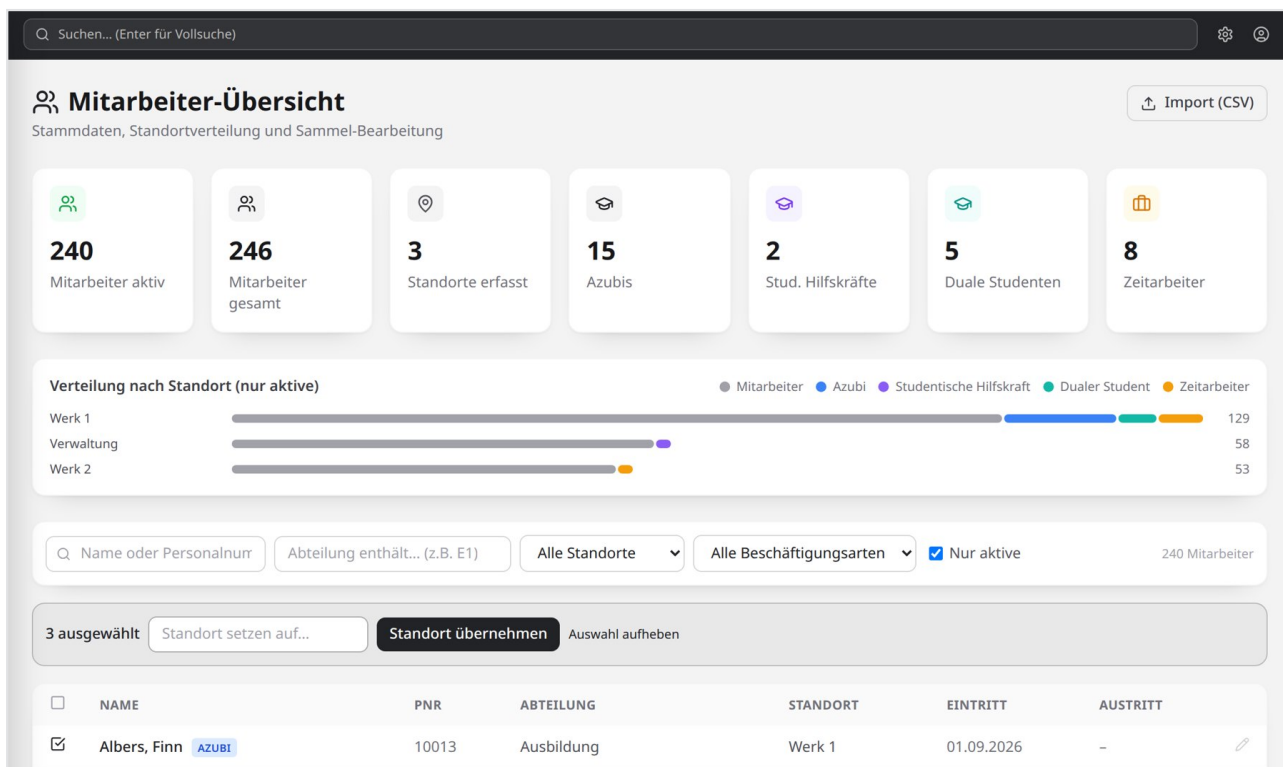


Abb. 40: Drei markierte Mitarbeiter, Leiste zum Setzen des Standorts

7.2 Eingruppierung

Die Seite Eingruppierung führt die Eingruppierungs-Historie je Mitarbeiter – Tarifgruppe und Stufe oder ein individuelles AT-Gehalt, jeweils mit „gültig ab“ und Bemerkung. Einträge, die aus einem Sitzungsbeschluss stammen, sind mit der Sitzung verknüpft.

Eingruppierung
Gehaltsstufen-Historie je Mitarbeiter

Import (CSV) Vorlage (CSV) + Neuer Eintrag

Überstunden Zeitmodell Liste Statistik

Filter: Alle Abteilungen Alle Mitarbeiter tt.mm.jjjj bis tt.mm.jjjj Alle Beschäftigungsarten

Nur aktive Mitarbeiter
518 Einträge gefunden

PNR	NAME	ABTEILUNG	GEHALTSSTUFE	GÜLTIG AB	BEMERKUNG
10019	Lange, Melanie	Produktion	Gruppe 3.1	01.11.2026	Höhergruppierung Schichtleitung Montage
10246	Hinrichs, Ali	Logistik	Gruppe 2.1	01.10.2026	Einstellung Lagerlogistik – Zustimmung BR
10245	Hofmann, Oliver	Konstruktion	Gruppe 4.1	01.10.2026	Einstellung Konstrukteur – Zustimmung BR

Abb. 41: Eingruppierung mit Historie und Bemerkungen

Die Seite hat vier Reiter: Überstunden und Zeitmodell (Kapitel 7.3), Liste und Statistik. In der Liste wird nach Abteilung, Mitarbeiter, Zeitraum und Beschäftigungsart gefiltert; „Neuer Eintrag“ erfasst eine Gehaltsstufe mit „gültig ab“. Das Personen-Symbol neben einem Namen öffnet dessen Stammdaten.

CSV-Import

„Vorlage (CSV)“ lädt eine leere Datei mit den richtigen Spalten herunter: PNR, Nachname, Vorname, Abteilung, Eintritt, Austritt, Gehaltsstufe, Gültig ab, Bemerkung. Ausgefüllt wird sie über „Import (CSV)“ eingelesen; eine Vorschau zeigt neue Mitarbeiter, neue Abteilungen und alle Einträge, bevor gespeichert wird. Einen Export der Gehaltsdaten gibt es bewusst nicht.

Sichtschutz

Sobald das Browserfenster den Fokus verliert – Wechsel in ein anderes Programm oder einen anderen Tab –, wird die Gehaltsliste unscharf geschaltet. Erst ein bewusster Klick auf „Ausgeblendet – klicken zum Anzeigen“ deckt sie wieder auf. So sieht niemand die Zahlen, der kurz ins Zimmer kommt oder über die Schulter schaut, wenn man gerade in ein anderes Fenster gewechselt ist.

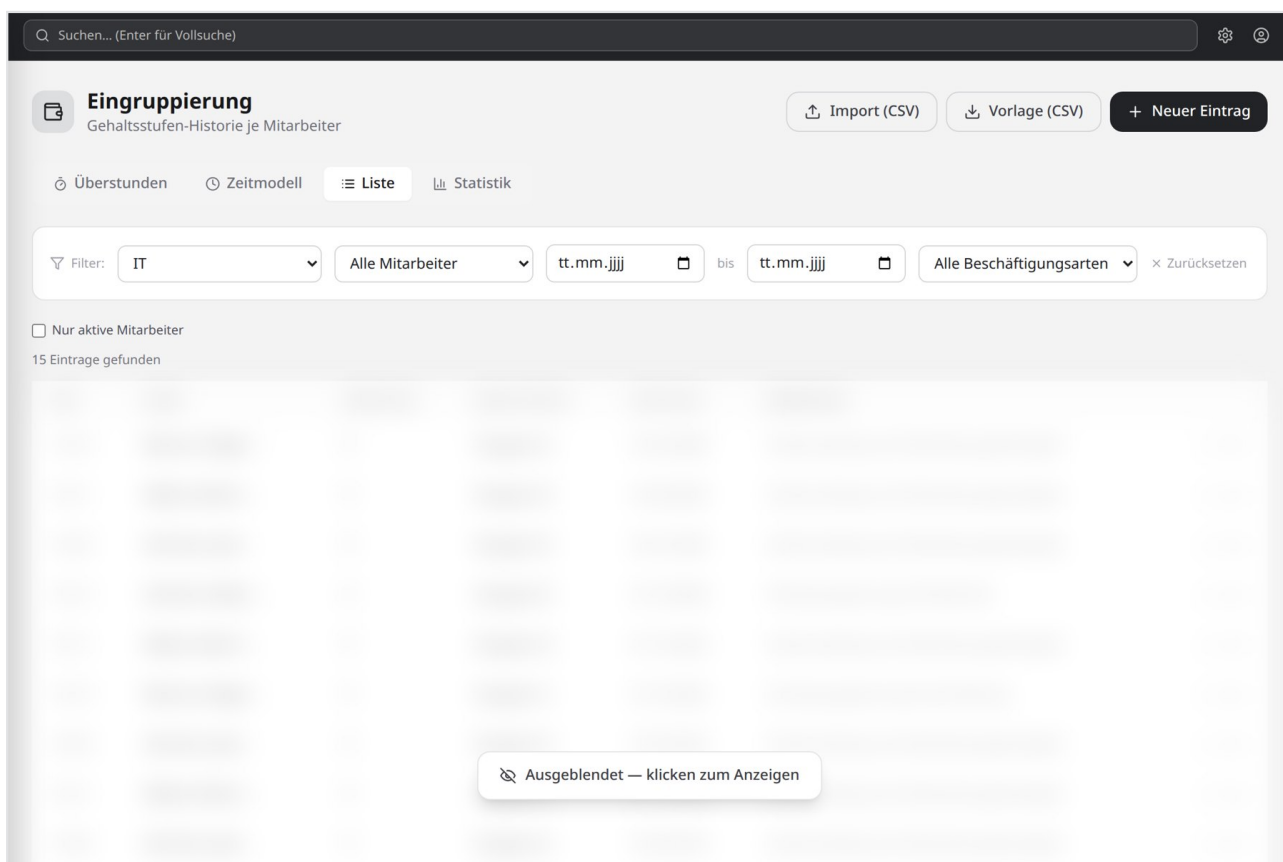


Abb. 42: Sichtschutz: Liste nach einem Fensterwechsel verdeckt

Der Reiter Statistik zeigt Kennzahlen (Mitarbeiter mit Gehaltseintrag, Zahl je Beschäftigungsart, AT-Fälle mit Durchschnittsgehalt) und Kreuztabellen: Gruppe × Stufe, Gruppe × Zeitmodell, Standort × Gruppe, Mitarbeiter je Werk sowie je Abteilung eine Matrix aus Gruppe und Stufe.

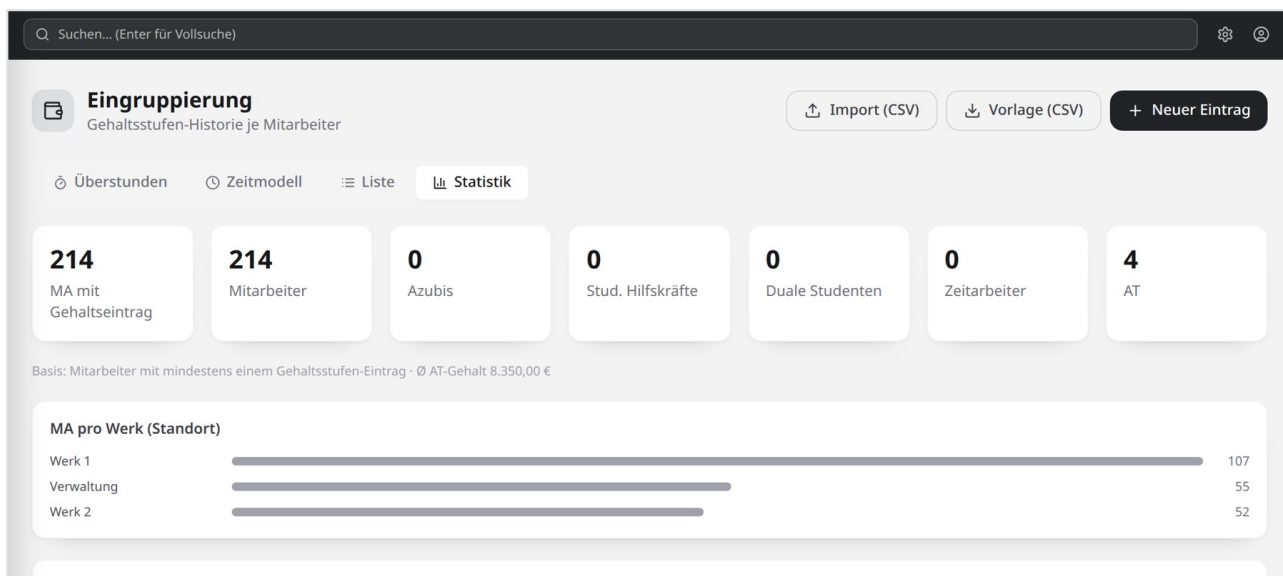


Abb. 43: Statistik: Verteilung nach Gruppe und Zeitmodell

7.3 Zeitmodelle und Überstunden

Zeitmodell und Überstundenregelung haben je eine eigene Historie mit echtem Gültigkeitszeitraum – von, bis oder unbefristet. Beide Reiter sind gleich aufgebaut: Filter nach Mitarbeiter, Abteilung und Beschäftigungsart, „Nur aktive“, und die Umschaltung zwischen Tabelle und Gantt. Die Gantt-Ansicht zeigt je Mitarbeiter einen Balken pro Zeitraum, gruppiert nach Abteilung; ein Doppelklick auf einen Balken öffnet ihn zum Bearbeiten. Eine Warnliste oben nennt Zeiträume, die in den nächsten 30 Tagen auslaufen.

Überstunden

Der erste Reiter der Eingruppierung. Mit „Neuer Zeitraum“ wird für einen Mitarbeiter festgehalten, welche Überstundenregelung ab wann gilt – als freier Text, z. B. „Gleitzeitkonto, Kappung bei 60 h“ oder „Mit AT-Gehalt pauschal abgegolten“, dazu eine Bemerkung.

Eingruppierung
Gehaltsstufen-Historie je Mitarbeiter

Import (CSV) Vorlage (CSV) + Neuer Eintrag

Überstunden Zeitmodell Liste Statistik

Alle Mitarbeiter Alle Abteilungen ☒ Nur aktive Alle Beschäftigungsarten

Tabelle Gantt + Neuer Zeitraum

NAME	REGELUNG	VON	BIS	BEMERKUNG
Schulze, Frank	Mit AT-Gehalt pauschal abgegolten	03.07.2026	unbefristet	-
Werner, Agnieszka	Auszahlung ab 20 h/Monat	12.05.2026	unbefristet	-
Peters, Thomas	Gleitzeitkonto, Kappung bei 60 h	08.05.2026	unbefristet	-
Hinrichs, Julia	Gleitzeitkonto, Kappung bei 60 h	15.02.2026	unbefristet	-

Abb. 44: Überstundenregelungen je Mitarbeiter in der Tabellenansicht

Zeitmodell

Hier wird das Arbeitszeitmodell (A, B, C oder D – was sich dahinter verbirgt, regelt die betriebliche Vereinbarung) mit Zeitraum geführt. Läuft ein Zeitmodell oder eine Überstundenregelung im laufenden Monat aus, erhalten Vorsitz und Stellvertretung am 15. eine Erinnerung (Kapitel 9.5).

