Bearbeitungsstand: 08.02.2022

Berechtigungs- und Rollenkonzept für die *Kommweb Beteiligungsmanagementsoftware*

1. Einführung

Das *Kommweb-System* des Herstellers Beratungsgesellschaft für Beteiligungsverwaltung Leipzig mbH (bbvl) ist eine Standard-Beteiligungsmanagementsoftware. Sie speichert zu einzelnen Beteiligungsunternehmen Stammdaten und Bewegungsdaten (insbesondere Wirtschaftsplan-, Quartals- und Jahresabschlussdaten) in einer Datenbank.

Die *Kommweb Beteiligungsmanagementsoftware* wurde im internen Netz der FHH durch Dataport installiert und ist somit vor Zugriff von außerhalb abgeschirmt. Der Zugriff zum System ist nur für die durch die Fachliche Leitstelle angelegte Nutzer/Innen der Fachbehörden und der HGV möglich und erfolgt passwortgeschützt. Die Beteiligungsunternehmen geben ihre Daten über ein externes, webbasiertes (ebenfalls passwortgeschütztes) Tool in das System ein und haben insofern keinen direkten Zugriff auf das Verfahren.

Die *Kommweb Beteiligungsmanagementsoftware* steuert den Zugriff auf die Daten in der Datenbank über ein zweistufiges Berechtigungskonzept. Die erste Stufe dient der Authentifizierung. Hier wird geregelt, ob der/die Benutzer/In berechtigt ist, sich am System anzumelden. Die zweite Stufe ist die Autorisierung. Hier wird gesteuert, was der/die Nutzer/In sehen darf bzw. welchen Zugriff er worauf hat.

2. Authentifizierung, Autorisierung und Berechtigungsverwaltung

Das *Kommweb-System* bietet eine eigene Authentifizierung an. Hierzu werden im Administratorenbereich durch die Fachliche Leitstelle einzelne Nutzer angelegt und mit einem Startpasswort versehen. Zusätzlich können im System Mindestkriterien an die Passwortqualität (gemäß FHH Passwort-RL vom 10.10.2007, MittVw Seite 96) definiert werden.

Die Autorisierung erfolgt ebenfalls im *Kommweb-System*. Die Berechtigungen werden von der Fachlichen Leitstelle im Menü Administration - Allgemeines vergeben. Angelegte Nutzer/Innen werden einzelnen Benutzergruppen zugeordnet. Ein Benutzer besitzt keinerlei Berechtigungen solange er nicht mindestens einer Benutzergruppe zugewiesen ist. Nur über Benutzergruppen können Rechte vergeben werden. Sollen Einzelberechtigungen vergeben werden, ist dies über die Anlage einer separaten Benutzergruppe möglich.

Die Anwender/Innen aus den Fachbehörden und der HGV können sich selbst im System registrieren und wählen dabei die für ihren jeweiligen Zuständigkeitsbereich erforderlichen Rechte zum Zwecke der Freigabe durch die Fachliche Leitstelle aus. Der Zugriff auf Daten und Funktionen des Systems besteht jedoch erst nach einer Prüfung und Freigabe durch die Fachliche Leitstelle. Diese legt für die einzelnen Benutzergruppen die Berechtigungen für die Objekte fest. Die Objekte haben für ihre einzelnen Ausprägungen feste Identifikationsmerkmale, die eineindeutig sind. Diese können aus der Datenbank (z. B. für die Menüpunkte) oder aus einer Konfigurationsdatei bezogen werden.

3. Rechtekategorien im *Kommweb-System*

3.1 Überblick

Das *Kommweb-System* kennt insgesamt acht Rechtekategorien, wobei jedes Recht definierten Benutzergruppen zugewiesen werden kann. Diese Rechtekategorien sind:

1. Menürechte
2. Feldrechte
3. Firmenrechte
4. Dokumentartrechte
5. Formularrechte
6. Controlling-Berichtrechte
7. Berichtsarten-Rechte
8. Vorgangsautomat

Die Berechtigungen lassen sich entlang dieser Rechtekategorien mit folgenden Zugriffsrechten abgestuft konkreter ausgestalten:

- *Kein Zugriff*
- *Lesen*
- *Ändern*
- *Hinzufügen*
- *Löschen*

Die übergeordneten Zugriffsrechte beinhalten jeweils die untergeordneten Zugriffsrechte. So beinhaltet beispielsweise das Recht *Ändern* automatisch das Recht *Lesen*. Das Recht *Löschen* ist das höchste Recht und beinhaltet alle anderen Rechte.

