

EPD²

Portalverwaltungsordnung der EPD²

Fünf universelle Panels PV-01 bis PV-05

Entwurf 1.2 · Stand 29. September 2026

ENTWURF · NICHT BESCHLOSSEN · RECHTLICH ZU PRÜFEN

Arbeitsfassung für Owner Review / Gründungs- und Implementierungsvorbereitung.

ENTWURF 1.2 · NICHT BESCHLOSSEN · RECHTLICH ZU PRÜFEN

Stand: 29. September 2026

Diese Fassung ersetzt im Entwurf die bisherige Vorstellung vieler rollenbezogener Einzelpanels durch fünf universelle Arbeitsoberflächen. Rollen, Mandate und technische Panels sind strikt getrennte Ebenen.

§ 1 Zweck, Rang und Grundsatz

(1) Diese Ordnung regelt die Zuordnung, Registrierung, Aktivierung, Nutzung, Beendigung und sicherheitsbedingte Unterbrechung administrativer Zugänge zum Parteiportal. Sie schafft kein Parteiamt und verändert weder gesetzliche noch satzungsmäßige Zuständigkeiten.

(2) Politische oder organisatorische Zuständigkeit entsteht ausschließlich aus Gesetz, Satzung, wirksamer Wahl, Bestellung, Beauftragung oder einem zuständigen Beschluss. Eine sichtbare Schaltfläche, eine technische Rolle, ein Panel, ein Account oder eine technische Freischaltung begründet keine materielle Befugnis.

(3) Es gilt das Trennungsprinzip:

- Rolle/Mandat bestimmt, welche Aufgabe eine Person rechtlich oder organisatorisch wahrnehmen darf;
- Scope begrenzt diese Aufgabe organisatorisch und verfahrensbezogen;
- Berechtigungsakt/Grant dokumentiert den technischen Zugang;
- Panel ist ausschließlich die Benutzeroberfläche, in der zulässige Funktionen angezeigt werden.

(4) Die Klassen A, A-I, B, R und T sind Berechtigungs- und Funktionsklassen. Sie sind keine eigenständigen Frontend-Panels. Die Oberfläche besteht aus genau fünf universellen Panels nach § 5 bis § 9.

§ 2 Rollenklassen und Referenzkennungen

(1) Klasse A bezeichnet institutionelle Leitungs- und Verwaltungsfunktionen. Für das technische Ausführungsregister werden folgende Referenzprofile verwendet:

- A-01 Bundesvorsitz;
- A-02 Mitglied des Bundesvorstands; Funktionen nur im Rahmen des Amtes und ausdrücklicher Zuständigkeit, bei weiteren Vorstandsmitgliedern nur für explizit zugewiesene Vorgänge;
- A-03 Landesvorsitz;
- A-04 Kreisvorsitz;
- A-05 ausdrücklich zugewiesene Leitungs- oder Verfahrensfunktion. A-05 ist ein technischer Sammelcode für eine dokumentierte Einzelzuweisung durch das zuständige Organ und begründet keine eigenständige Amtsklasse.

(2) Klasse A-I bezeichnet unabhängige Kontroll- und Schiedsgerichtsfunktionen:

- AI-01 Revision/Rechnungsprüfung;
- AI-02 Parteischiedsgericht;
- AI-03 unabhängige Berechtigungsprüfung.

(3) Klasse B bezeichnet zweck- und scopegebundene Fachrollen:

- B-01 Identitätsprüfer;
- B-02 Mitgliedschaft-Sachbearbeiter;
- B-03 Mitgliedschaft-Reviewer;
- B-04 Publikationsprüfer;

- B-05 Diskussionsleitung;
- B-06 Versammlungsoperator;
- B-07 Citizen-Office Caseworker;
- B-08 Antragsprüfung;
- B-09 Dokumentenprüfer.

(4) R-01 Berechtigungsverwaltung registriert und kontrolliert Berechtigungsakte und Fachgrants. R-01 schafft keine politische Zuständigkeit und darf einen eigenen Akt nicht selbst freigeben.

(5) Klasse T bezeichnet technische Betreiberrollen ohne Parteientscheidungsbefugnis:

- T-01 System Admin;
- T-02 Security Admin.