Eingruppierung
Gehaltsstufen-Historie je Mitarbeiter

Import (CSV) Vorlage (CSV) + Neuer Eintrag

Überstunden **Zeitmodell** Liste Statistik

Alle Mitarbeiter Alle Abteilungen ☒ Nur aktive Befristet & unbefristet Alle Beschäftigungsarten A B C D

Tabelle Gantt + Neuer Zeitraum

	NAME	ZEITMODELL	VON	BIS	BEMERKUNG
☐	Hinrichs, Ali	A	01.10.2026	unbefristet	-
☐	Hofmann, Oliver	A	01.10.2026	unbefristet	-

Abb. 45: Zeitmodell-Historie mit Ablaufwarnung

7.4 Betriebsvereinbarungen

Das Register führt alle Betriebsvereinbarungen mit Status (aktiv, gekündigt, abgelöst, befristet ausgelaufen), Geltungsbereich und Laufzeitende. Vor Ablauf erscheint ein Warnhinweis; das hinterlegte PDF ist verknüpft und im Volltext durchsuchbar.

Betriebsvereinbarungen
Register aller BVs mit Status und Laufzeit

+ Neue BV

Filter: Volltextsuche (Titel, Geltungsbereich, Alle Status

6 Betriebsvereinbarungen

TITEL	ABSCHLUSS	GELTUNGSBEREICH	STATUS	LAUFZEITENDE	DOKUMENT
BV Arbeitszeit und Gleitzeit	01.07.2019	Alle Beschäftigten außer Schichtbetrieb	Aktiv	unbefristet	Betriebsvereinbarung Arbeitszeit und Gleitzeit

Abb. 46: Register der Betriebsvereinbarungen

7.5 Geschäftsordnung

Nach § 36 BetrVG gibt sich der Betriebsrat eine schriftliche Geschäftsordnung – meist zu Beginn der Amtszeit, mit Regeln zu Einladungsfrist, Sitzungsrhythmus, Video-Teilnahme oder Protokoll. Unter Dokumente & Wissen → Geschäftsordnung liegen alle Fassungen mit Beschlussdatum, Bemerkung und verknüpftem PDF. Die Fassung mit dem jüngsten Beschlussdatum ist als „Aktuell gültig“ markiert, ältere bleiben als Nachweis erhalten.

1 Neue Fassung erfassen

Das PDF der beschlossenen Geschäftsordnung zuerst unter Dokumente hochladen (Kategorie „Geschäftsordnung“, 10 Jahre Aufbewahrung).

2 Im Register eintragen

„Neue Fassung“: Beschlussdatum, kurze Bemerkung (z. B. was sich geändert hat) und das Dokument auswählen. Die bisherige Fassung rückt automatisch nach unten.

Lesen dürfen alle Mitglieder; anlegen, ändern und löschen nur Vorsitz und Stellvertretung. Ob der Beschluss wirksam zustande kam (Mehrheit der Mitglieder, § 36 BetrVG), prüft BR-DMS nicht – das Register ist reine Ablage.

BESCHLOSSEN AM	BEMERKUNG	DOKUMENT
21.05.2026 Aktuell gültig	Zu Beginn der Amtszeit neu beschlossen; Einladungsfrist auf 5 Arbeitstage verlängert, Regeln für Video-Teilnahme (§ 30 Abs. 2 BetrVG) ergänzt.	Geschäftsordnung des Betriebsrats (Fassung 2026)
19.05.2022	Abgelöst durch die Fassung 2026.	Geschäftsordnung des Betriebsrats (Fassung 2022)

Abb. 47: Geschäftsordnung mit aktueller und abgelöster Fassung

7.6 Schulungen und Qualifikationsmatrix

Schulungstermine werden mit Datum, Ort, Anbieter, Kosten, Status und Teilnehmenden erfasst. Daraus berechnet BR-DMS laufend die Qualifikationsmatrix – wer welche Qualifikation hat und wann sie abläuft (z. B. Ersthelfer alle 24 Monate). Kosten von BR-Schulungen erscheinen zusätzlich in der Kostenübersicht (Kapitel 5.6).

DATUM	QUALIFIKATION	ORT / ANBIETER	STATUS	TEILNEHMER	KOSTEN
06.11.2026	Ersthelfer/in	Schulungszentrum · DRK Kreisverband	Geplant	10	700.00 €
30.10.2026	BR-Grundlagen Teil 1	Schulungszentrum · ifb / W.A.F. Seminar	Geplant	2	2380.00 €

Abb. 48: Schulungstermine mit Status und Kosten

KAPITEL 8

Abläufe in der Praxis

8.1 Vom Dokument zum Protokoll

Der typische Weg einer Anhörung nach § 99 durch das System:

1**Dokument geht ein**

Per Upload oder automatisch über den Watch-Folder. Das System liest den Text aus, verschlüsselt die Datei, legt die Frist an und zeigt das Dokument im Eingang.

2**Sichten und zuordnen**

Der Vorsitz prüft Kategorie und Frist, vergibt bei Bedarf ein Aktenzeichen und verknüpft das Dokument mit einem TOP der nächsten Sitzung.

3**Vorbereiten**

Ein Mitglied erhält die Aufgabe, eine Stellungnahme vorzubereiten. Unterlagen hängen am TOP.

4**Einladen**

Die Tagesordnung wird fixiert; alle Mitglieder erhalten Einladung und PDF.

5**Beraten und beschließen**

In der Sitzung werden Anwesenheit, Beratungsergebnis und Beschluss mit Abstimmung erfasst.

6**Abschließen**

Frist erledigen, Ein- oder Umgruppierung in die Eingruppierung übernehmen, Protokoll finalisieren. Die Stellungnahme im Vorgang am Dokument vorbereiten, als Entwurf gegenlesen und versenden (Kapitel 3.4).

7**Aufbewahren und löschen**

Das Dokument bleibt für die Dauer der Aufbewahrungsfrist erhalten und wird danach automatisch zur Löschung vorgemerkt und sicher gelöscht.

8.2 Daily Business

Aufgabe	Wer	Wo im System
Eingang sichten	Vorsitz / Stellvertretung	Eingang
Fristen im Blick behalten	Vorsitz / Stellvertretung	Dashboard, Fristenkalender
Eigene Aufgaben bearbeiten	Alle	Aufgaben
Nachrichten lesen	Alle	Nachrichten
Kummerkasten bearbeiten	Zuständige Mitglieder	Kummerkasten
Ablaufende BVs und Zeitmodelle prüfen	Vorsitz	Betriebsvereinbarungen, Eingruppierung
Audit-Log prüfen	Vorsitz / Admin	Audit-Log
Backups kontrollieren	Admin	Einstellungen → System

TEIL II



Administration

Einstellungen, Benutzer, Design und Module – für Vorsitz und Admin. Dazu die vollständige Übersicht der Rollen und Berechtigungen.

KAPITEL 9

Einstellungen

Die Einstellungen erreichen Sie über das Zahnrad oben rechts im Kopfbalken. Welche Reiter sichtbar sind, hängt von der Rolle ab.

Reiter	Inhalt
Löschfristen	Aufbewahrungsfristen je Dokumentkategorie, Test der Erinnerungsmails
Protokoll-Layout	Kopf- und Fußzeile, Farbe, Logo und Unterschriftenzeilen der PDFs
Benutzerverwaltung	Benutzer, Rollen, Wahlrang, ständige Vertretung, Geschlechterquote, Zugriff des Admins
Design	Farbschema, Schriftgröße, Hell/Dunkel
System	E-Mail-Absender, Watch-Folder, Backup-Übersicht, automatisches Abmelden, Gefahrenzone (Admin)
Module	Optionale Bereiche ein- und ausschalten (nur Admin)
Gesetzestexte	Stand der Gesetzesdatenbank, manuelles Aktualisieren (nur Admin)
Amtsübergabe	PDF mit Mitgliederliste, aktiven Dokumenten und Beschlussregister

9.1 Benutzer und Gremium

Hier werden die Zugänge angelegt. Für die Nachrück-Logik werden zusätzlich Geschlecht und Wahlrang aus dem Wahlprotokoll hinterlegt sowie Minderheitengeschlecht und Mindestsitze nach § 15 Abs. 2 BetrVG. Ein Ersatzmitglied kann einem Mitglied als ständige Vertretung zugeordnet werden.

Q Suchen... (Enter für Vollsuche) ⚙️ 👤

⚙️ Einstellungen

🕒 Löschfristen 📄 Protokoll-Layout 👤 **Benutzerverwaltung** 🎨 Design 📁 System ⬇️ Amtsübergabe

Zugriff des Admins auf Inhalte

Betreut jemand außerhalb des Gremiums die Technik (z. B. die IT), kann der Admin auf die Verwaltung beschränkt werden: Benutzer, Einstellungen, Module und Gesetzestexte. Sitzungen, Dokumente, Personaldaten, Aufgaben und das Audit-Log sind dann für ihn gesperrt. Nur Vorsitz und Stellvertretung können das ändern.

☒ **Voller Zugriff** – Der Admin sieht alles, wie Vorsitz (Standard).

☐ **Nur technische Verwaltung** – Der Admin sieht keine Inhalte des Gremiums.

Geschlechterquote (§15 Abs. 2 BetrVG)

Werte aus dem Wahlprotokoll der letzten BR-Wahl. Wird beim automatischen Ersatzmitglieder-Vorschlag in Sitzungen nur als Warnung angezeigt, nie blockierend.

Minderheitengeschlecht Weiblich Mindestsitze 3 Speichern

Abb. 49: Benutzerverwaltung mit Geschlechterquote und Wahlrang

- **Anlegen** – Name, E-Mail, Rolle; das Passwort wird beim ersten Login geändert
- **Deaktivieren** – Zugang sperren, ohne Historie zu verlieren

- **Passwort zurücksetzen** – Durch Vorsitz oder Admin, alternativ per E-Mail-Link durch die Person selbst
- **Adresse für Einladungen** – Zweitadresse unter der E-Mail (z. B. br-name@...); leer = Hauptadresse. Angemeldet wird immer mit der Hauptadresse. Beide Adressen kann jede Person auch selbst unter „Mein Konto“ ändern
- **Zwei-Faktor-Anmeldung** – Ein Schild neben „Aktiv“ zeigt, wer sie eingerichtet hat (nur für Vorsitz, Stellvertretung und Admin sichtbar). „2FA reset“ entfernt sie, z. B. bei verlorenem Handy; die Person wird abgemeldet und meldet sich danach mit dem Passwort an

9.2 Zugriff des Admins auf Inhalte

Standardmäßig darf der Admin alles, was auch der Vorsitz darf. Betreut jemand außerhalb des Gremiums die Technik – etwa die IT-Abteilung –, stellen Vorsitz oder Stellvertretung unter Benutzerverwaltung auf „Nur technische Verwaltung“ um. Der Admin selbst kann diese Einstellung nicht ändern; jede Änderung steht im Audit-Log.

Der Admin ...	Nur technische Verwaltung
verwaltet Benutzer, Einstellungen, Design, Module	Ja
aktualisiert Gesetzestexte, sieht Backups	Ja
liest und schreibt eigene Nachrichten	Ja
sieht Sitzungen, Dokumente, Fristen, Aufgaben, Wahlen	Nein
sieht Mitarbeiter, Eingruppierung, Betriebsvereinbarungen	Nein
sieht Audit-Log, Suche, Amtsübergabe	Nein
setzt Passwörter anderer zurück, ändert die eigene Rolle	Nein

Suchen... (Enter für Vollsuche)

Einstellungen

🕒 Löschfristen
📄 Protokoll-Layout
👤 **Benutzerverwaltung**
🎨 Design
📁 System
🔧 Module
📖 Gesetzestexte
📄 Amtsübergabe

Zugriff des Admins auf Inhalte

Betreut jemand außerhalb des Gremiums die Technik (z. B. die IT), kann der Admin auf die Verwaltung beschränkt werden: Benutzer, Einstellungen, Module und Gesetzestexte. Sitzungen, Dokumente, Personaldaten, Aufgaben und das Audit-Log sind dann für ihn gesperrt. Festgelegt von Vorsitz oder Stellvertretung.

☒ **Voller Zugriff** – Der Admin sieht alles, wie Vorsitz (Standard).
 ☐ **Nur technische Verwaltung** – Der Admin sieht keine Inhalte des Gremiums.

Geschlechterquote (§15 Abs. 2 BetrVG)

Werte aus dem Wahlprotokoll der letzten BR-Wahl. Wird beim automatischen Ersatzmitglieder-Vorschlag in Sitzungen nur als Warnung angezeigt, nie blockierend.

Minderheitengeschlecht Weiblich
 Mindestsitze 3
Speichern

Abb. 50: Ansicht des Admins ohne Inhaltszugriff

Grenzen

Neue Benutzerkonten darf der Admin weiter anlegen – sonst könnte er seine Aufgabe nicht erfüllen. Damit er sich nicht unbemerkt ein Zweitkonto mit Gremiumsrolle anlegt, erhalten Vorsitz und Stellvertretung bei jedem neuen Konto eine Nachricht. Wer Zugriff auf Server oder Datenbank hat, kann technisch immer an die Daten – die Einstellung regelt den Zugang über die Anwendung.

9.3 Design

Ein Klick auf ein Farbschema setzt alle Farben auf einmal; „Board“ ist der Standard, „Board Rot“ nutzt die rote Akzentfarbe. Einzelne Farben, Schriftgröße und Hell-/Dunkelmodus lassen sich anpassen. Das Design gilt für alle Benutzer und auch auf der Anmeldeseite und im Kummerkasten.