Die Rechtekategorien 2-7 werden als „einschränkende“ Rechte bezeichnet, da sie die vergebenen Menürechte (Rechtekategorie 1) nur weiter einschränken können. Die Menürechte besitzen dabei die meisten Ausprägungen. Die übrigen Rechtekategorien (2-7) schränken die Menürechte dann nur noch weiter ein, sodass hier nur die Ausprägungen *Zugriff* oder *Kein Zugriff* vergeben werden können. Lediglich die Feldrechte weichen hier etwas ab, diese können die Ausprägungen *Lesen* (als Pendant zu *Zugriff*), *Kein Zugriff* und *Ändern* annehmen. Der Vorgangsautomat weicht von der gesamten Logik ab und stellt in sich eine eigenständige Rechtekategorie dar.

Rechtekategorie	**Mögliche Ausprägungen**
1. Menürechte	Kein Zugriff Lesen Ändern Hinzufügen Löschen
2. Feldrechte	Kein Zugriff Lesen Ändern
3. Firmenrechte	Kein Zugriff Zugriff
4. Dokumentartrechte	Kein Zugriff Zugriff

Rechtekategorie	Mögliche Ausprägungen
5. Formularrechte	Kein Zugriff Zugriff
6. Controlling-Berichtrechte	Kein Zugriff Zugriff
7. Berichtsarten-Rechte	Kein Zugriff Zugriff

3.2 Systemeinstellungen

Für alle Berechtigungen – außer Menürechte und Vorgangsautomat – gilt je eine Standardeinstellung, die vergeben wird, wenn keine Einstellung vorgenommen wurde. Dabei kann in den Systemeinstellungen definiert werden, ob diese Standardeinstellung Zugriff verweigert oder Zugriff gewährt. Dementsprechend wird über diese Systemeinstellung festgelegt, ob für die Firmen-, Dokumentenart-, Formular-, Controlling-Berichts- und Berichtsarten-Rechte der Standardwert *Zugriff* (für Feldrechte *Lesen* oder *Ändern*) oder *Kein Zugriff* lautet.

Für die Menürechte wird diese Systemeinstellung konstant mit *Kein Zugriff* festgelegt und kann auch nicht verändert werden. Andernfalls könnten durch eine standardmäßige Vergabe von *Zugriff* Konstellationen entstehen, die der Datensicherheit in der *Kommweb* widersprechen.

Technisch erfolgt die Umsetzung dabei so, dass noch nicht vergebene Berechtigungen auch keinen Datensatz in der jeweiligen Tabelle darstellen. Erst mit expliziter Festlegung eines Rechts wird ein Datensatz erzeugt. Im Umkehrschluss bedeutet das, dass das Rechteobjekt in der *Kommweb* ggf. einen Umweg über die Systemeinstellung gehen muss, um die jeweils gültige Berechtigung zu ermitteln.

3.3 Allgemeingültige Einstellungen

Für alle nachfolgenden Rechtekategorien gilt im *Kommweb-System*:

- Solange keine Berechtigung definiert ist, gilt der in den Systemeinstellungen definierte Standardwert. In der Administration wird dann neben den tatsächlichen Werten eine letzte Spalte namens Standardeinstellung angezeigt, die für die bisher nicht vergebenen Rechte aktiviert ist. Gleichzeitig wird über der Konfigurationsmatrix ein Text angezeigt, der die Standardeinstellung mitteilt: Die Standardeinstellung für … *[Recht]* ist *Kein Zugriff*/*Zugriff*/*etc.*
- Wenn der Administrator eine bereits vergebene Berechtigung wieder auf die Standardeinstellung zurücksetzen möchte, kann er entsprechend diese aktivieren. In der Datenbank wird dadurch der zugehörige Berechtigungseintrag entfernt.
- Es besteht die Möglichkeit, die Berechtigungen nicht nur einzeln zuzuweisen, sondern auch für alle zu setzen (*Auswahl für alle übernehmen*).