System- und Sicherheitsadministration sind personell und funktional zu trennen, soweit die konkrete privilegierte Handlung dies erfordert.

§ 3 Serverseitige Autorisierung

(1) Jeder API-Aufruf aus einem Portal-Panel wird serverseitig vor der Ausführung validiert. Die Mindestformel lautet:

```
Auth = f(Role, Org_Scope, Proc_Scope, Validity, Two_Factor) -> {YES | NO}
```

Die konkrete Request-Prüfung bezieht zusätzlich die angeforderte Aktion, das betroffene Objekt, die Entscheidungsgrundlage, etwaige Maker/Checker-Anforderungen und den aktuellen Sicherheitszustand ein.

(2) Ein Frontend-Element darf nur angezeigt werden, wenn die Session die hierfür vom Backend ausgegebenen Capabilities enthält. Die Anzeige ist jedoch niemals Autorisierungsnachweis. Der Backend-Validator entscheidet bei jedem Request erneut anhand des maßgeblichen Zustands.

(3) Clientseitig dürfen keine festen Parteifunktionen oder Rollennamen als Sicherheitslogik hart codiert werden. Die Oberfläche wird aus versionierten Capability-Sets gerendert. Gibt der Backend-Knoten für ein Modul keine Capability zurück, wird das Modul im Frontend nicht gerendert.

(4) Capability-Informationen in einem Session-Token dienen der Darstellung und der Request-Bindung. Widerruf, Ablauf und Sicherheitsunterbrechung müssen serverseitig sofort durchsetzbar bleiben. Ein abgelaufener oder widerrufener Grant darf nicht bis zum regulären Tokenablauf weiterwirken.

§ 4 Mandat, Zugang und Zustände

(1) Politisches oder organisatorisches Mandat und technischer Zugang werden in getrennten Zustandsmodellen geführt. Eine technische Sicherheitsmaßnahme darf einen rechtlich oder satzungsmäßig bestehenden Auftrag nicht beenden.

(2) Bei einer Sicherheitsunterbrechung ist insbesondere zulässig:

- MANDATE_STATE = EFFECTIVE;
- ACCESS_STATE = SECURITY_SUSPENDED;
- SESSIONS = REVOKED.

(3) Die Beendigung eines Mandats, einer Bestellung oder einer unabhängigen Funktion darf nur aus der dafür zuständigen Entscheidung abgeleitet werden. T-01 und T-02 dürfen MANDATE_STATE nicht setzen, ändern oder beenden.

(4) Fachgrants der Klasse B verwenden mindestens die Zustände REQUESTED, CHECKED, ACTIVE, REVALIDATION_PENDING, REVOKED und EXPIRED. Sensible B-Funktionen dürfen nicht unmittelbar vom Antrag in ACTIVE wechseln, wenn die Ausführungsmatrix eine getrennte Prüfung verlangt.

§ 5 PV-01 Management Console

(1) PV-01 Management Console ist die gemeinsame Verwaltungsoberfläche für A-01 bis A-05 sowie R-01. Sie ist kein Parteiorgan. Der sichtbare Funktionsumfang wird dynamisch aus Rolle, Organisationsbereich, Verfahrensbereich, Laufzeit, Beschlusslage und Capability-Satz gebildet.

(2) Kernmodule sind:

- Organe & Beschlüsse: Protokolle und Beschlussreferenzen registrieren, Vorgänge und Aufgaben mit einer Resolution_ID verknüpfen. Der Upload dokumentiert einen bereits gefassten Beschluss und erzeugt nicht selbst die politische Entscheidung. Finalisierte Protokolle dürfen nicht still überschrieben werden.
- Haushalt & Finanzen: nur für ausdrücklich finanzzuständige A-Profile und nur nach Beitrags-/Finanzordnung; Budgetentwürfe, Freigabevorgänge und Zahlungs-/Kontrollschritte werden als getrennte Capabilities dargestellt. PV-01 ersetzt weder Vier-Augen-Prinzip noch die unabhängige Rechnungsprüfung.
- Berechtigungen: zulässige B-Rollen nach geschlossener Delegationsmatrix beantragen beziehungsweise vergeben. Ein Antrag erzeugt einen Grant-Akt in REQUESTED oder CHECKED, nicht durch bloße A-Handlung unmittelbar in ACTIVE.
- Zulassungsfreischaltung R-01: R-01 darf einen geprüften Fachgrant nur dann in ACTIVE überführen, wenn die festgelegte Maker/Checker-Trennung erfüllt ist, der Akt auf eine gültige Entscheidungsgrundlage verweist und R-01 nicht selbst Aussteller des Akts ist.
- Revalidierung: bestehende B-Grants nach Leitungswechsel einzeln bestätigen, ändern oder widerrufen. Eine pauschale Funktion „alle verlängern“ ist unzulässig.
- Audit: Verlauf von Grants, Freigaben und Widerrufen im eigenen zulässigen Org-Scope anzeigen.