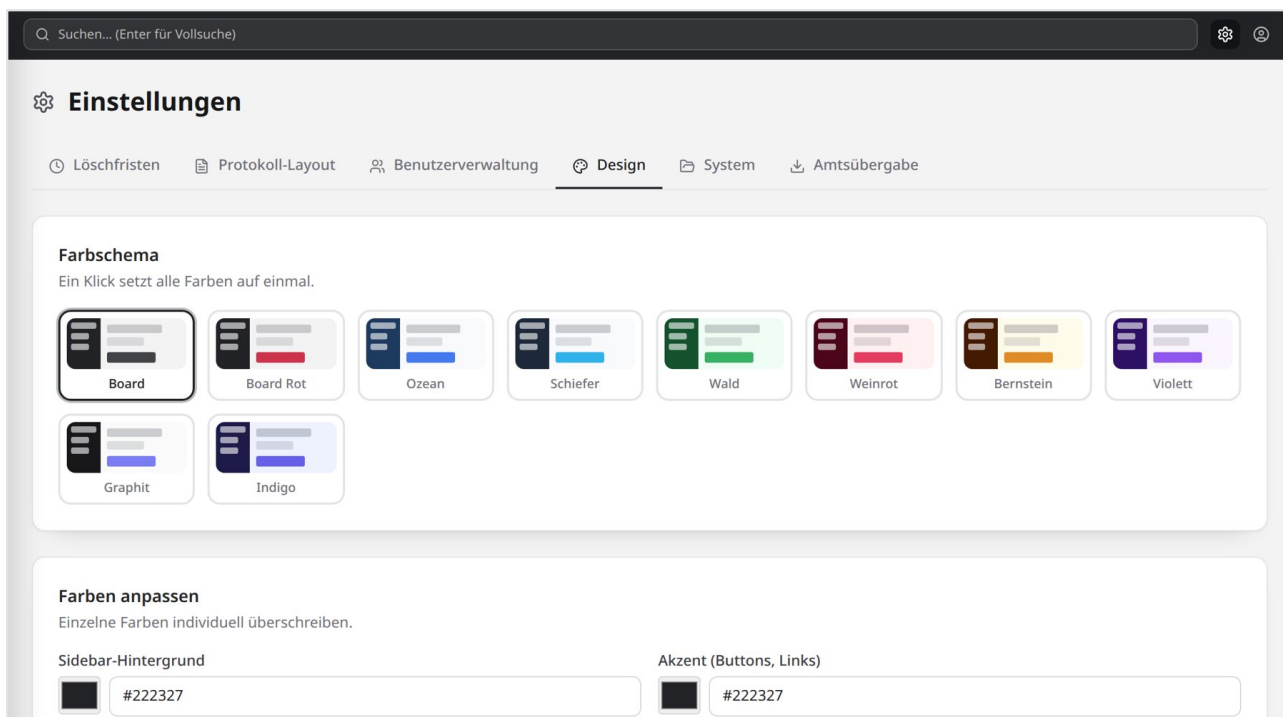


Abb. 51: Design-Einstellungen mit Farbschemata

9.4 Module

Nicht jeder Betriebsrat braucht alles. Diese Bereiche lassen sich abschalten; sie verschwinden dann aus der Seitenleiste, Direktaufrufe führen zum Dashboard. Die Daten bleiben erhalten.

Modul	Umfasst
Personalverwaltung	Mitarbeiter, Eingruppierung, Zeitmodelle, Überstunden, Schulungen
Betriebsvereinbarungen	Das BV-Register
Gremien	Andere Gremien, Mitglieder, Fremdprotokolle
Wissensarchiv	Wissenseinträge
Ressourcen	Linksammlung

Modul	Umfasst
Themensammlung	Export öffentlicher TOPs
Kosten (§ 40)	Jahresübersicht der BR-Kosten mit Export

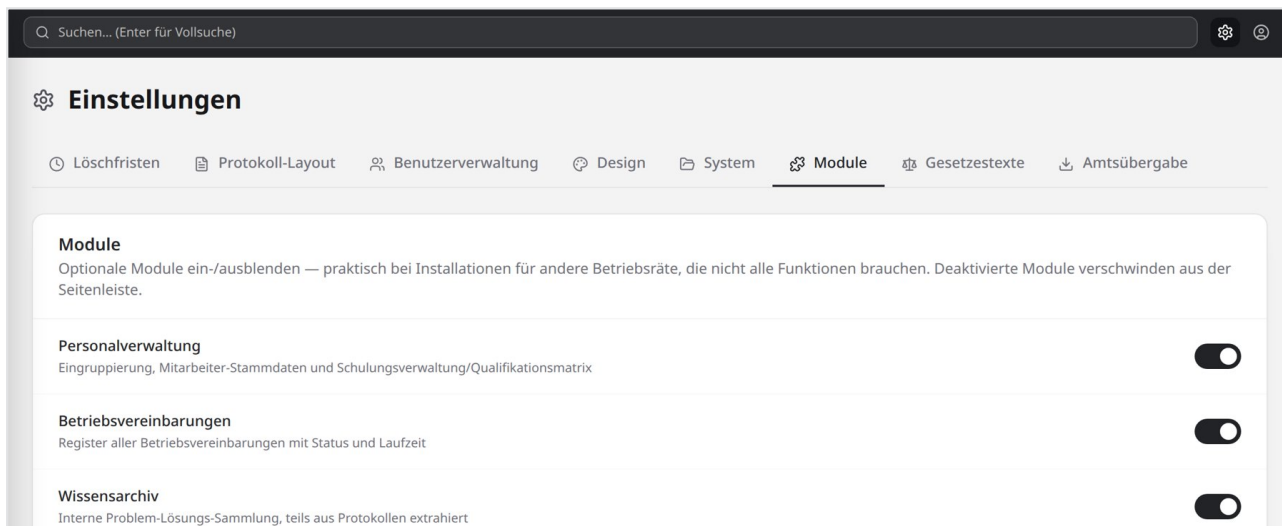


Abb. 52: Module ein- und ausschalten (Admin)

9.5 Löschfristen und Erinnerungsmails

Der Reiter legt je Dokumentkategorie fest, nach wie vielen Tagen ein Dokument zur Löschung vorgemerkt wird; „Bearbeiten“ in der Zeile ändert die Frist, „Angepasst“ zeigt Abweichungen vom Standard. Änderungen gelten nur für neu hochgeladene Dokumente – bestehende behalten ihr Löschdatum, das sich je Dokument im Bearbeiten-Dialog ändern lässt.

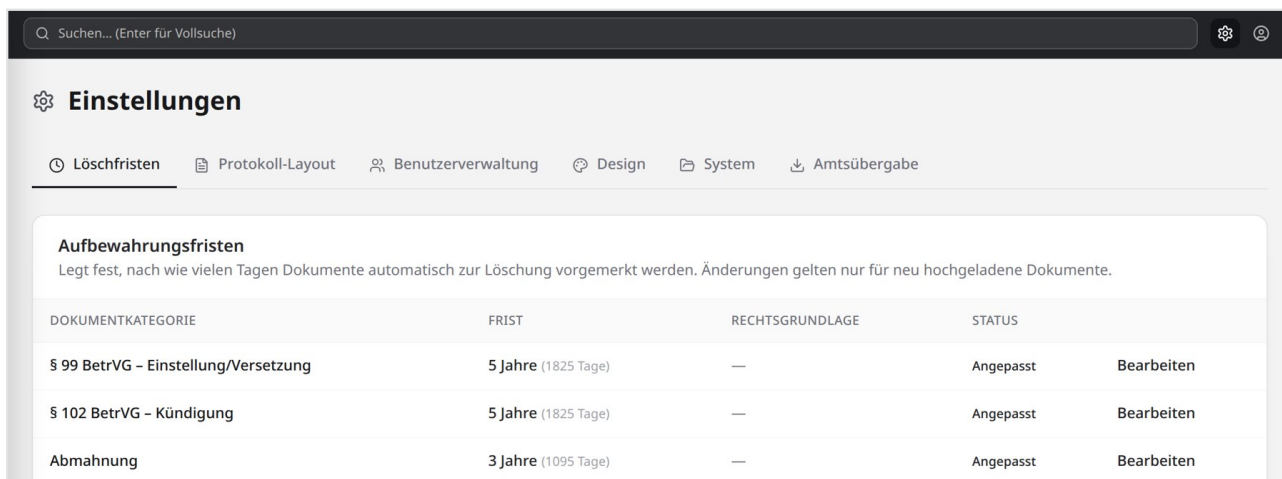


Abb. 53: Aufbewahrungsfristen je Dokumentkategorie

Kategorie	Standard-Aufbewahrung
Anhörung § 99 / § 102	5 Jahre
Abmahnung	3 Jahre
Bewerbung	90 Tage

Kategorie	Standard-Aufbewahrung
Bewerbung (Alternativ)	30 Tage
Zeitmodell § 87	5 Jahre
Information des Arbeitgebers, Arbeitsschutz, Schriftverkehr	5 Jahre
Protokoll	4 Jahre
Betriebsvereinbarung	10 Jahre
Sonstiges	5 Jahre

Darunter stehen zwei Erinnerungsmails, die das System selbst verschickt. Mit „Jetzt testen“ lässt sich jede sofort auslösen, statt auf den nächsten Termin zu warten:

- **Fristen-Erinnerung** – Täglich um 7:00 Uhr an Vorsitz und Stellvertretung, aber nur, wenn in den nächsten 7 Tagen Fristen fällig werden
- **Zeitmodell-/Überstunden-Ablauf** – Monatlich am 15. um 7:00 Uhr, wenn im laufenden Monat Zeiträume auslaufen

Die tägliche Fristen-Erinnerung lässt sich mit dem Schalter „Automatischer Versand“ pausieren, etwa während der Betriebsferien. „Jetzt testen“ funktioniert auch im pausierten Zustand.

9.6 Protokoll-Layout

Hier wird das Aussehen der Sitzungs-PDFs festgelegt – Tagesordnungen, Einladungen, Protokolle und Niederschriften. Bestehende PDFs behalten ihr Aussehen, bis sie in der Sitzung neu generiert werden (Kapitel 4.4).

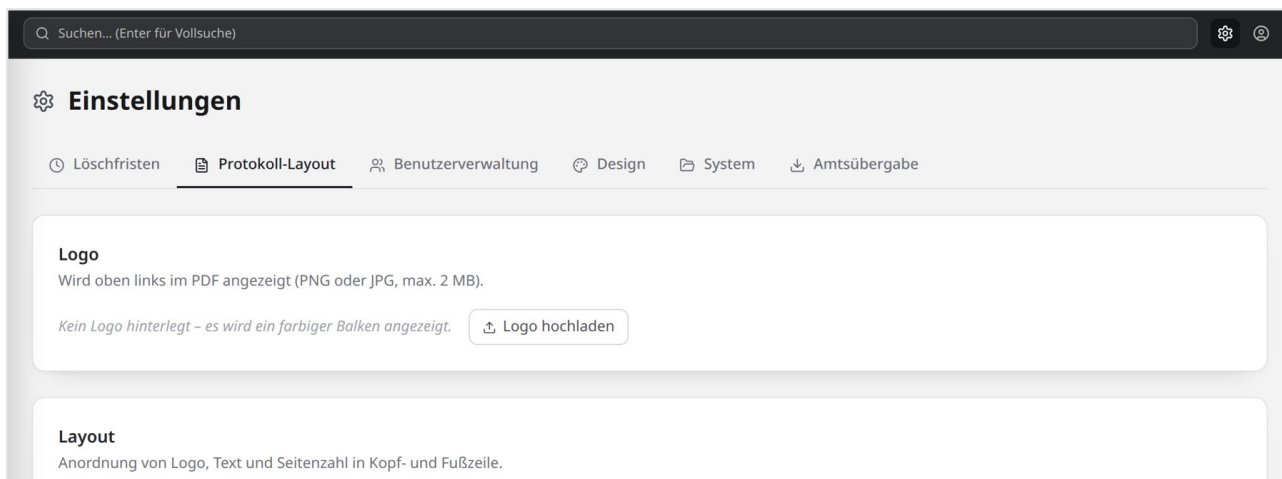


Abb. 54: Logo und Anordnung von Kopf- und Fußzeile

- **Logo** – PNG oder JPG bis 2 MB; ohne Logo erscheint ein farbiger Balken
- **Layout** – Logo links, rechts oder kein Logo; in der Fußzeile Bezeichnung links und Seitenzahl rechts oder umgekehrt
- **Kopfzeile & Farbe** – Kopfzeile groß (z. B. „Betriebsrat“), Unterzeile klein (z. B. die Firma) und die Akzentfarbe
- **Fußzeile & Unterschriften** – Fußzeilentext, Bezeichnung der Unterschriftenzeilen für Vorsitz und

Zeuge/Zeugin sowie der Ort vor dem Datum (leer = nur Datum)

9.7 System

Suchen... (Enter für Vollsuche)

Einstellungen

🕒 Löschfristen 📄 Protokoll-Layout 👤 Benutzerverwaltung 🎨 Design 📁 **System** 📄 Amtsübergabe

E-Mail-Absender
 Von dieser Adresse gehen Einladungen, Fristen-Erinnerungen und Passwort-Links raus. Der Mailserver muss das SMTP-Konto für diese Adresse freigeben – das richtet die IT ein.

Es ist kein Mailserver eingerichtet (SMTP_HOST in der .env) – es werden keine Mails verschickt.

Betriebsrat Nordwerk betriebsrat@nordwerk-demo.lokal

Betriebsrat Nordwerk · Werk 1, Raum 104
 Tel. 0123 456-78

Speichern

Abb. 55: E-Mail-Absender und Watch-Folder

- **E-Mail-Absender** – Name und Adresse für alle Mails (ohne Eintrag gilt SMTP_FROM) und die Signatur unter Einladungen. Ein Hinweis erscheint, solange kein Mailserver eingerichtet ist
- **Watch-Folder** – Ob die Ordnerüberwachung läuft, der Basispfad, welcher Unterordner zu welcher Kategorie gehört (Kapitel 12.6) und die letzten Importe mit Fehlermeldung
- **Backup & Restore** – Anzahl, Alter, Größe und Vollständigkeit der Backups; dazu die Hinweise zum Schlüssel und zur Wiederherstellung (Kapitel 13.2)
- **Sicherheit** – Automatisches Abmelden nach 0 bis 480 Minuten Inaktivität (0 = aus)
- **Zwei-Faktor-Anmeldung (nur Admin)** – „Aus“ (Standard) oder „An“; bei „An“ zusätzlich die Rollen, für die sie Pflicht ist

Ersetzt dabei die komplette aktuelle Datenbank — vorher sicherstellen, dass das wirklich gewollt ist.

Sicherheit
 Meldet inaktive Benutzer automatisch ab (kein Klick/Tastendruck/Scrollen). 0 = deaktiviert.

Automatisch abmelden nach Minuten Inaktivität **Speichern**

Zwei-Faktor-Anmeldung
 Zusätzlich zum Passwort ein 6-stelliger Code aus einer Authenticator-App. Eingerichtet wird sie von jeder Person selbst unter „Mein Konto“ (Klick auf den eigenen Namen).

☒ **Aus** – Niemand wird nach einem Code gefragt – auch wer ihn schon eingerichtet hat.

☐ **An** – Jede Person kann sie einrichten; für die unten gewählten Rollen ist sie Pflicht.

