Wolters Kluwer

When you have to be right

AnNoText

Berechtigungs-management

Datum: 23. Dezember 2021

Inhaltsverzeichnis

1 Glossar

Nice to know:
Hier erfahren Sie interessante Randinformationen zum Thema.

Best Practice:
In den Best Practice Rubriken zeigen wir Ihnen, wie unsere Software AnNoText Sie bei den spezifischen Anforderungen unterstützt.

2 Was versteht man unter Berechtigungsmanagement?

Eine einheitliche Definition dafür, was genau unter „Berechtigungsmanagement“ zu verstehen ist, existiert nicht. Wir sprechen im Allgemeinen von der Organisation der Zugriffsmöglichkeiten von bestimmten Personen auf bestimmte Informationen unter Einsatz von technologischen Mitteln.

Gemäß der Definition des Bundesamtes für Sicherheit in der Informationstechnik geht es beim Berechtigungsmanagement darum, ob und wie „Benutzer oder IT-Komponenten auf Informationen oder Dienste zugreifen und diese benutzen dürfen, ihnen also basierend auf dem Benutzerprofil Zutritt, Zugang oder Zugriff zu gewähren oder zu verweigern ist. Berechtigungsmanagement bezeichnet die Prozesse, die für Zuweisung, Entzug und Kontrolle der Rechte erforderlich sind.“[1]

Während z. B. eine Firewall Sie vor externen Gefahren schützt, ist das Ziel des Berechtigungsmanagements, dass interne Anwender:innen ausschließlich auf die IT-Ressourcen und Informationen zugreifen können, die sie für ihre Arbeit benötigen und für die sie autorisiert sind. Unautorisierten Benutzer:innen soll der Zugriff verwehrt werden.

Nice to know
Das Bundesamt für Sicherheit in der Informationstechnik definiert in einem eigenen Baustein ORP4 (ORP.4: Identitäts- und Berechtigungsmanagement) die Anforderungen an den Zugang zu schützenswerten Ressourcen einer Institution. Den vollständigen Leitfaden erhalten Sie auf der Website des BSI.

[1] ORP: Organisation und Personal ORP.4: Identitäts- und Berechtigungsmanagement, https://www.bsi.bund.de/

3 Warum sollte ein Berechtigungsmanagement eingesetzt werden?

Die wachsende Bedeutung des Datenschutzes und die damit verbundenen regulatorischen Vorgaben sind insbesondere für Kanzleien relevant. Zum einen begründet der tägliche Umgang mit vertraulichen Informationen ein hohes Schutzniveau. Aber auch aus Gründen der Compliance und des Berufsrechts (z.B. §2 BORA Berufsordnung für Rechtsanwälte) sind Kanzleien aufgefordert, die Zugriffe auf Mandantendaten für Rechtsanwält:innen als auch für administrativ Mitarbeitende restriktiv zu organisieren.

Ergänzend ergibt sich aus der Datenschutzgrundverordnung DSGVO ein gesetzlicher Schutzanspruch für sensible Daten. Zu den Grundsätzen der Datenverarbeitung gehört u. a. der Grundsatz der Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f, 32 Abs. 1 lit. b DSGVO). Werden demnach personenbezogene Daten verarbeitet, müssen ihre Integrität und Vertraulichkeit hinreichend gewährleistet sein. Dazu gehört auch, dass Unberechtigte keinen Zugang zu diesen Informationen haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können.

Mögliche Gefahren für Ihre Daten kommen in vielen Fällen nicht von außen, sondern von innen. Denn häufig geht die Gefahr für Cyber-Kriminalität von unwissenden Mitarbeitenden innerhalb der Kanzlei aus. In bestimmten Fällen führt Datendiebstahl dadurch zur Katastrophe, dass Zugriffsrechte existieren, die eigentlich nicht (mehr) bestehen sollten. Doch auch wenn es für die Vergabe von Zugriffsberechtigungen einen strukturierten Prozess gibt, wird die Deaktivierung von Zugriffsrechten in vielen Kanzleien allzu oft vergessen. Referatswechsel, Kanzlei-Austritte und die Vergabe von Sonderrechten münden in einer uneinheitlichen (und nicht Compliance-konformen) Berechtigungslandschaft.

3.1 Prüfpunkt: Prozesse beim Berechtigungsmanagement

Sollte in Ihrer Kanzlei ein Konzept zum Berechtigungsmanagement nur unzureichend definiert oder umgesetzt sein, so ist nicht gewährleistet, dass mögliche Zugriffe auf Informationen auf das erforderliche Maß eingeschränkt sind. Ein Verstoß gegen die Prinzipien „Need-to-Know“ bzw. „Least-Privilege“ liegt vor.

Nice to know

Need-to-Know: Grundsatz, bei dem der Zugriffs auf personenbezogenen Daten auf die Personen beschränkt wird, die diesen Zugriff zur Wahrnehmung ihrer Aufgaben zwingend benötigen.

Least-Privilege: Prinzip der Informationssicherheit, bei dem einem Benutzer nur die für seine Tätigkeit mindestens erforderliche Zugriffs- bzw. Berechtigungsebene gewährt wird. Das Least-Privilege-Prinzip gilt als Best Practice in der Cyber-Sicherheitsbranche und ist ein wesentlicher Schritt zum Schutz privilegierter Zugriffe auf hochwertige Daten und Ressourcen.