(3) A-02 erhält keine Generalverwaltung. Bei einem Mitglied des Bundesvorstands erscheinen nur satzungsmäßige Aufgaben oder ausdrücklich durch Organbeschluss zugewiesene Vorgänge. Entsprechendes gilt für A-05.

(4) Kein Benutzer von PV-01 darf A-, A-I- oder T-Rollen frei erzeugen, den eigenen Scope erweitern, einen eigenen kritischen Akt freigeben oder durch technische Handlung die Wahl, Abwahl oder Bestellung eines Parteiamentes ersetzen.

§ 6 PV-02 Operations Console

(1) PV-02 Operations Console ist die gemeinsame Vorgangs- und Ticketoberfläche für aktive B-Grants B-01 bis B-09. Es werden keine neun getrennten Anwendungen betrieben. Tickettyp, Datenfelder, Aktionen und Scope werden aus dem aktiven Grant und der jeweiligen Workflow-Definition geladen.

(2) Die Aufgabenwarteschlange darf nur Vorgänge anbieten, deren Typ und Scope dem aktiven Grant entsprechen. Mit Vorgang sperren / in Arbeit nehmen wird der Vorgang der handelnden Person zugeordnet und gegen parallele Bearbeitung geschützt.

(3) Für Mitgliedschaftsanträge gelten insbesondere:

- B-01 und B-02 dürfen Daten und Nachweise prüfen, Mängel melden und einen Vorgang zur nächsten Prüfstufe geben;
- B-03 darf eine Zweitprüfung nur durchführen, wenn die Person nicht die maßgebliche Erstbearbeitung vorgenommen hat;

- eine Fachprüfung darf nicht allein die satzungsmäßige Aufnahme- oder Ablehnungsentscheidung ersetzen; nach § 3 der Satzung trifft diese der zuständige Vorstand, solange ein solcher nicht besteht der Bundesvorstand. Der Fachworkflow endet deshalb in READY_FOR_BOARD_APPROVAL oder einem gleichwertigen Vorbereitungszustand.

(4) B-05 darf in dem konkret zugewiesenen Diskussionsraum Inhalte nach der geltenden Moderationsregel verbergen und Verwarnhinweise dokumentieren. B-05 darf keine Mitgliedschaft beenden, keine Wahlrechte entziehen und keine disziplinarische Sanktion außerhalb der Moderationsregel verhängen.

(5) B-04 und B-08 dürfen veröffentlichungs- oder antragsbezogene formale Prüfungen innerhalb ihrer zugewiesenen Kompetenz durchführen. Eine formale Prüfung darf nicht zur politischen oder ideologischen Inhaltskontrolle werden. Wo eine materielle Organentscheidung erforderlich ist, endet der Fachworkflow vor dieser Entscheidung. Offizielle Veröffentlichungen werden nur durch das nach Satzung, Geschäftsordnung oder einer gesonderten Publikationsordnung zuständige Organ beziehungsweise eine dort ausdrücklich bezeichnete Freigabestelle endgültig freigegeben; der Publikationsprüfer erhält nicht allein aufgrund von B-04 eine politische Veröffentlichungsbefugnis.

(6) B-06, B-07 und B-09 arbeiten ausschließlich in dem zugewiesenen Versammlungs-, Fall- oder Dokumentenscope. Sie erhalten keine darüber hinausgehende Verwaltungsbefugnis.