Speichern

Abb. 56: Zwei-Faktor-Anmeldung: aus, an und Pflicht je Rolle

„Aus“ heißt wirklich aus: Niemand wird nach einem Code gefragt, auch wer ihn schon eingerichtet hat – eine Installation ohne Diensthandys merkt von der Funktion nichts. Bei „An“ kann jede Person sie unter „Mein Konto“ einrichten; für die angehakten Rollen ist sie Pflicht und wird bei der nächsten Anmeldung verlangt. Unterstützt wird jede Authenticator-App nach dem TOTP-Standard (z. B. Microsoft oder Google

Authenticator, FreeOTP); BR-DMS braucht dafür keine Verbindung ins Internet.

Gefahrenzone – Eingruppierung

Nur für den Admin. „Nur Gehaltsstufen-Einträge löschen“ entfernt alle Gehaltsstufen, Mitarbeiter und Abteilungen bleiben – gedacht für einen fehlerhaften Import. „Eingruppierung komplett löschen“ entfernt zusätzlich alle Mitarbeiter und Abteilungen, etwa für einen Neustart nach Testdaten. Beide Knöpfe werden erst aktiv, wenn „LÖSCHEN“ einge tippt ist, und sind nicht umkehrbar.

Ersetzt dabei die komplette aktuelle Datenbank — vorher sicherstellen, dass das wirklich gewollt ist.

Sicherheit
Meldet inaktive Benutzer automatisch ab (kein Klick/Tastendruck/Scrollen). 0 = deaktiviert.

Automatisch abmelden nach Minuten Inaktivität **Speichern**

Zwei-Faktor-Anmeldung
Zusätzlich zum Passwort ein 6-stelliger Code aus einer Authenticator-App. Eingerichtet wird sie von jeder Person selbst unter „Mein Konto“ (Klick auf den eigenen Namen).

☒ Aus – Niemand wird nach einem Code gefragt – auch wer ihn schon eingerichtet hat.
☐ An – Jede Person kann sie einrichten; für die unten gewählten Rollen ist sie Pflicht.

Speichern

⚠ Gefahrenzone – Eingruppierung
Nur für Admins. Beide Aktionen können nicht rückgängig gemacht werden. Es gibt bewusst keinen Daten-Export aus der App (siehe unten) – vorher ggf. ein reguläres Datenbank-Backup ziehen (`./backup.sh` , siehe oben).

Nur Gehaltsstufen-Einträge löschen
Löscht alle Gehaltsstufen-Einträge (z.B. um nach einem fehlerhaften Import mit inkonsistenter Stufen-Schreibweise neu zu importieren). Mitarbeiter und Abteilungen bleiben erhalten.

"LÖSCHEN" eintippen zum Freischa **Nur Einträge löschen**

Eingruppierung komplett löschen
Löscht alle Gehaltsstufen-Einträge, Mitarbeiter UND Abteilungen unwiderruflich. Für einen kompletten Neustart, z.B. nach Testdaten.

"LÖSCHEN" eintippen zum Freischa **Alles löschen**

Abb. 57: Gefahrenzone mit Bestätigung durch Eintippen

Vorher sichern

Vor dem Löschen ein Datenbank-Backup ziehen (`./backup.sh`, Kapitel 13.2) – aus der App heraus gibt es bewusst keinen Export der Gehaltsdaten.

9.8 Gesetzestexte

Nur für den Admin. Die Tabelle zeigt je Gesetz die Zahl der Paragraphen und den Stand des letzten Imports von `gesetze-im-internet.de`. Der Import läuft automatisch am 1. jedes Monats um 3:00 Uhr; „Jetzt aktualisieren“ startet ihn sofort. „Automatischen Ablauf testen“ führt genau den nächtlichen Ablauf aus – einschließlich der Nachricht an Vorsitz und Stellvertretung, falls sich an einem bereits bekannten Paragraphen wirklich etwas geändert hat.

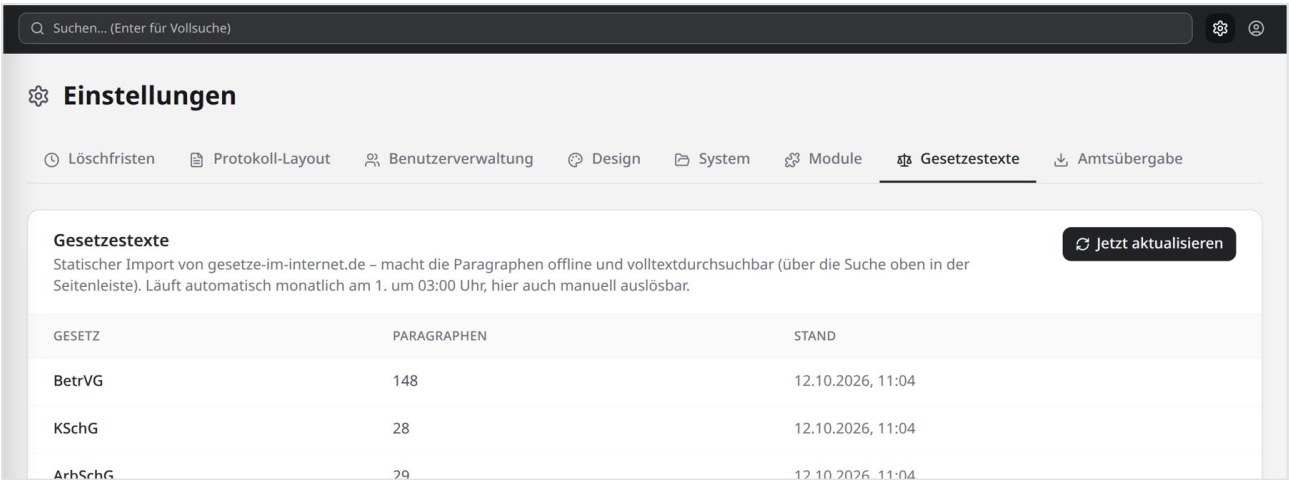


Abb. 58: Stand der Gesetzestexte

9.9 Amtsübergabe

Für Vorsitz, Stellvertretung und Admin. „PDF öffnen“ erzeugt eine lesbare Übersicht als Grundlage für das Übergabegespräch an eine neue Vorsitzende oder einen neuen Vorsitzenden – kein vollständiger Datenexport.

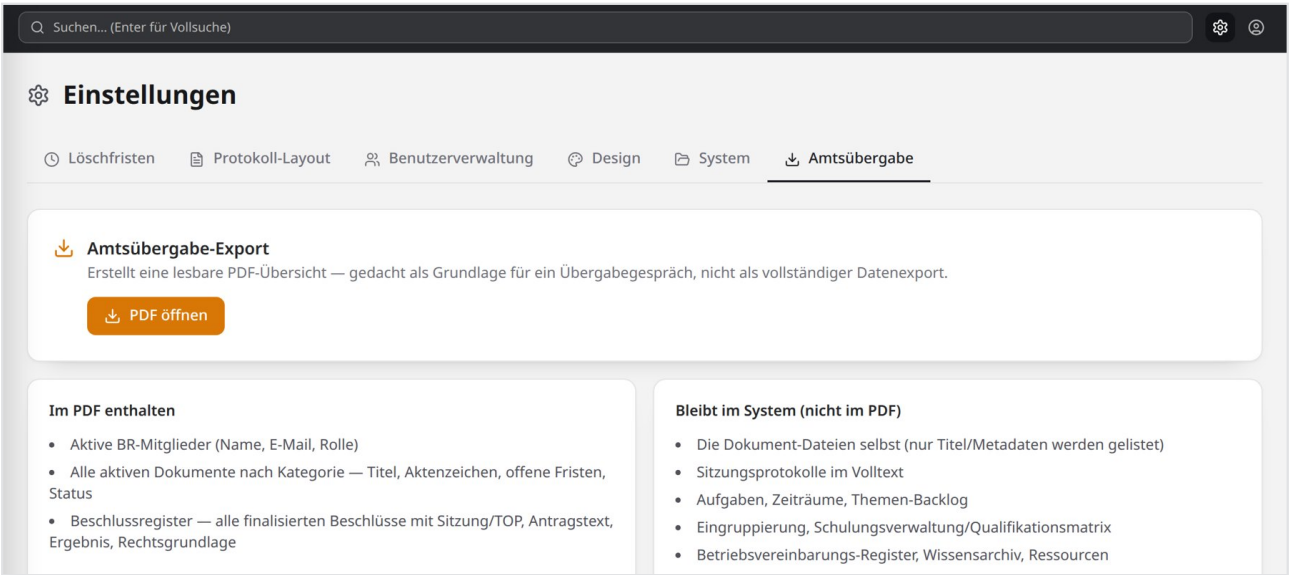


Abb. 59: Amtsübergabe: Inhalt des PDFs und Ablauf

Im PDF enthalten	Bleibt im System
Aktive BR-Mitglieder mit E-Mail und Rolle	Dokument-Dateien selbst (nur Titel und Metadaten im PDF)
Aktive Dokumente nach Kategorie mit Aktenzeichen, offenen Fristen und Status	Protokolle im Volltext
Beschlussregister mit Sitzung/TOP, Antrag, Ergebnis und Rechtsgrundlage	Aufgaben, Themen-Backlog, Eingruppierung, Schulungen, BVs, Wissen, Audit-Log

1 Neue Zugänge anlegen

Neue/n Vorsitzende/n bzw. Stellvertretung in der Benutzerverwaltung mit passender Rolle anlegen.

2 Übergabe besprechen

Dieses PDF exportieren und im Übergabegespräch gemeinsam durchgehen.

3 Alte Zugänge deaktivieren

Ausscheidende deaktivieren, nicht löschen – die Historie bleibt nachvollziehbar.

4 Technik separat übergeben

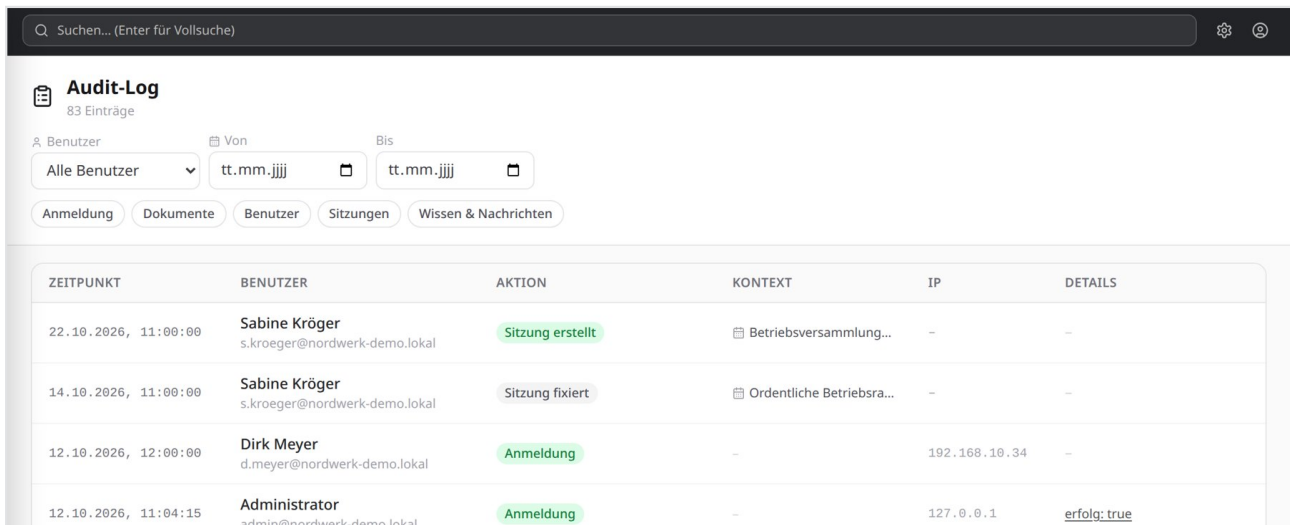
NAS-Zugang, Docker und Datenbank-Zugangsdaten liegen außerhalb der App und werden sicher getrennt weitergegeben.

5 Sichern

Für eine vollständige technische Sicherung ein Datenbank-Backup erstellen (Kapitel 13.2).

9.10 Audit-Log

Das Audit-Log protokolliert unveränderlich alle sicherheitsrelevanten Vorgänge – Anmeldungen, Dokumentzugriffe, Änderungen an Sitzungen, Benutzern und Einstellungen – mit Zeitpunkt, Person, IP-Adresse und Browser. Einsehbar für Vorsitz, Stellvertretung und Admin, filterbar nach Person, Aktion und Zeitraum.



The screenshot shows the 'Audit-Log' interface with 83 entries. It includes filters for 'Benutzer' (Alle Benutzer), 'Von' (tt.mm.jjjj), and 'Bis' (tt.mm.jjjj). Below the filters are tabs for 'Anmeldung', 'Dokumente', 'Benutzer', 'Sitzungen', and 'Wissen & Nachrichten'. The table below displays log entries with columns: ZEITPUNKT, BENUTZER, AKTION, KONTEXT, IP, and DETAILS.

ZEITPUNKT	BENUTZER	AKTION	KONTEXT	IP	DETAILS
22.10.2026, 11:00:00	Sabine Kröger s.kroeger@nordwerk-demo.lokal	Sitzung erstellt	Betriebsversammlung...	-	-
14.10.2026, 11:00:00	Sabine Kröger s.kroeger@nordwerk-demo.lokal	Sitzung fixiert	Ordentliche Betriebsra...	-	-
12.10.2026, 12:00:00	Dirk Meyer d.meyer@nordwerk-demo.lokal	Anmeldung	-	192.168.10.34	-
12.10.2026, 11:04:15	Administrator admin@nordwerk-demo.lokal	Anmeldung	-	127.0.0.1	erfolg: true

Abb. 60: Audit-Log mit Filtern

KAPITEL 10

Rollen & Berechtigungen

Jede Aktion wird im Backend gegen die Rolle geprüft – auch wenn jemand versucht, eine Seite direkt aufzurufen. Die Tabelle zeigt die wichtigsten Rechte.