3.4 Menürechte

Über die Menürechte wird definiert, welche Zugriffsrechte auf die einzelnen *Kommweb*-Menüs gelten. Hier werden also die wesentlichen Berechtigungen definiert, d. h. das prinzipielle Verarbeitungsrecht vergeben. Über die übrigen einschränkenden Rechte (2-7) kann diese Zugriffsberechtigung nun lediglich weiter eingeschränkt werden.

Zeige 1 bis 12 von 12 Einträgen

Menü-Name	kein Zugriff	lesen	ändern	hinzufügen	löschen	für alle Untermenüs
Unternehmen	○	◉	○	○	○	☐
Stadt	○	◉	○	○	○	☐
Administration	◉	○	○	○	○	☐
Analyse	○	◉	○	○	○	☐
Berichte	○	◉	○	○	○	☐
Controlling	○	◉	○	○	○	☐
GF-Verträge	◉	○	○	○	○	☐
Hilfe	○	◉	○	○	○	
Gremiendienst	◉	○	○	○	○	
Aufgaben	○	◉	○	○	○	☐
Personen	○	◉	○	○	○	☐
Einstieg Extern	○	◉	○	○	○	

Bei den meisten Menüs werden zusätzlich immer Firmenrechte beachtet werden müssen. Es existieren allerdings auch Menüs, die keinen Firmenbezug besitzen, z. B. die Administrationsmenüs oder auch die Hauptmenüpunkte. Für diese Menüs gelten innerhalb der Benutzergruppe nur die Menürechte, die definierten Firmenrechte werden hierbei ignoriert.

Das Menü GF-Verträge enthält Informationen und Dokumente (z.B. Anstellungsverträge, Ziel- oder Tantiemevereinbarungen) zu den Geschäftsleitungen der Beteiligungsunternehmen. Der Zugang zu diesem Menü erfordert eine separate Authentifizierung über ein Passwort, das durch die Fachliche Leistelle vergeben wird.

3.5 Feldrechte

Auch auf Ebene der einzelnen Stammdaten-Felder können die Berechtigungen definiert werden. Dabei schränken die Feldrechte die Menürechte weiter ein, weshalb nur folgende Ausprägungen möglich sind: *Kein Zugriff*, *Lesen, Ändern*.

3.6 Firmenrechte

Mithilfe der Firmenrechte kann gesteuert werden, welche Beteiligungsunternehmen die Anwender/In in der *Kommweb* verarbeiten darf. Zur Definition der jeweiligen Berechtigung muss das Unternehmen bereits angelegt sein.

3.7 Dokumentartrechte

Für Beteiligungsunternehmen können bestimmte Dokumente (z.B. Gesellschaftsvertrag, Satzung) in der *Kommweb* gespeichert werden. Über die Dokumentartrechte kann nun definiert werden, auf welche Dokumentarten der Anwender ggf. keinen Zugriff erhalten soll. Demnach wird hier ebenfalls nur zwischen *Zugriff* und *kein Zugriff* unterschieden. Die Darstellung der Administration in der *Kommweb* ist analog der Firmenrechte.

3.8 Formularrechte

Mit den Formularrechten können Berichtsrechte weiter eingeschränkt werden. Hier kann innerhalb der jeweiligen Berichte der Zugriff weiter auf bestimmte Formulare eingeschränkt werden. Auch hier wird zwischen *Zugriff* und *kein Zugriff* unterschieden und die Darstellung der Administration in der *Kommweb* ist analog der Firmenrechte.

3.9 Controlling-Berichtsrechte

Ähnlich den Formularrechten kann über Controlling-Berichtsrechte definiert werden, welche Berichte im Controlling (z.B. Jahresabschluss oder Quartalsberichte) von der Benutzergruppe gesehen werden dürfen, d. h. *Zugriff* oder *kein Zugriff* besteht. Die Darstellung der Administration in der *Kommweb* ist analog der Firmenrechte.

3.10 Berichtsarten-Rechte

Hier wird definiert, ob die jeweilige Benutzergruppe Zugriff auf einen (Auswertungs-)Bericht (z.B. Beteiligungsbericht), besitzt oder nicht, d. h. *Zugriff* oder *kein Zugriff*. Die Darstellung der Administration in der *Kommweb* ist analog der Firmenrechte.