§ 7 PV-03 Independent Oversight Console

(1) PV-03 Independent Oversight Console ist der vom Verwaltungs- und Betreiberbereich getrennte Arbeitsbereich für AI-01 bis AI-03.

(2) PV-03 ist gegenüber den Kerndaten der Partei grundsätzlich kontrollierend und nicht administrativ. Eigene unabhängige Verfahrensdaten dürfen innerhalb der jeweiligen Zuständigkeit geschrieben werden.

(3) AI-02 kann in einer zugewiesenen Verfahrensakte Prozesshandlungen dokumentieren und Entscheidungen/Urteile ablegen. Daraus resultierende technische Maßnahmen werden über den geregelten Ausführungsweg umgesetzt; das Schiedsgericht sperrt Benutzer nicht unmittelbar über die Sicherheitsadministration.

(4) AI-01 kann Prüfvermerke, Feststellungen und Berichte im eigenen Prüfauftrag dokumentieren und veröffentlichen. Ein Revisionszugang berechtigt nicht zur Veränderung, Löschung oder Freigabe der geprüften Finanzvorgänge.

(5) Der unabhängige Auditbereich ermöglicht den nach Prüfauftrag berechtigten A-I-Funktionen die Einsicht beziehungsweise den Export unveränderbarer Auditdaten. Besonders geschützte Inhaltsdaten werden nur gezeigt, soweit sie für den Prüfauftrag erforderlich sind. Auditdaten dürfen durch PV-03 nicht gelöscht oder umgeschrieben werden.

(6) Der Export besonders sensibler Systemlogs setzt erhöhte Authentisierung voraus; die technische Spezifikation kann hierfür einen Hardware-gebundenen Faktor verlangen.

§ 8 PV-04 Infrastructure Console

(1) PV-04 Infrastructure Console ist ausschließlich T-01 zugänglich und dient Betrieb, Deployment, Wartung, Datenbankmigrationen und der technischen Vollziehung validierter A-/A-I-Berechtigungsakte.

(2) Das Modul Activation Engine darf eine technische Aktivierung nur ausführen, wenn der Berechtigungsakt im dafür vorgesehenen validierten Zustand steht. T-01 darf keinen politischen oder parteiinternen Akt erzeugen und keine Rolle in der Datenbank manuell vergeben.

(3) Datenbankmigrationen, Service-Restarts und vergleichbare Eingriffe dürfen nur über dokumentierte technische Verfahren, genehmigte Change-/Maintenance-Prozesse und vollständiges Audit erfolgen. Direkte SQL-Manipulationen der Berechtigungstabellen zur Umgehung der Autorisierungslogik sind unzulässig.

§ 9 PV-05 Security Command Center

(1) PV-05 Security Command Center ist ausschließlich T-02 zugänglich. Es dient der Abwehr konkreter Sicherheitsvorfälle und darf nicht als Disziplinar- oder Organisationsinstrument verwendet werden.

(2) Bei einem dokumentierten Sicherheitsvorfall kann T-02 EMERGENCY SUSPENSION auslösen. Dadurch werden ausschließlich technische Zustände verändert: ACCESS_STATE = SECURITY_SUSPENDED; aktive Sessions werden unverzüglich widerrufen. MANDATE_STATE bleibt unberührt.

(3) Die Sicherheitsunterbrechung erzeugt unverzüglich einen unveränderbaren Incident Record und eine Benachrichtigung an den unabhängigen Kontrollpfad. Die unabhängige Prüfung ist grundsätzlich binnen 24 Stunden einzuleiten und nach der geltenden Sicherheitsordnung abzuschließen.

(4) Eine Revalidierung des Sicherheitskanals und eine Wiederfreigabe setzen den dokumentierten Incident-Abschluss beziehungsweise die vorgeschriebene unabhängige Prüfung voraus. T-02 darf die eigene Maßnahme nicht still löschen und keine parteipolitischen Statusdaten verändern.

§ 10 Berechtigungsverwaltung und Berechtigungsakt

(1) R-01 ist eine formale Registrierungs- und Kontrollstelle, kein Parteiorgan. Die Bestellung, Unvereinbarkeiten und unabhängige A-I-Prüfspur richten sich nach Satzung und dieser Ordnung.