Berechtigung	Vorsitz	Stellv.	Mitglied	Ersatz	JAV	SBV	Admin
Dokumente lesen	Ja	Ja	Ja	Ja	–	–	Ja
Dokumente hochladen und bearbeiten	Ja	Ja	Ja	Vertr.	–	–	Ja
Vertrauliche Dokumente anderer	Ja	Ja	–	–	–	–	Ja
Eingang bearbeiten	Ja	Ja	–	–	–	–	Ja
Sitzungen und Protokolle lesen	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Vertrauliche TOPs sehen	Ja	Ja	Ja	Ja	–	–	Ja
TOPs bearbeiten	Ja	Ja	Ja	Vertr.	–	–	Ja
Sitzung anlegen, fixieren, finalisieren	Ja	Ja	–	–	–	–	Ja
Beschlüsse erfassen und finalisieren	Ja	Ja	–	–	–	–	Ja
Eingruppierung bearbeiten	Ja	Ja	Ja	Vertr.	–	–	Ja
Mitarbeiter- und Wählerliste einsehen, Mitarbeiter anlegen	Ja	Ja	Ja	Vertr.	–	–	Ja
Mitarbeiter-Stammdaten ändern, importieren, löschen	Ja	Ja	–	–	–	–	Ja
Kummerkasten lesen und bearbeiten	Ja	Ja	Ja	Ja	–	–	Ja
Betriebsvereinbarungen anlegen	Ja	Ja	–	–	–	–	Ja
Geschäftsordnung pflegen	Ja	Ja	–	–	–	–	Ja
Kostenübersicht (§ 40) einsehen	Ja	Ja	Ja	Vertr.	–	–	Ja
Kosten eintragen und ändern	Ja	Ja	–	–	–	–	Ja
Gremien, Mitglieder und Fremdprotokolle verwalten	Ja	Ja	–	–	–	–	Ja
Benutzer verwalten, Design ändern	Ja	Ja	–	–	–	–	Ja
Audit-Log einsehen	Ja	Ja	–	–	–	–	Ja
Module ein-/ausschalten	–	–	–	–	–	–	Ja

„Vertr.“ = nur solange das Ersatzmitglied aktiv als Vertretung eingetragen ist, sonst lesend – Mitarbeiter- und Wählerliste mit ihren Personaldaten sieht es ohne aktive Vertretung gar nicht. Die Rollen JAV und SBV

dürfen ausschließlich Sitzungen und Protokolle lesen. Beide nehmen an Sitzungen beratend teil (§ 67 BetrVG, § 178 Abs. 4 SGB IX), werden automatisch geladen, in Einladung, Unterschriftenliste und Sitzungspaket als eigene Gruppe geführt und sehen in der Sidebar nur „Sitzungen“. Vertrauliche TOPs bleiben für sie überall verborgen – auch Beschlüsse, Abstimmung und TOP-Auszug dazu. Das vollständige Protokoll-PDF und das Sitzungspaket erhalten sie nur für Sitzungen ohne vertrauliche TOPs.

Admin gehört nicht zum Gremium: Er taucht nicht auf Anwesenheitslisten auf und nimmt nicht an Abstimmungen teil. Die Spalte zeigt den Standard – haben Vorsitz oder Stellvertretung den Admin auf die technische Verwaltung beschränkt, gilt für ihn bei allen Inhalten „–“ (Kapitel 9.2).

TEIL III



Technik

Architektur, Sicherheit, Installation, Betrieb und Datenbank – für die technische Betreuung der Installation.

KAPITEL 11

Architektur & Sicherheit

11.1 Aufbau

BR-DMS besteht aus vier Docker-Containern in einem eigenen Netz. Von außen erreichbar ist ausschließlich der HTTPS-Proxy; Frontend, Backend und Datenbank haben keine eigenen Ports.

Container	Technologie	Aufgabe
proxy	Nginx 1.30	TLS-Terminierung, einziger Zugang (Port 8443, 8080 leitet um); läuft im Netz des Hosts, damit das Audit-Log die echte Adresse des Arbeitsplatzes sieht
frontend	React 18, Vite, Tailwind CSS (über Nginx)	Benutzeroberfläche im Browser; nur lokal auf dem Host erreichbar (127.0.0.1:18080)
backend	Node.js 24, Fastify 5, Prisma	REST-API, Geschäftslogik, PDF-Erzeugung, Hintergrundjobs
postgres	PostgreSQL 16	Datenhaltung, nur im internen Docker-Netz

Hintergrundjobs im Backend erinnern an Fristen, legen Wiedervorlagen zurück in den Eingang, warnen vor ablaufenden Regelungen, aktualisieren monatlich die Gesetzestexte und löschen Dokumente nach Ablauf der Aufbewahrungsfrist.

11.2 Sicherheit

BR-DMS schützt die Daten in mehreren Schichten: Netz und Container, Anmeldung und Rechte in der Anwendung, Verschlüsselung der Daten und verschlüsselte Backups. Dazu kommt, was organisatorisch geregelt sein muss – denn wer den Server selbst verwaltet, steht technisch über jeder Anwendung.

Netz und Container

Mechanismus	Umsetzung
Ein einziger Zugang	Nur der Proxy (Nginx) hat Ports zum Host: HTTPS (Standard 8443) und HTTP, das ausschließlich auf HTTPS umleitet. Frontend, Backend und Datenbank haben keine eigenen Ports
Datenbank abgeschottet	PostgreSQL ist nur im internen Docker-Netz von BR-DMS erreichbar, nicht vom NAS oder aus dem Firmennetz
Transport	TLS 1.2 und 1.3; eigenes Zertifikat (selbstsigniert oder von der Firmen-CA, Kapitel 12.4)
Intranet-Betrieb	Gedacht für das interne Netz; eine Freigabe ins Internet ist nicht vorgesehen
Ohne Root-Rechte	Das Backend läuft als eigener, nicht privilegierter Benutzer (PUID/PGID)
Nur lesend eingebunden	Zertifikate, Proxy-Konfiguration und Backup-Ordner sind im Container schreibgeschützt eingebunden

Anmeldung und Rechte

Mechanismus	Umsetzung
Passwörter	scrypt-Hash mit Salt, mindestens 8 Zeichen; Vergleich in konstanter Zeit
Anmeldeversuche	Höchstens 10 Versuche in 10 Minuten, danach gesperrt
Sitzungsdauer	Token 24 Stunden („eingeloggt bleiben“) bzw. 1 Stunde; automatisches Abmelden nach Inaktivität einstellbar (Kapitel 9.7)
Abmelden	Abmelden und jeder Passwortwechsel (selbst, per Link oder durch den Vorsitz) machen alle ausgestellten Tokens sofort ungültig – auch auf anderen Rechnern
Zwei-Faktor	Optional Einmalcode per Authenticator-App (TOTP), Pflicht je Rolle einstellbar (Kapitel 9.7); Schlüssel verschlüsselt gespeichert, jeder Code gilt nur einmal, 10 Wiederherstellungscodes nur als Hash
Herkunft	Die Schnittstelle nimmt Anfragen nur von der eigenen Adresse (APP_URL) an
Rollen	Jede Schnittstelle prüft die Rolle auf dem Server, nicht nur die Oberfläche (Kapitel 10)
Vertrauliches	Eine zentrale Regel: Vorsitz, Stellvertretung und Admin sehen alles Vertrauliche, andere nur eigene Uploads bzw. Fremdprotokolle ihres Gremiums
JAV und SBV	Nur Sitzungen und Protokolle, vertrauliche TOPs ausgeblendet – zentral gesperrt
Admin ohne Inhalte	Betreut die IT die Technik, kann der Vorsitz den Admin auf die Verwaltung beschränken (Kapitel 9.2)
Sichtschutz	Personal- und Gehaltslisten werden beim Fensterwechsel verdeckt (Kapitel 7)
Audit-Log	Über 50 Aktionstypen mit Zeitpunkt, Person, IP-Adresse und Browser (Kapitel 9.10)
Rollentests	Automatische Tests prüfen alle Schnittstellen je Rolle gegen eine leere Test-Datenbank – vor jedem Update (deploy_update.sh) und bei jeder Änderung auf GitHub; ein Stand mit falschen Rechten wird nicht eingespielt

Daten

Mechanismus	Umsetzung
Dokumente	Jede Datei einzeln mit AES-256-GCM verschlüsselt, mit eigenem, per scrypt aus dem ENCRYPTION_KEY abgeleiteten Schlüssel; GCM erkennt Manipulationen, dazu eine SHA-256-Prüfsumme
Fremdprotokolle, Scans	Ebenso verschlüsselt wie Dokumente
Protokolle	Finalisierte Versionen sind unveränderlich und tragen eine SHA-256-Prüfsumme
Löschen	Aufbewahrungsfristen je Kategorie löschen automatisch; Dateien werden vor dem Löschen überschrieben
Datenbank	Metadaten, Protokolltexte, Personaldaten und der Suchtext der Dokumente liegen in der Datenbank unverschlüsselt – geschützt durch das abgeschottete Netz und die Rechte auf dem NAS; zusätzlich ist die Volume-Verschlüsselung des NAS möglich

Backups

Mechanismus	Umsetzung
Verschlüsselt	Mit BACKUP_KEY verschlüsselt backup.sh Datenbank-Dump und Dokumenten-Archiv komplett mit AES-256 (256-Bit-Schlüssel), ohne Klartext-Zwischendatei (Kapitel 13.2)
Schlüssel	Der BACKUP_KEY ist ein 256-Bit-Zufallswert; der eigentliche Schlüssel wird per PBKDF2 (HMAC-SHA256, 600.000 Durchläufe, eigener Zufalls-Salt je Datei) daraus abgeleitet – das macht systematisches Durchprobieren praktisch aussichtslos
Kopie bei Dritten	So verschlüsselt kann eine Kopie z. B. bei der IT liegen, ohne dass sie lesbar ist – den Schlüssel hat nur der Betriebsrat
Prüfung	restore.sh prüft den Schlüssel, bevor etwas überschrieben wird; Einstellungen → System warnt bei unverschlüsselten Backups
Aufbewahrung	30 Tage rollierend auf dem NAS

- **RAID ist kein Backup** – RAID 1 schützt nur gegen den Ausfall einer Platte. Löschen, Verschlüsselungstrojaner, ein Defekt des NAS oder ein Brand treffen beide Platten. Deshalb: Snapshots auf dem NAS und eine verschlüsselte Kopie an einem anderen Ort
- **Wiederherstellung üben** – Ein Backup gilt erst als Backup, wenn es einmal auf einem anderen System eingespielt wurde

Organisatorisch

- **Schlüssel** – ENCRYPTION_KEY und BACKUP_KEY ausdrucken und außerhalb des NAS verschlossen aufbewahren. Ohne sie sind Dokumente bzw. Backups nicht wiederherstellbar
- **Server-Administration** – Die Schlüssel stehen in der .env auf dem NAS. Wer Administrator des NAS ist, kommt technisch an alle Daten. Deshalb nur Vorsitz und Stellvertretung als Admins (Kapitel 11.3); hilft die IT, dann nur gemeinsam mit einem Admin (Vier-Augen-Prinzip)
- **Freigaben auf dem NAS** – Den Datenordner von BR-DMS nicht als Netzwerkfreigabe anbieten. Freigaben für die Mitglieder (Arbeitsfreigabe, Watch-Folder) liegen getrennt davon (Kapitel 11.3)
- **Updates** – Neue Stände zuerst in der Demo prüfen, dann einspielen (Kapitel 13.1)

Empfehlung

Zwei-Faktor-Anmeldung mindestens für Vorsitz, Stellvertretung und Admin – diese Konten sehen alles Vertrauliche. Voraussetzung ist ein Diensthandy mit Authenticator-App (Kapitel 9.7).

11.3 Den Server (NAS) absichern

BR-DMS ist nur so sicher wie der Server, auf dem es läuft. Wer das NAS administriert, kommt an alles: die .env mit ENCRYPTION_KEY und BACKUP_KEY, die Datenbank und die Backups. Keine Anwendung kann davor schützen. Deshalb gilt: so wenige Admins wie möglich – und nur aus dem Betriebsrat. Gemeint sind hier die Konten des NAS, nicht die Rollen in BR-DMS (Kapitel 10).

Wer darf was auf dem NAS?

Wer	Rechte auf dem NAS
Vorsitz und Stellvertretung	Im Alltag ein normales Konto ohne Admin-Rechte wie die Mitglieder. Für die Verwaltung (Container, Updates, Einstellungen) ein getrenntes Admin-Konto mit zweitem Faktor, das nur dafür benutzt wird. Sonst hat niemand Admin-Rechte
Mitglieder	Normales Konto ohne Admin-Rechte, nur für die Arbeitsfreigabe (Zeitschriften, Tabellen, Arbeitsdokumente, auch für die Datei-Links aus Kapitel 12.8) und ggf. den Watch-Folder. Kein Zugriff auf den Datenordner von BR-DMS, die Backups oder die Container
IT	Kein Konto. Sie erhält nur die verschlüsselte Backup-Kopie; Hilfe am NAS nur gemeinsam mit einem Admin (Vier-Augen-Prinzip)

Docker = Admin

Wer Container starten darf, kann jeden Ordner des NAS in einen Container einbinden und damit alles lesen. Zugriff auf Docker bzw. die Container Station ist deshalb gleichbedeutend mit Admin-Rechten und gehört nur in die Hände der Admins.

Wo liegen die Schlüssel?

Eine häufige Frage: Muss die .env mit den Schlüsseln die ganze Zeit auf dem NAS liegen? Ja – und die Schlüssel lägen auch ohne sie dort. BR-DMS entschlüsselt Dokumente beim Öffnen selbst und braucht den ENCRYPTION_KEY deshalb im laufenden Betrieb. In der Datenbank stehen die Schlüssel nicht; dort liegt nur, was mit ihnen verschlüsselt ist (Dokumentdaten, Geheimnisse der Zwei-Faktor-Anmeldung).