Bei den Berichtsarten ist zu erwähnen, dass innerhalb der Berichtsdefinition (Berichte > Allgemeiner Aufbau) zusätzlich keine Feldrechte geprüft werden. Wenn der definierte Bericht aber dann erzeugt (Berichte > Daten für Bericht erzeugen) oder angezeigt (Berichte > Daten

für Bericht bearbeiten) wird, erfolgt die Prüfung auf die notwendigen Feldrechte. Fehlen hier einzelne Rechte, wird das Feld im Bericht zwar angezeigt, allerdings statt des tatsächlichen Wertes wird „Keine Berechtigung“ ausgegeben. Tritt dies für mindestens einen Wert auf, darf auch keine Freigabe mehr möglich sein (Daten freigeben ist gesperrt).

3.11 Vorgangsautomat

Der Vorgangsautomat dient der Definition des Vier-Augen-Prinzips. Ein Vier-Augen-Prinzip ist bei verschiedene Vorgängen (z.B. ein Beteiligungsunternehmen oder Gremium zu löschen) vorgesehen und im System bereits verankert. Zusätzliche Kontrollmechanismen können, wobei auch umfangreichere Prinzipien definierbar sind, im System angelegt werden. Hier sind mehrere Einstellungen notwendig:

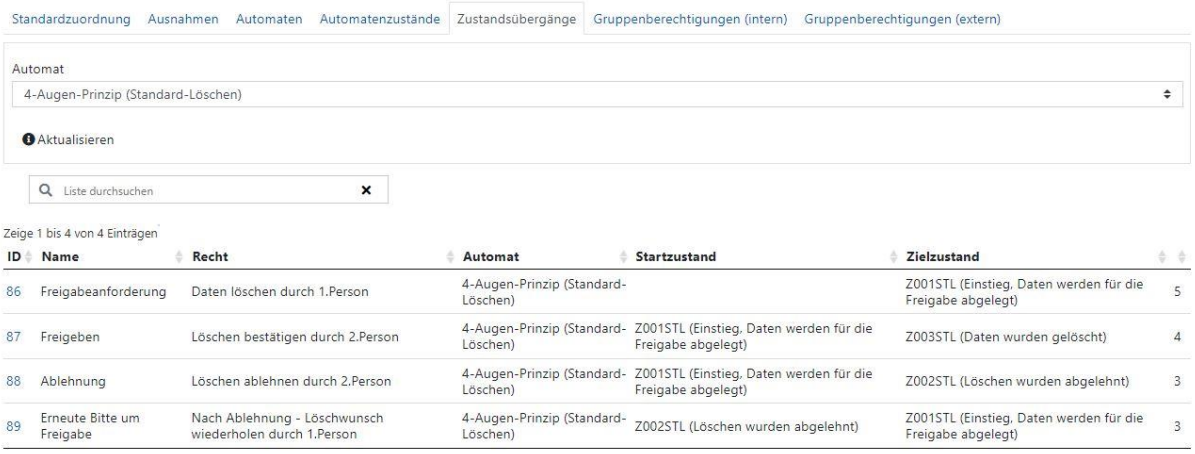
- Automaten: Hier wird der eigentliche Automat namentlich definiert, wobei ein Automat für mehrere Menüs gelten kann, aber auch für jedes Menü ein eigener Automat möglich ist.

ID	Name	Beschreibung	Hinweis	
92	4-Augen-Prinzip (Standard-Löschen)	Standardautomat für das Löschen von Datensätzen	keine	Bearbeiten
91	4-Augen-Prinzip (Standard)	Standard 4 Augenprinzip	keine	Bearbeiten
90	Controlling	Workflow für das Einsammeln von Daten aus dem externen Bereich	keine	Bearbeiten

- Automatenzustände: Für jeden definierten Automaten werden hier die einzelnen Zustände definiert, wobei spezielle Zustände (Einstiegsstatus, Endstatus des Automaten, Bearbeitungsmodus, Zwischenspeichern) festgelegt werden können

ID	Automat	Position	Name	Beschreibung	Optionen
79	4-Augen-Prinzip (Standard-Löschen)	1	Z001STL	Einstieg, Daten werden für die Freigabe abgelegt	Einstiegsstatus
80	4-Augen-Prinzip (Standard-Löschen)	2	Z002STL	Löschen wurden abgelehnt	
81	4-Augen-Prinzip (Standard-Löschen)	3	Z003STL	Daten wurden gelöscht	Endstatus des Automaten