(2) Ein A- oder A-I-Zugang erfordert einen Berechtigungsakt mit mindestens: Akt-ID, Person/Kontoreferenz, Rollenprofil, Org-Scope, gegebenenfalls Proc-Scope, Beschluss-/Wahlreferenz, ausstellendes Organ, Datum, Annahme, Wirksamkeitsbeginn, festes Ende oder dokumentierte Fortdauergrundlage, registrierende und kontrollierende Person, Status, Betreiberzustellung, Aktivierungszeit sowie Sperr-/Widerrufsreferenz.

(3) R-01 darf nur eine bereits bestehende Zuständigkeit registrieren. OCR, automatisierte Extraktion oder ein hochgeladenes Protokoll können die Erfassung unterstützen, erzeugen aber keine Befugnis.

(4) A- und A-I-Akte benötigen getrennte Erfassung und Kontrolle. Für A-I ist ein von der Parteiführung funktional unabhängiger Registrierungs- und Kontrollpfad vorzusehen. Die allgemeine R-Stelle wird nach Satzung/Ordnung bestellt; die unabhängige A-I-Prüfspur darf weder durch Vorstandsanweisung verzögert noch inhaltlich umgedeutet werden. Eine formale Zurückweisung ist nur mit dokumentiertem Grundcode und überprüfbarem Nachweis zulässig.

§ 11 Aktivierung, Delegation, Revalidierung und Ende

(1) Für A und A-I gilt grundsätzlich: wirksame Wahl/Bestellung/Beauftragung -> Registrierung/Kontrolle -> Berechtigungsakt -> authentifizierte Zustellung -> technische Vollziehung durch T-01 -> aktiver Zugang.

(2) Der technische Betreiber bestätigt den Eingang eines vollständigen, authentisierten A-/A-I-Akts unverzüglich und vollzieht ihn grundsätzlich unverzüglich, spätestens binnen 24 fortlaufenden Stunden. Wochenenden und Feiertage sind eingeschlossen. Betreibervertrag und Betriebsverfahren regeln Bereitschaft, Ersatzkanal, Fehlercodes, Eskalation und Nachweis. Diese Frist ist ein organisations- und vertragsrechtlicher Standard dieser Ordnung, keine behauptete gesetzliche Frist.

(3) B-Grants werden nur über die geschlossene Delegationsmatrix beantragt. Die Matrix berücksichtigt Role, Org_Scope, Proc_Scope, Validity und erforderliche Prüfstufen. Eine einfache hierarchische Regel „höherer Scope darf alles darunter“ ist unzulässig.

(4) Bei einem Leitungswechsel werden fortbestehende B-Grants nicht automatisch zu persönlichen Rechten des Nachfolgers und nicht automatisch gelöscht. Soweit die Ausführungsmatrix dies vorsieht, wechseln sie in REVALIDATION_PENDING. Folgenreiche Aktionen bleiben bis zur Einzelprüfung gesperrt; eine pauschale Massenbestätigung ist ausgeschlossen.

(5) Ablauf, Widerruf oder Ende der zugrunde liegenden Bestellung beendet den technischen Zugang nach dem festgelegten Verfahren. Historische Akte und Auditspuren werden nicht überschrieben.

§ 12 Audit, Vier-Augen-Prinzip und Unvereinbarkeiten

(1) Kritische Freigaben müssen Maker/Checker-Trennung unterstützen. Niemand darf seinen eigenen kritischen Akt genehmigen oder eine Sicherheitsmaßnahme allein ausführen und zugleich deren unabhängige Kontrolle ersetzen.

(2) Auditdaten enthalten mindestens Identität beziehungsweise technische Kontoreferenz des Handelnden, Zeit, Aktion, Objekt, Scope, Entscheidungs-/Aktreferenz, Ergebnis und gegebenenfalls Checker. Auditdaten sind gegen nachträgliche Veränderung zu schützen.

(3) Besonders geschützte Daten dürfen im Audit nur im erforderlichen Umfang erscheinen. Geheime Stimmen und eine Zuordnung geheimer Stimmen zu Personen dürfen nicht protokolliert oder über Betreiberpanels zugänglich gemacht werden.