Ort	Wozu
.env im Datenordner	Docker liest sie bei jeder Installation, jedem Update und Neubau; backup.sh liest jede Nacht den BACKUP_KEY daraus – ohne ihn würde unverschlüsselt gesichert
Konfiguration der Container	Docker übernimmt die Werte beim Anlegen. Deshalb startet BR-DMS nach einem Neustart des NAS auch ohne .env – ein Admin kann sie dort aber ebenso auslesen
Arbeitsspeicher des Backends	Solange BR-DMS läuft

Die .env nach dem Start zu löschen, bringt daher keine Sicherheit, legt aber Backups und Updates lahm. Entscheidend ist, wer die Schlüssel lesen kann:

Wer	Kommt an die Schlüssel?
Mitglieder mit Konto für die Arbeitsfreigabe	Nein – solange der Datenordner keine Freigabe ist und die .env nur für ihren Besitzer lesbar ist (chmod 600)
Admins des NAS	Ja, immer. Dagegen hilft nur das Kontenkonzept oben
Wer eine Platte ausbaut oder das NAS mitnimmt	Ja, wenn das Volume des NAS nicht verschlüsselt ist – die .env liegt auf derselben Platte wie die verschlüsselten Dokumente

Die Verschlüsselung der Dokumente schützt also vor allem Kopien, die das NAS verlassen. Gegen den Diebstahl von Platten oder Gerät hilft nur die Volume-Verschlüsselung des NAS. Mit automatischem Entsperren liegt deren Schlüssel wieder auf dem NAS – das schützt einzelne ausgebaute Platten, nicht das ganze Gerät. Mit Entsperren von Hand muss ein Admin das Volume nach jedem Neustart per Passwort öffnen, bevor BR-DMS startet: der stärkste Schutz, aber mit Aufwand bei jedem Neustart.

```
# Rechte der .env prüfen (Pfad = DATA_PATH), erwartet: -rw-----
ls -l /share/Container/br-dms/.env
```

Checkliste

Maßnahme	Warum
Standardkonto „admin“ deaktivieren, getrenntes Verwaltungskonto mit eigenem Namen anlegen	„admin“ ist das Erste, was Angreifer ausprobieren
Im Alltag ohne Admin-Rechte arbeiten, das Verwaltungskonto nur zum Verwalten benutzen	Ein Trojaner auf dem Arbeits-PC bekommt dann höchstens die Rechte eines normalen Kontos
Lange Passphrase (ab etwa 20 Zeichen) und zweiter Faktor (Authenticator-App) für das Verwaltungskonto	Ein erratenes oder abgefangenes Passwort allein reicht dann nicht. Nutzen zwei Personen das Konto, den QR-Code bei der Einrichtung auf beiden Handys scannen
Kein Zugang aus dem Internet: Cloud-Dienst des Herstellers (z. B. myQNAPcloud, QuickConnect), UPnP und Portfreigaben im Router aus	Erpressungstrojaner gegen NAS-Geräte kamen fast immer über aus dem Internet erreichbare Geräte
Firmware und Apps zeitnah aktualisieren	Die bekannten Angriffe nutzten Lücken, für die es längst Updates gab
Optional: Verwaltungsoberfläche per Firewall nur von den Rechnern der Admins erreichbar	Sinnvoll in großen Firmennetzen; sonst kann jeder im Netz den Login ausprobieren
Automatische Sperre nach Fehlversuchen einschalten	Bremst das Durchprobieren von Passwörtern
Den Dateien von BR-DMS das Verwaltungskonto als Besitzer geben (PUID) und eine Gruppe nur für Admins (PGID), nicht „users“ bzw. „everyone“; die .env nur für den Besitzer lesbar (chmod 600). Der Installationsassistent schlägt beides vor	In „users“ bzw. „everyone“ sind alle Konten des NAS – auch die der Mitglieder
Arbeitsfreigabe und Datenordner von BR-DMS strikt trennen; den Datenordner (DATA_PATH) und die Backups nie als Freigabe anbieten	Was in BR-DMS liegt, schützen Rollen und Verschlüsselung – eine Freigabe würde beides umgehen
Freigaben nur über SMB 3, SMB 1 abschalten	SMB 1 ist veraltet und war Einfallstor für Trojaner wie WannaCry
SSH nur bei Bedarf einschalten, am besten nur mit Schlüssel	Weniger Angriffsfläche im Alltag
Volume-Verschlüsselung des NAS erwägen (Entsperren von Hand = stärkster Schutz)	Nur sie schützt Datenbank und .env, wenn Platten oder das ganze NAS abhandenkommen

Maßnahme	Warum
Snapshots einrichten	Schreibgeschützte Stände helfen gegen Löschen und Verschlüsselungstrojaner (Kapitel 13.2)
Sicherheitsprüfung des NAS regelmäßig laufen lassen (QNAP: Security Counselor, Synology: Sicherheitsberater)	Findet unsichere Einstellungen, die sich mit der Zeit eingeschlichen haben
Zugangsdaten des Verwaltungskontos versiegelt zu den Schlüsseln legen (Kapitel 13.2)	Fallen beide Admins aus, ist das Gremium sonst ausgesperrt
Bei einem Amtswechsel Passphrase und zweiten Faktor am selben Tag neu setzen	Wer aus dem Amt scheidet, behält sonst den Zugang

KAPITEL 12

Installation

12.1 Voraussetzungen

Komponente	Mindestens	Empfohlen
Host	Docker-fähiges System (NAS, Linux-Server, VM)	aktuelle Version
Docker / Compose	Docker 20.10, Compose V2	Docker 24+, Compose 2.20+
Arbeitsspeicher	2 GB	4 GB
Speicher	20 GB	100 GB+
Werkzeuge auf dem Host	bash, python3, openssl	–

Bevor es losgeht, sollten diese Angaben bereitliegen:

- **Adresse des Servers** – IP-Adresse und/oder Rechnername, unter dem BR-DMS im Netz aufgerufen wird (z. B. 192.168.1.100 und br-nas)
- **Datenverzeichnis** – wo Datenbank und Dokumente liegen sollen; auf dem NAS ein eigener Ordner, z. B. /volume1/docker/br-dms
- **Admin-Zugang** – E-Mail-Adresse und ein Passwort mit mindestens 8 Zeichen für das erste Konto
- **Optional E-Mail** – SMTP-Server, Port, Benutzer und Passwort eines Postfachs (stehen in dessen Einstellungen)
- **Optional Scanner-Ordner** – falls Dokumente automatisch importiert werden sollen (Kapitel 12.6)

12.2 Schritt für Schritt

Alle Befehle werden auf dem Server im Projektordner ausgeführt (bei einem NAS per SSH).

1

Dateien bereitstellen

Repository klonen oder Release entpacken und in den Ordner wechseln.

2

Assistent starten

bash installation.sh – fragt alles Nötige ab, erzeugt die Schlüssel selbst und schreibt die .env (Kapitel 12.3). Am Ende zeigt er die folgenden Befehle fertig ausgefüllt an.

3

Verzeichnisse anlegen

Unterordner für Datenbank, Dokumente, Logs, Eingang, Backups und Zertifikat.

4

Zertifikat erzeugen

Ohne Zertifikat startet der HTTPS-Proxy nicht – es muss vor dem ersten Start da sein (Kapitel 12.4).

5

Starten

docker compose up -d --build. Der erste Start dauert einige Minuten; das Backend legt alle Tabellen und das erste Admin-Konto an.

6

Anmelden

`https://<Adresse>:8443` öffnen, mit `ADMIN_EMAIL` und `ADMIN_PASSWORD` anmelden, Passwort ändern (Klick auf den Namen) und unter Einstellungen → Benutzerverwaltung das Gremium anlegen.

```
bash installation.sh
mkdir -p /srv/br-dms/{storage,postgres,logs,watch_inbox,backups,certs}
bash proxy/generate-selfsigned-cert.sh /srv/br-dms br-nas 192.168.1.100
docker compose up -d --build
docker compose logs -f backend      # Start beobachten, Ende mit Strg+C
```

Sofort sichern

Jetzt den `ENCRYPTION_KEY` aus der `.env` in einen Passwort-Manager kopieren. Ohne ihn lassen sich die Dokumente auch aus einem Backup nicht mehr öffnen.

12.3 Der Installationsassistent – Frage für Frage

Werte in [eckigen Klammern] sind Vorschläge: Enter übernimmt sie. Felder ohne Vorschlag – etwa Passwörter – müssen ausgefüllt werden, sonst fragt der Assistent erneut. Bei Ja/Nein-Fragen gilt mit Enter der Großbuchstabe: [J/n] heißt Ja, [j/N] heißt Nein. Vor dem Schreiben zeigt der Assistent eine Zusammenfassung; erst nach Bestätigung entsteht die `.env`.

Frage	Was eintragen	Nur Enter
Zielsystem	1 = Linux-Server/VM oder NAS mit SSH-Shell, 2 = Synology, 3 = QNAP (2/3 nutzen die Deploy-Skripte)	1
Erreichbar unter	IP-Adresse oder Name des Servers	localhost (NAS: 192.168.1.100)
Datenverzeichnis	Ordner für Datenbank und Dokumente	./data bzw. NAS-Standardpfad
SSH-Benutzer (nur 2/3)	Das Verwaltungskonto aus Kapitel 11.3 – nicht „admin“	Pflicht
PUID / PGID	Wird erkannt (bei NAS per SSH mit dem Verwaltungskonto) – bestätigen. Beim NAS schlägt der Assistent statt der Gruppe aller Konten die Gruppe <code>administrators</code> vor	erkannter Wert
JWT_SECRET, ENCRYPTION_KEY	Nichts – nur bei einem Umzug den alten Schlüssel eingeben	neu erzeugt
Datenbankpasswort	Nichts	neu erzeugt
Admin-E-Mail	Login des ersten Kontos	admin@br-dms.lokal
Admin-Passwort	Mindestens 8 Zeichen, zweimal	Pflicht
HTTPS-Port / HTTP-Port	Nur ändern, wenn belegt oder 443/80 gewünscht	8443 / 8080

Frage	Was eintragen	Nur Enter
Weitere Namen fürs Zertifikat	Alle weiteren Adressen, unter denen BR-DMS aufgerufen wird	Rechnername
E-Mail konfigurieren?	Server, Port, Benutzer, Passwort, Absender	Nein
Watch-Folder aktivieren?	Ja, wenn ein Scanner-Ordner importiert werden soll	Nein

Der Assistent darf jederzeit erneut laufen, etwa um E-Mail nachzutragen. Eine vorhandene .env lädt er als Vorschlag; bei den Schlüsseln fragt er, ob sie bleiben sollen – hier immer Ja wählen, sonst sind bestehende Dokumente und Anmeldungen ungültig. APP_URL setzt er selbst aus Adresse und HTTPS-Port zusammen. Die .env ist danach nur für ihren Besitzer lesbar (chmod 600) – sie enthält die Schlüssel.

12.4 HTTPS-Zertifikat

BR-DMS ist nur über HTTPS erreichbar. Der Proxy erwartet zwei Dateien in <DATA_PATH>/certs/: fullchain.pem (Zertifikat) und privkey.pem (privater Schlüssel). Das Zertifikat gilt nur für die Adressen, die darin stehen – wer BR-DMS per IP und per Name aufruft, nimmt beide auf. Es gibt drei Wege:

Weg	Aufwand	Browser-Warnung
Selbstsigniert mit dem mitgelieferten Skript	eine Minute	bis es einmal je PC importiert ist
Von der internen Firmen-CA (IT fragen)	gering, wenn es eine CA gibt	keine auf Firmen-PCs
Let's Encrypt per DNS-Challenge (eigene Domain)	mittel, Erneuerung alle 90 Tage	keine

Selbstsigniert

Erster Parameter ist das Datenverzeichnis, danach alle Namen und IP-Adressen. Gültig 825 Tage; danach den Befehl erneut ausführen und das neue Zertifikat wieder importieren.

```
bash proxy/generate-selfsigned-cert.sh /srv/br-dms br-nas 192.168.1.100
docker compose restart proxy          # nur nötig, wenn BR-DMS schon läuft
```

Damit der Browser nicht mehr warnt, wird das Zertifikat einmal pro PC als vertrauenswürdig importiert. Dazu fullchain.pem auf den PC kopieren und in br-dms.crt umbenennen:

- **Windows (Edge, Chrome)** – Doppelklick auf br-dms.crt → Zertifikat installieren → Lokaler Computer → „Alle Zertifikate in folgendem Speicher speichern“ → Vertrauenswürdige Stammzertifizierungsstellen → Fertig stellen; Browser neu starten
- **macOS (Safari, Chrome)** – Doppelklick öffnet die Schlüsselbundverwaltung, Schlüsselbund „System“ wählen; danach das Zertifikat öffnen → Vertrauen → „Immer vertrauen“
- **Firefox** – Einstellungen → Datenschutz & Sicherheit → Zertifikate anzeigen → Zertifizierungsstellen → Importieren → „Dieser CA vertrauen, um Websites zu identifizieren“
- **Auf vielen PCs auf einmal** – die IT verteilt das Zertifikat per Gruppenrichtlinie

Eigenes Zertifikat (Firmen-CA oder Let's Encrypt)

Bei der IT ein Zertifikat für den Rechnernamen anfragen – wichtig: der Name muss als „Subject Alternative Name“ (SAN) eingetragen sein. Kommt es als .pfx-Datei, wird es so umgewandelt; danach beide Dateien nach `<DATA_PATH>/certs/` legen und den Proxy neu starten. Ein Let's-Encrypt-Zertifikat per DNS-Challenge braucht keinen offenen Port ins Internet, nur einen TXT-Eintrag in der öffentlichen DNS-Zone der Domain; Ergebnis ebenso als `fullchain.pem` und `privkey.pem` ablegen.

```
openssl pkcs12 -in zertifikat.pfx -clcerts -nokeys -out /srv/br-dms/certs/fullchain.pem
openssl pkcs12 -in zertifikat.pfx -nocerts -nodes -out /srv/br-dms/certs/privkey.pem
docker compose restart proxy
```

Ändert sich dadurch die Adresse (z. B. `https://br-dms.firma.de`), auch `APP_URL` in der `.env` anpassen und `docker compose up -d` ausführen.

12.5 Die .env von Hand

Wer den Assistenten nicht nutzt, kopiert `.env.example` nach `.env` und ersetzt jedes `BITTE_AENDERN`. Die Schlüssel erzeugt `openssl rand -hex 32` (je einmal für `JWT_SECRET` und `ENCRYPTION_KEY`). Danach `chmod 600 .env`, damit nur der Besitzer die Schlüssel lesen kann. Die Tabelle zeigt, was passiert, wenn ein Wert leer bleibt:

Variable	Bedeutung	Wenn leer
<code>DATA_PATH</code>	Datenverzeichnis auf dem Host	Pflicht – sonst landen die Daten unter / des Hosts
<code>POSTGRES_PASSWORD</code>	Datenbank; nur Buchstaben, Ziffern, - und _	Backend startet nicht
<code>JWT_SECRET</code>	Signiert Anmeldungen (<code>openssl rand -hex 32</code>)	Backend startet nicht
<code>ENCRYPTION_KEY</code>	Verschlüsselt Dokumente, genau 64 Hex-Zeichen	Backend startet nicht
<code>ADMIN_EMAIL</code>	Login des ersten Kontos	<code>admin@br-dms.lokal</code>
<code>ADMIN_PASSWORD</code>	Passwort des ersten Kontos, mind. 8 Zeichen	Erste Installation startet nicht
<code>APP_URL</code>	Adresse wie im Browser, z. B. <code>https://br-nas:8443</code>	Links in E-Mails führen ins Leere
<code>PUID / PGID</code>	Besitzer der Dateien auf dem Host (NAS: Verwaltungskonto, Gruppe nur für Admins)	1000 / 100
<code>SMTP_HOST, _PORT, _USER, _PASS, _FROM</code>	E-Mail-Versand	keine E-Mails, sonst alles normal
<code>WATCH_FOLDER_ENABLED</code>	Scanner-Ordner importieren	aus
<code>WATCH_INBOX_PATH</code>	Eigener Eingangsordner	<code><DATA_PATH>/watch_inbox</code>
<code>SYSTEM_USER_ID</code>	Konto für Importe	erstes Admin-Konto

Variable	Bedeutung	Wenn leer
UPDATE_CHECK_ENABLED	Täglich nach neuen Versionen auf GitHub fragen (false = aus)	an
PROXY_HTTPS_PORT / _HTTP_PORT	Ports des Proxys	8443 / 8080

Fehlen Schlüssel oder steht noch ein Platzhalter darin, startet das Backend bewusst nicht und nennt den Grund im Log (docker compose logs backend, Zeilen mit [Konfiguration]). ADMIN_EMAIL und ADMIN_PASSWORD werden nur beim allerersten Start gelesen – spätere Änderungen in der .env wirken nicht mehr; das Passwort wird dann in der App geändert. Nach jeder anderen Änderung an der .env: docker compose up -d.