- Zustandsübergänge: Hier erfolgt die Definition der einzelnen Übergänge zwischen den definierten Zuständen eines Automaten



ID	Name	Recht	Automat	Startzustand	Zielzustand	
86	Freigabeanforderung	Daten löschen durch 1.Person	4-Augen-Prinzip (Standard-Löschen)		Z001STL (Einstieg, Daten werden für die Freigabe abgelegt)	5
87	Freigeben	Löschen bestätigen durch 2.Person	4-Augen-Prinzip (Standard-Löschen)	Z001STL (Einstieg, Daten werden für die Freigabe abgelegt)	Z003STL (Daten wurden gelöscht)	4
88	Ablehnung	Löschen ablehnen durch 2.Person	4-Augen-Prinzip (Standard-Löschen)	Z001STL (Einstieg, Daten werden für die Freigabe abgelegt)	Z002STL (Löschen wurden abgelehnt)	3
89	Erneute Bitte um Freigabe	Nach Ablehnung - Löschwunsch wiederholen durch 1.Person	4-Augen-Prinzip (Standard-Löschen)	Z002STL (Löschen wurden abgelehnt)	Z001STL (Einstieg, Daten werden für die Freigabe abgelegt)	3

- Gruppenberechtigungen: Abschließend werden den Berechtigungsgruppen Rechte auf einzelne Zustandsübergänge gegeben

4. Berechtigungsverwaltung

Nach den oben dargestellten Prinzipien lassen sich die jeweiligen Berechtigungen also gruppen- oder personenspezifisch nach den Bedürfnissen der Fachbehörden individuell ausgestalten. So können die Rechte im System feingegliedert sowohl beteiligungs- als auch informationsspezifisch vergeben werden. Dadurch können gruppenspezifische Rollen entlang der drei Dimensionen

1. Art des Rechtes (z.B. Lesen, Ändern, Hinzufügen, Löschen, usw.),
2. konkrete Beteiligung (zugewiesene Rechte auf bestimmte Beteiligungen) und
3. Informationstyp (z.B. Stammdaten, Controlling Daten, Geschäftsführer-angelegenheiten)

flexibel ausgestaltet werden. Beim Informationstyp können zusätzlich je Menü einzelne Datenfelder berechtigt werden, so dass ausgewählte Nutzer/Innen beispielsweise zwar die Stammdaten zu einem bestimmten Unternehmen sehen können, innerhalb der Menüs Basisinformationen aber z.B. nicht die dazugehörigen Handelsregisterdaten. Ebenso lässt sich einstellen, dass einzelne Nutzer/Innen z.B. grundsätzlich den Jahresabschluss sehen dürfen, aber dort z.B. keine Berechtigung auf das Blatt „Finanzplan“ erhalten.

Die *Kommweb Beteiligungsmanagementsoftware* wird durch verschiedene Akteure der FHH genutzt, denen entsprechende Nutzungsrechte zur Aufgabenwahrnehmung im Rahmen ihrer jeweiligen Zuständigkeit durch die Fachliche Leitstelle eingerichtet werden. Insbesondere werden Nutzungsrechte an folgende Beschäftigtengruppen übertragen:

- FHH-Beschäftigte in den Fachbehörden mit Aufgaben im Beteiligungsmanagement oder damit zusammenhängenden Haushaltsangelegenheiten,

- Zentrale Stellen mit besonderen zentralen Aufgaben (z.B. Finanzbehörde – Fachliche Leitstelle, Grundsatzbereiche, erweitertes Verantwortungsmodell, Portfolioanalyseeinheit, Jahres- und Konzernabschluss; Senatskanzlei; Konzernholding HGV),
- Systemadministration (Fachliche Leitstelle, IT-Dienstleister),
- Prüfer/Innen des Rechnungshofes und der zuständigen Innenrevisionen

Der Umfang der Nutzungsrechte, die den einzelnen Nutzer/Innen übertragen werden, orientiert sich dabei eng an den konkreten Aufgaben und Zuständigkeiten der jeweiligen Beschäftigten.