§ 13 Technischer Betreiber und Verbot universeller Administrationsmacht

(1) EPD Plattform e.V. betreibt die technische Infrastruktur auf vertraglicher Grundlage. Der Betreiber ist kein Parteiorgan und erhält durch Betrieb, Systemadministration oder Sicherheitsadministration keine politischen, mitgliedschaftlichen, gerichtlichen oder finanziellen Entscheidungsbefugnisse.

(2) Eine universelle Rolle ADMIN_ALL, ein dauerhaftes Superadmin-Konto oder ein Mechanismus, mit dem eine einzelne Person beliebige Parteirechte vergeben kann, ist unzulässig.

(3) Notfallzugänge sind zweckgebunden, zeitlich eng befristet, besonders protokolliert und nachträglich unabhängig zu kontrollieren. Sie dürfen keine politische Zuständigkeit erzeugen.

§ 14 Ersteinrichtung und Wiederanlauf

(1) Die erste technische Inbetriebnahme der fünf Panels wird aufgrund eines dokumentierten Initialbeschlusses durchgeführt. Mindestens zwei voneinander unabhängige Personen bestätigen die Zuordnung der initialen Berechtigungsakte. Der Betreiber richtet nur die technisch erforderlichen T-Funktionen und die validierten initialen Zugänge ein.

(2) Scheitert die Initialisierung, bleibt der Versuch vollständig protokolliert. Ein erneuter Bootstrap ist nur aufgrund eines neuen ausdrücklich dokumentierten Beschlusses und erneuter getrennter Kontrolle zulässig. Ein fehlgeschlagener Bootstrap darf nicht in einen dauerhaften Notfall-Superadmin überführt werden.

(3) Nach dokumentierter Abnahme enden Bootstrap-Sonderrechte.

§ 15 Technisches Ausführungsregister und Änderungen

- (1) Die fünf Panel-IDs PV-01 bis PV-05 bezeichnen technische Arbeitsoberflächen. Rollenprofile, Capabilities, Buttons, API-Aktionen, Routen, Datenobjekte und detaillierte Workflow-Zustände werden in einem versionierten technischen Ausführungsregister geführt.
- (2) Das technische Ausführungsregister darf die in Satzung und dieser Ordnung festgelegten Zuständigkeiten nur konkretisieren oder verengen, niemals erweitern. Eine neue UI-Schaltfläche oder Route erzeugt keine neue materielle Befugnis.
- (3) Änderungen der technischen Darstellung, internen Route oder Komponentenzuordnung bedürfen keiner Satzungsänderung, solange Zuständigkeit, Unabhängigkeit, Scope-Grenzen, Maker/Checker-Regeln und Verbote dieser Ordnung unverändert bleiben.
- (4) Die Anlage „PV-01...PV-05 Panel- und Aktionsmatrix“ ist das initiale technische Ausführungsregister. Sie ist für die Implementierung verbindliche Spezifikation, aber kein selbständiger Ursprung politischer Zuständigkeit.

§ 16 Inkrafttreten

- (1) Diese Ordnung tritt mit dem satzungsmäßig zuständigen Beschluss in Kraft.
- (2) Vor einer produktiven Aktivierung sind Betreibervertrag, technische Ausführungsmatrix, Berechtigungsakt-Schema, Auditregeln, Incident-Verfahren und Bootstrap-Abnahme miteinander abzugleichen.
- (3) Bis zur produktiven Freigabe bleiben alle in dieser Ordnung beschriebenen Panels und Rollen reine Soll-Spezifikation.

Rechtlicher Arbeitsstand

Diese Ordnung ist ein Governance- und Technikentwurf. Maßgeblich bleiben insbesondere die zwingenden Vorgaben des Parteiengesetzes und die beschlossene Satzung. Die fünf Panelbezeichnungen sind technische Referenzen, keine gesetzlichen oder parteirechtlichen Organe.

Rechtliche Arbeitsgrundlagen: Parteiengesetz, insbesondere §§ 6, 9, 11 und 14; Unterlagensammlung der Bundeswahlleiterin nach § 6 Abs. 3 PartG.