12.6 Watch-Folder

Mit WATCH_FOLDER_ENABLED=true überwacht das Backend einen Ordner – etwa die Ablage eines Scanners – und importiert neue PDF-, DOCX-, DOCM- und XLSX-Dateien sowie E-Mails (EML, MSG) automatisch in den Eingang; PDF- und Office-Anhänge von E-Mails werden dabei gleich als eigene Dokumente abgelegt. Der Unterordner bestimmt die Kategorie: anhoerung_99, anhoerung_102 (ordentliche Kündigung), anhoerung_102_ausserordentlich, abmahnung, bewerbung, bewerbung_alternativ, zeitmodell_87, betriebsvereinbarung, arbeitgeber_info, arbeitsschutz, schriftverkehr, protokoll, sonstiges. Dateien aus unbekannten Ordnern landen unter „Sonstiges“. Jeder Import und jeder Fehler wird im Audit-Log protokolliert.

Importe werden dem ersten Admin-Konto zugeordnet. Soll es ein anderes Konto sein, dessen ID als SYSTEM_USER_ID eintragen – sie steht in der Benutzerverwaltung als graue Zeile unter dem Namen, ein Klick kopiert sie. Empfohlen ist ein eigener, separat freigegebener Ordner (WATCH_INBOX_PATH): Wer einliefert, sieht dann nur diesen Ordner, nicht das restliche Datenverzeichnis.

Ein Unterordner fällt aus diesem Schema heraus: protokoll_scan ist für Scans der Anwesenheitsliste und der Unterschriftenseite (Kapitel 4.4) gedacht, nicht für normale Dokumente. Erlaubt sind PDF, JPG und PNG. Dateien landen dort nicht im Eingang als Dokument, sondern als „wartender Scan“, der sich per Klick einer Sitzung und einem oder beiden Nachweisen zuordnen lässt.

12.7 Wenn etwas nicht klappt

Problem	Ursache und Lösung
Seite lädt nicht, Proxy startet nicht	Zertifikat fehlt in <DATA_PATH>/certs – Skript ausführen (12.4), dann docker compose up -d
Backend startet immer wieder neu	docker compose logs backend: Zeilen mit [Konfiguration] nennen den fehlenden Wert in der .env
„Verbindung nicht privat“	Selbstsigniertes Zertifikat: einmal importieren (12.4); oder die Adresse fehlt im Zertifikat – mit allen Namen neu erzeugen
Links in E-Mails funktionieren nicht	APP_URL entspricht nicht der Adresse im Browser (https, Name, Port) – anpassen, docker compose up -d

Problem	Ursache und Lösung
Port bereits belegt	PROXY_HTTPS_PORT / PROXY_HTTP_PORT in der .env ändern
Keine E-Mails	SMTP-Werte prüfen; bei Einladungen zeigt die Einladungskarte den Fehler je Empfänger, sonst steht er im Backend-Log
„Permission denied“ im Log	PUID/PGID passen nicht zum Besitzer des Datenverzeichnisses (id auf dem Host)
Dokumente nach Umzug nicht lesbar	ENCRYPTION_KEY stimmt nicht mit dem alten System überein – alten Schlüssel eintragen

12.8 Datei-Links im Editor (Windows)

Ein UNC-Pfad (\\server\\freigabe\...), der im Editor einer Sitzung, Aufgabe oder im Wissensarchiv eingefügt wird, wird automatisch in einen brdmsfile://-Link umgewandelt. Browser blockieren file://-Links auf Netzwerkfreigaben aus Sicherheitsgründen – der Link öffnet die Datei stattdessen über einen kleinen, lokal installierten Protokoll-Handler mit der Standard-App (Word, Explorer, ...), genau wie ein Doppelklick im Explorer.

Jeder Windows-PC, auf dem jemand solche Links anklicken will, richtet den Handler einmalig selbst ein – keine Admin-Rechte nötig, es wird nur in HKEY_CURRENT_USER geschrieben:

1 Ordner kopieren

tools/brdmsfile-protokoll aus dem Projekt auf den PC kopieren (Netzlaufwerk oder USB-Stick).

2 Installieren.ps1 ausführen

Rechtsklick → „Mit PowerShell ausführen“. Das Skript kompiliert einen kleinen Helfer (BrdmsFileOpener.exe) mit dem in jedem Windows 10/11 enthaltenen C#-Compiler und registriert ihn für das brdmsfile://-Protokoll.

3 Einmal bestätigen

Beim ersten Klick auf einen Link fragt der Browser, ob er „BR-DMS Datei-Link“ öffnen darf – bestätigen.

Virens Scanner-Meldung bei einer älteren Einrichtung

Wurde brdmsfile:// auf einem PC schon vor dieser .exe-Variante eingerichtet, ruft die Registry dort noch die ältere, rein skriptbasierte Lösung auf: powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -File OpenBrdmsFile.ps1 "<Link>". Genau diese Kombination (Hidden + Bypass, aus dem Browser heraus gestartet) schlägt bei praktisch jedem Virens Scanner oder EDR an – unabhängig vom Inhalt des Skripts. Abhilfe: Installieren.ps1 auf diesem PC erneut ausführen; das überschreibt die Registry-Verknüpfung und zeigt danach direkt auf die kompilierte .exe, ganz ohne PowerShell-Aufruf.

Auch die .exe-Variante kann vereinzelt auffallen, weil sie lokal frisch kompiliert, unsigniert ist und einen URL-Protokoll-Handler registriert – ein Muster, das auch Schadsoftware nutzt. Der Quellcode (tools/brdmsfile-protokoll/BrdmsFileOpener.cs) ist kurz und für die IT einsehbar: Das Programm liest nur die übergebene Adresse, baut daraus einen Pfad und öffnet ihn mit der Standard-App – ohne Internetzugriff oder Datenversand. Bei einer Meldung trotzdem: %LOCALAPPDATA%\BR-DMS\BrdmsFileOpener.exe von der Prüfung ausnehmen oder firmenintern signieren.

Öffnet ein Link trotzdem nichts, steht die Fehlermeldung in %LOCALAPPDATA%\BR-DMS\log.txt.

KAPITEL 13

Betrieb

13.1 Updates einspielen

Die Deploy-Skripte übertragen den aktuellen Quellstand per SSH auf den Host. Ziel-Host, Benutzer und Pfad stehen in `.env.deploy` (Vorlage: `.env.deploy.example`). Alle drei Skripte übertragen dieselben Dateien aus `deploy_dateien.txt` und verhalten sich gleich – sie unterscheiden sich nur darin, auf welchem Rechner sie laufen.

Erscheint eine neue Haupt- oder Funktionsversion (z. B. 1.3.0), zeigt BR-DMS Vorsitz, Stellvertretung und Admin oben einen Hinweis mit Link zu den Neuerungen. Dafür fragt das Backend einmal täglich die Releases auf GitHub ab; reine Fehlerkorrekturen (1.2.x) lösen keinen Hinweis aus. Wer keine Anfrage nach außen möchte, setzt `UPDATE_CHECK_ENABLED=false` in der `.env`.

Skript	Läuft auf	Übertragung
<code>deploy_update.sh</code>	Linux / macOS	tar über SSH
<code>deploy_update.ps1</code>	Windows 10/11 (OpenSSH und tar eingebaut)	tar über SSH
<code>deploy_komplett.py</code>	überall mit Python 3	Python über SSH (Host braucht python3 ≥ 3.8)

- **Sauberer Stand** – `backend/src`, `backend/prisma` und `frontend/src` werden auf dem Host ersetzt; gelöschte oder umbenannte Dateien bleiben nicht liegen
- **Abbruchsicher** – Übertragen wird erst in einen Zwischenordner; bricht die Verbindung ab, bleibt der alte Stand erhalten
- **Daten bleiben** – `.env`, Datenbank, Dokumente, Zertifikate und Backups auf dem Host werden nie angefasst
- **Passende Befehle** – Das docker-Programm wird am Pfad erkannt (QNAP `/share/...`, Synology `/volume...`) oder über `DOCKER_BIN` festgelegt
- **Sicherheitsprüfung** – Vor dem Übertragen prüft `npm audit` Backend und Frontend auf bekannte Lücken (hoch/kritisch) und fragt bei Funden nach, ob trotzdem übertragen werden soll
- **Frische Basis-Images** – Beim Bauen werden `node`, `nginx` und `postgres` neu geladen; sonst blieben auf dem Host die einmal geladenen Images mit ihren alten Sicherheitslücken liegen

```
cp .env.deploy.example .env.deploy # einmalig: NAS_USER, NAS_HOST, DATA_PATH
./deploy_update.sh --trocken        # Probelauf: zeigt nur, was übertragen würde
./deploy_update.sh                  # übertragen, danach Befehle anzeigen
./deploy_update.sh --bauen          # übertragen und direkt neu bauen/starten

# Windows: .\deploy_update.ps1 -Trocken | -Bauen
# Python:  python3 deploy_komplett.py --trocken | --bauen
```

Neu bauen und starten auf dem Host

Ohne --bauen werden die Container danach per SSH auf dem Host neu gebaut. Auf NAS-Systemen liegt das docker-Programm nicht im Standardpfad, deshalb mit vollem Pfad und sudo:

System	Datenverzeichnis	docker-Programm
QNAP (Container Station)	/share/Container/br-dms	/share/CACHEDEV1_DATA/.qpkg/container-station/bin/docker
Synology (Container Manager, DSM 7.2+)	/volume1/docker/br-dms	/usr/local/bin/docker
Linux-Server / VM	frei wählbar	docker

Jede Zeile ist ein vollständiger Befehl und kann einzeln kopiert werden – erst ins Datenverzeichnis wechseln, dann bauen und starten:

```
# QNAP
cd /share/Container/br-dms
sudo /share/CACHEDEV1_DATA/.qpkg/container-station/bin/docker compose pull postgres proxy
sudo /share/CACHEDEV1_DATA/.qpkg/container-station/bin/docker compose build --pull
sudo /share/CACHEDEV1_DATA/.qpkg/container-station/bin/docker compose up -d

# Synology
cd /volume1/docker/br-dms
sudo /usr/local/bin/docker compose pull postgres proxy
sudo /usr/local/bin/docker compose build --pull
sudo /usr/local/bin/docker compose up -d

# Linux-Server / VM
cd <DATA_PATH>
docker compose pull postgres proxy && docker compose build --pull && docker compose up
```

- **Nur Backend neu** – ... compose build --pull backend, danach ... compose up -d
- **Frontend ohne Cache** – ... compose build --pull --no-cache frontend, danach ... compose up -d (wenn Änderungen nicht ankommen)
- **Log ansehen** – sudo <docker-Programm> logs brdms_backend --tail 40 -f

Pfad finden

Weicht der Pfad ab (andere Volume- oder Container-Station-Version), zeigt „which docker“ bzw. „ls /share/*.qpkg/container-station/bin/docker“ per SSH auf der NAS den richtigen Ort. Ältere Synology-Versionen (Paket „Docker“ statt „Container Manager“) kennen nur docker-compose mit Bindestrich.

Sicherheitslücken rechtzeitig erkennen

Neue Lücken werden laufend in Programmbibliotheken, Node.js, nginx und PostgreSQL gefunden. Damit sie nicht unbemerkt bleiben, prüfen mehrere Stellen automatisch:

Wer prüft	Was	Wie erfahre ich davon?
Dependabot (GitHub)	Bekannte Lücken in allen Paketen und Docker-Images; schlägt Updates wöchentlich als Pull Request vor, Sicherheitsupdates sofort	E-Mail von GitHub; Repository → Security
CodeQL (GitHub)	Eigener Code bei jedem Push: ungeprüfte Eingaben in HTML (XSS), Pfadmanipulation u. Ä.	Repository → Security → Code scanning
Update-Skript	npm audit vor jeder Übertragung; frische Basis-Images beim Bauen	Warnung im Terminal, Rückfrage
NAS-Hersteller	Firmware und Container Station / Container Manager	Sicherheitsprüfung des NAS (Kapitel 11.3)

Laufzeiten im Blick behalten: Node.js 24 wird bis April 2028 gepflegt, PostgreSQL 16 bis November 2028, nginx im stabilen Zweig jeweils etwa ein Jahr. Rechtzeitig vorher schlägt Dependabot den Wechsel vor.

13.2 Backup und Wiederherstellung

backup.sh sichert Datenbank und verschlüsselte Dokumente nach <DATA_PATH>/backups/; Sicherungen älter als 30 Tage werden entfernt. restore.sh führt interaktiv durch die Wiederherstellung und verlangt vor dem Überschreiben eine ausdrückliche Bestätigung.

```
sudo bash <DATA_PATH>/backup.sh
# -> db_<Zeit>.sql.gz.enc, storage_<Zeit>.tar.gz.enc, info_<Zeit>.txt
sudo bash <DATA_PATH>/restore.sh # interaktiv

# ohne Rückfragen, z. B. mit einer Datei außerhalb von backups/:
sudo bash <DATA_PATH>/restore.sh /pfad/db_<Zeit>.sql.gz.enc --mit-storage --ja
```

restore.sh spielt die Datenbank in einem einzigen Schritt ein: Tritt ein Fehler auf, bricht es ab und die Datenbank bleibt auf dem Stand vor dem Restore – es bleibt nie etwas halb eingespielt zurück. Das Skript muss nicht aus dem Datenverzeichnis gestartet werden; es findet die .env neben sich selbst.

Vorher vergleicht restore.sh die Version aus info_<Zeit>.txt mit dem laufenden System. Ein Backup einer neueren Version spielt es nicht ein – erst das System aktualisieren (erzwingen: --trotzdem). Ältere Backups werden eingespielt; das Backend ergänzt beim Start die seither neuen Tabellen und Felder, und restore.sh wartet, bis das gelungen ist. Einstellungen → System zeigt die Version jeder Sicherung.

Für tägliche Sicherungen den Aufgabenplaner der NAS (z. B. 02:00 Uhr, Benutzer root) bzw. cron verwenden. Den Zustand der Backups zeigt Einstellungen → System.

Wiederherstellung

Bei einer Wiederherstellung auf einem anderen System muss der ENCRYPTION_KEY in der .env schon vorher exakt dem des Quellsystems entsprechen, bei verschlüsselten Backups zusätzlich der BACKUP_KEY.

Ausführliche Anleitung

Das Sicherungskonzept zum Erklären im Gremium, das Einrichten der nächtlichen Sicherung auf QNAP und Synology, die Wiederherstellung für jeden Schadensfall sowie Vordrucke für Schlüsselblatt und Testprotokoll stehen in der eigenen Anleitung BR-DMS_Backup-Anleitung.pdf.

Verschlüsselte Backups

Steht ein BACKUP_KEY in der .env (der Einrichtungsassistent erzeugt ihn, sonst openssl rand -hex 32), verschlüsselt backup.sh Datenbank-Dump und Dokumenten-Archiv komplett – ohne unverschlüsselte Zwischendatei. Verfahren: AES-256-CBC mit 256-Bit-Schlüssel (OpenSSL); der Schlüssel wird per PBKDF2 (HMAC-SHA256, 600.000 Durchläufe, eigener Zufalls-Salt je Datei) aus dem BACKUP_KEY abgeleitet, der selbst ein 256-Bit-Zufallswert ist. Das ist wichtig, weil der Datenbank-Dump sonst Protokolle, Beschlüsse, Personal- und Gehaltsdaten und den Suchtext der Dokumente im Klartext enthält. Nur so verschlüsselt sollte eine Kopie das NAS verlassen, etwa zur Sicherung bei der IT: Sie kann die Dateien aufbewahren, aber nicht lesen. Ohne BACKUP_KEY sichert das Skript weiter unverschlüsselt und warnt; Einstellungen → System zeigt das ebenfalls an.

- **Schlüssel sichern** – ENCRYPTION_KEY und BACKUP_KEY ausdrucken und außerhalb des NAS verschlossen aufbewahren
- **Wiederherstellen** – restore.sh erkennt die Endung .enc und prüft den Schlüssel, bevor etwas überschrieben wird
- **Kopie außer Haus** – RAID schützt nur gegen den Ausfall einer Platte, nicht gegen Löschen, Verschlüsselungstrojaner, Defekt oder Brand des NAS; deshalb zusätzlich eine Kopie an einem anderen Ort und Snapshots auf dem NAS

```
# Notfall: von Hand entschlüsseln (ohne restore.sh)
openssl enc -d -aes-256-cbc -pbkdf2 -iter 600000 -pass pass:<BACKUP_KEY> \
-in db_<Zeit>.sql.gz.enc | gunzip > db.sql
```

13.3 Demo-Instanz

Für Vorführungen startet ein Befehl eine komplett getrennte Instanz mit erfundenen Daten: „Nordwerk Maschinenbau GmbH“ mit rund 250 Beschäftigten, 9er-Gremium, drei Ersatzmitgliedern, JAV und SBV, acht Sitzungen, vier weiteren Gremien mit Fremdprotokollen, verschlüsselten Beispiel-PDFs, Fristen, Gehaltshistorie und mehr. Mit Internetverbindung werden auch die Gesetzestexte geladen. Alle Daten werden relativ zum aktuellen Datum erzeugt. Die Abbildungen in diesem Handbuch stammen aus dieser Demo.

```
./demo/demo.sh start      # bauen, starten, befüllen -> https://localhost:8444
./demo/demo.sh stop      # anhalten, Daten bleiben
./demo/demo.sh reset     # alles löschen und frisch einspielen
./demo/demo.sh logs      # Backend-Log verfolgen
./demo/demo.sh entfernen # Demo komplett löschen (fragt nach)

# Anmeldung: s.kroeger / Demo2026! (Vorsitz) – weitere Konten zeigt start
```

Die Demo läuft neben einer echten Installation auf demselben Rechner: eigene Container

(brdms_demo_...), eigene Docker-Volumes statt des Datenverzeichnisses, eigener Port 8444 und eigene, beim ersten Start erzeugte Schlüssel in demo/.env.demo. „entfernen“ löscht Container, Volumes, die gebauten Demo-Images, Schlüssel und Zertifikat der Demo – nur dieses Projekt, eine echte Installation bleibt unberührt.

Demodaten lassen sich nicht über echte Daten spielen: Das Demo-Skript schreibt nur in eine leere Datenbank und bricht sonst ab. Soll das Gremium die Demo auf dem NAS ausprobieren, übernimmt demo_modus.sh das Sichern, Umschalten und Zurückholen (Kapitel 13.4).

Die Screenshots dieses Handbuchs werden aus der laufenden Demo neu erzeugt (braucht Node.js ab Version 22 und Chrome oder Chromium; ein anderer Browser über CHROME=/pfad/zum/browser):

```
node tools/handbuch-screenshots/screenshots.mjs
python3 generate_manual.py
```

13.4 Demo auf dem Server – das Gremium ausprobieren lassen

Bevor BR-DMS mit echten Daten genutzt wird, soll das Gremium oft erst einmal „herumspielen“ – auf dem NAS, damit alle von ihrem Arbeitsplatz aus mitmachen können. demo_modus.sh schaltet die Installation dafür vorübergehend auf die Demodaten aus Kapitel 13.3 um und danach zurück auf die echten Daten. Das Skript liegt im Datenverzeichnis neben backup.sh und restore.sh (die Deploy-Skripte übertragen es) und läuft auf QNAP, Synology und Linux gleich – das docker-Programm sucht es selbst.

Aufruf	Was passiert
sudo bash demo_modus.sh status	Zeigt, ob echte oder Demodaten laufen und welche Sicherungen es gibt
sudo bash demo_modus.sh demo	Backup der echten Daten, Kopie mit .env nach sicherung_vor_demo/<Zeit>; E-Mail-Versand und Watch-Folder aus; Datenbank und Dokumente leeren; Demodaten einspielen
sudo bash demo_modus.sh neu	Demo von vorn beginnen – alles, was das Gremium angelegt hat, ist weg; die Sicherung der echten Daten bleibt unberührt
sudo bash demo_modus.sh echt	Ursprüngliche .env zurück, Demodaten löschen, echte Daten aus der Sicherung einspielen

- **Sicher vor dem Aufräumen** – Die Sicherung liegt außerhalb von backups/, wo backup.sh nach 30 Tagen löscht; die Demo darf also beliebig lange laufen
- **Keine Mails an erfundene Adressen** – Während der Demo sind E-Mail-Versand und Watch-Folder aus; „echt“ holt die ursprüngliche .env samt allen Einstellungen zurück
- **Nichts aus Versehen** – Jeder Schritt, der Daten löscht, verlangt ein eingetipptes Wort (DEMO, NEU, ECHT); „demo“ verweigert, wenn schon Demodaten laufen, damit sie nicht als „echte Daten“ gesichert werden
- **Voraussetzung** – In der .env muss ADMIN_PASSWORD stehen (mind. 8 Zeichen); damit startet die geleerte Installation. ENCRYPTION_KEY und BACKUP_KEY während der Demo nicht ändern

Demo-Konten

Anmelden in der Demo: Alle Konten haben das Passwort Demo2026!, z. B. s.kroeger@nordwerk-demo.lokal (Vorsitz), t.brandt@... (Stellvertretung), m.yilmaz@... (Mitglied), m.engel@... (Ersatzmitglied). Das Skript zeigt die Liste am Ende an. Die beiden Backup-Dateien aus sicherung_vor_demo/ zusätzlich auf einen PC kopieren.

Von Hand, Befehl für Befehl

Dasselbe ohne Skript, etwa zum Nachvollziehen. Erst die Zeile mit D= für das eigene System ausführen, dann die übrigen Befehle der Reihe nach. <Zeit> ist der Zeitstempel des Backups, PUID und PGID stehen in der .env.

```
# QNAP
D=/share/CACHEDEV1_DATA/.qpkg/container-station/bin/docker
cd /share/Container/br-dms

# Synology
D=/usr/local/bin/docker
cd /volume1/docker/br-dms
```

Umschalten auf Demodaten:

```
# 1. echte Daten sichern, <Zeit> des neuesten Backups ablesen
sudo bash backup.sh
ls -lh backups/
sudo mkdir -p sicherung_vor_demo/<Zeit>
sudo cp -a backups/*<Zeit>* .env sicherung_vor_demo/<Zeit>/

# 2. E-Mail-Versand und Watch-Folder aus
sudo sed -i 's/^SMTP_/#SMTP_/' .env
sudo sed -i 's/^WATCH_FOLDER_ENABLED=.*/WATCH_FOLDER_ENABLED=false/' .env

# 3. stoppen, Datenbank und Dokumente leeren, leer starten
sudo $D compose down
sudo rm -rf postgres storage && sudo mkdir postgres storage
sudo $D compose up -d

# 4. warten, bis „healthy“ erscheint, dann Demodaten einspielen
sudo $D inspect -f '{{.State.Health.Status}}' brdms_backend
sudo $D exec -u <PUID>:<PGID> brdms_backend node dist/demo/demo-daten.js
```

Zurück zu den echten Daten:

```
sudo $D compose down
# ursprüngliche .env zurück
sudo cp -a sicherung_vor_demo/<Zeit>/ .env .env
sudo rm -rf postgres storage && sudo mkdir postgres storage
# leer starten und warten, bis „healthy“ erscheint
sudo $D compose up -d
sudo bash restore.sh \
    sicherung_vor_demo/<Zeit>/db_<Zeit>.sql.gz.enc --mit-storage --ja
```

Erst sichern, dann löschen

Beim Umschalten werden Datenbank und Dokumente gelöscht. Vorher prüfen, dass in `sicherung_vor_demo/<Zeit>/` beide Backup-Dateien (`db_...` und `storage_...`) und die `.env` liegen – das Skript prüft das selbst und bricht sonst ab, bevor etwas gelöscht wird.

KAPITEL 14

Datenbank

Das Schema wird mit Prisma verwaltet (backend/prisma/schema.prisma) und beim Start automatisch angeglichen. Die wichtigsten Tabellen:

Bereich	Tabellen
Benutzer	Benutzer, PasswortReset, AuditLog
Dokumente	Dokument, DokumentVersion, Frist, Kommentar
Sitzungen	Sitzung, SitzungVersion, TOP, TopDokument, Anwesenheit, Beschluss, Abstimmung, ProtocolBlock, SitzungsVorlage
Zusammenarbeit	Aufgabe (inkl. Vorhaben und Themen-Backlog), Nachricht, KummerkastenEintrag
Wissen	WissensEintrag, Ressource, GesetzParagraph
Personal	Mitarbeiter, Abteilung, GehaltsstufenEintrag, ZeitmodellEintrag, UeberstundenEintrag
Weitere	Betriebsvereinbarung, Qualifikation, Schulungstermin, SchulungsTeilnahme, Gremium, GremiumMitglied, Fremdprotokoll
System	SystemEinstellung, Aufbewahrungsregel

14.1 Wichtige Statuswerte

Feld	Werte
Rolle	VORSITZ, STELLVERTRETER, MITGLIED, ERSATZMITGLIED, JAV, SBV, ADMIN
Sitzungsstatus	ENTWURF, TAGESORDNUNG_FIXIERT, PROTOKOLL_ENTWURF, PROTOKOLL_FINAL, ABGESAGT
TOP-Status	OFFEN, BESCHLOSSEN, ABGELEHNT, VERTAGT, ZUR_KENNTNIS
Dokumentstatus	AKTIV, ARCHIVIERT, LOESCHVORMERKUNG, GELOESCHT
Fristtyp	ANHOERUNG_99_WOCHE, ANHOERUNG_102_ORDENTLICH, ANHOERUNG_102_AUSSERORDENTLICH, ZEITMODELL_87_WOCHE, WIDERSPRUCH, BENUTZERDEFINIERT
Anwesenheit	ANWESEND, ABWESEND_ENTSCHULDIGT, ABWESEND_UNENTSCHULDIGT, ERSATZ_FUER
BV-Status	AKTIV, GEKUENDIGT, ABGELOEST, BEFRISTET_AUSGELAUFEN
Beschäftigungsart	MITARBEITER, AZUBI, STUDENT, DUALER_STUDENT, ZEITARBEITER

Autor, Lizenz & Support

Entwicklung

BR-DMS wurde entwickelt von Tim van der Hoven – Programmierung mit Unterstützung von Claude (Anthropic).

Support

Fragen, Fehlermeldungen und Wünsche bitte per E-Mail an support@vanderhoven.eu. Hilfreich sind die Versionsnummer (in der App unter „Über BR-DMS“) und eine kurze Beschreibung, was passiert ist.

Hinter der Versionsnummer steht der genaue Programmstand, z. B. „1.3.1 · a1b2c3d“. Die Zeichen nach dem Punkt bezeichnen den Stand im Quellcode; ein „+“ am Ende heißt, dass bei der Installation noch nicht festgeschriebene Änderungen dabei waren.

Fehler direkt aus BR-DMS melden

Im Fenster „Über BR-DMS“ gibt es unter der Version das Formular „Fehler melden“: kurzen Titel und Beschreibung eintragen, dann eine der beiden Schaltflächen wählen. Version, aufgerufene Seite und Browser hängt BR-DMS automatisch an – so ist klar, auf welchen Programmstand sich die Meldung bezieht.

- **Auf GitHub melden** – Öffnet eine vorausgefüllte Fehlermeldung (Issue) im öffentlichen Projekt auf GitHub. Dort lässt sich der Text noch prüfen; nach dem Absenden sehen Sie die Meldung und alle Antworten darauf. Dafür ist ein kostenloses GitHub-Konto nötig
- **Per E-Mail** – Öffnet Ihr E-Mail-Programm mit demselben Text an support@vanderhoven.eu

GitHub-Meldungen sind öffentlich einsehbar. Bitte keine Namen, Personaldaten oder Inhalte aus Dokumenten und Sitzungen eintragen – im Zweifel per E-Mail melden.

Lizenz

Copyright © 2026 Tim van der Hoven. BR-DMS ist Open Source und steht unter der GNU Affero General Public License v3.0 (AGPL-3.0). Nutzung, Änderung und Weitergabe sind erlaubt, solange der Urheberhinweis erhalten bleibt und Änderungen – auch beim Betrieb als gehosteter Dienst – unter derselben Lizenz offengelegt werden. Der vollständige Lizenztext liegt als Datei LICENSE bei.