Häufig wissen Administratoren nicht, wo wichtige Daten liegen und wer für seine Tätigkeit in der Kanzlei tatsächlich den Zugriff darauf benötigt. Auch erhält der Administrator keine Informationen über personelle Veränderungen, so dass ein Benutzerprofil eines ausgeschiedenen Mitarbeitenden nicht gelöscht wird. Unter Umständen könnte mit diesem Benutzerprofil weiterhin auf sensible Informationen zugegriffen werden. Denkbar ist zudem, dass Mitarbeiter, die in ein neues Referat versetzt werden, ihre bisherigen Berechtigungen behalten und dadurch mit der Zeit über umfangreiche Berechtigungen verfügen, die mit dem Erfordernis der eigentlichen Arbeit nicht korrespondieren.

3.2 Prüfpunkt: Zentrale Managementmöglichkeit für Benutzerzugänge

Eine fehlende zentrale Managementmöglichkeit für Benutzerzugänge kann gravierende Sicherheitslücken bedeuten.

Dieses Szenario ist häufig anzutreffen: Je nach Kanzleigröße und Anzahl der Standorte sind verschiedene Personen in unterschiedlichsten Organisationseinheiten für die Vergabe von Berechtigungen zuständig. Doch werden Berechtigungen dezentral von verschiedenen Personen administriert, führt dies unter Umständen dazu, dass Benutzer Berechtigungen sporadisch auf Zuruf oder umgekehrt nur über unnötig komplizierte Wege erhalten. Dadurch können einerseits fehlende Berechtigungen die tägliche Arbeit erschweren, andererseits können so Berechtigungen ohne Erfordernis vergeben werden und so ein Sicherheitsrisiko darstellen. So ist es nicht möglich, bei einem Cyber-Angriff oder einem Passwortdiebstahl in einem Arbeitsschritt alle Benutzerzugänge eines Mitarbeiters zu deaktivieren. Auch können in diesem Szenario bei Ausscheiden eines Mitarbeiters nicht in einem Arbeitsschritt alle Zugänge gesperrt werden.

4 Technische Umsetzung in AnNoText

4.1 Grundkonfiguration

Das Berechtigungsmanagement ist in AnNoText zentral organisiert. Zur Sicherheit müssen Sie vorher nochmal das Admin-Passwort eingeben. Klicken Sie in der Grundkonfiguration den Haken „Aktiv“ an, falls nicht geschehen und wählen „Individuell“ aus.

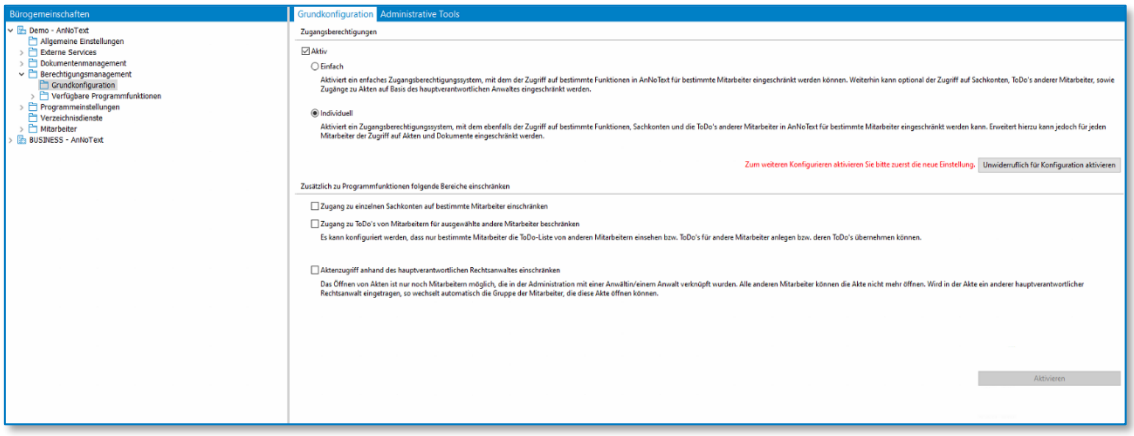

Abbildung 1: Berechtigungsmanagement – Grundkonfiguration

4.2 Mitarbeitergruppen

Das Aktivieren bewirkt zunächst, dass im Berechtigungsmanagement automatisch der Ordner **Zugangsberechtigungen über Mitarbeiter-Gruppen** für „Administratoren“ und „Jeder“ angelegt wird.

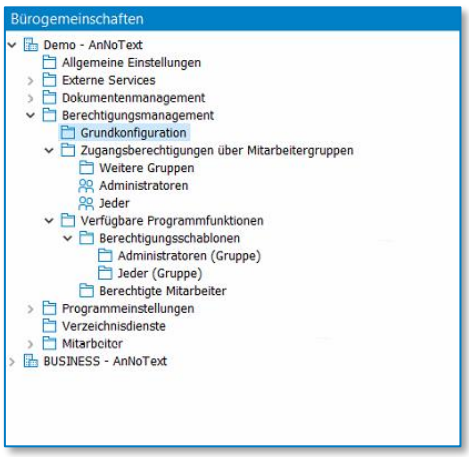

Abbildung 2: Berechtigungsmanagement – Allgemeine Einstellungen

Zur Mitarbeiter-Gruppe „**Administratoren“** können bestimmte Mitarbeiter zugeordnet werden, die administrative Tätigkeiten im Umgang mit AnNoText für die Kanzlei ausführen dürfen. Sie können selbstverständlich selbst entscheiden, welche Mitarbeiterinnen und Mitarbeiter den Administratoren zugeordnet werden soll.

Durch die Aktivierung der **Individuellen Berechtigungen** besteht generell die Möglichkeit, auch weitere, eigene Mitarbeiter-Gruppen anzulegen. In diesen Gruppen kann eine beliebige Anzahl von Mitarbeitern in einer Mitarbeiter-Gruppe zusammengeführt (z.B. einer Mitarbeiter-Gruppe „Sekretär:innen“) werden.

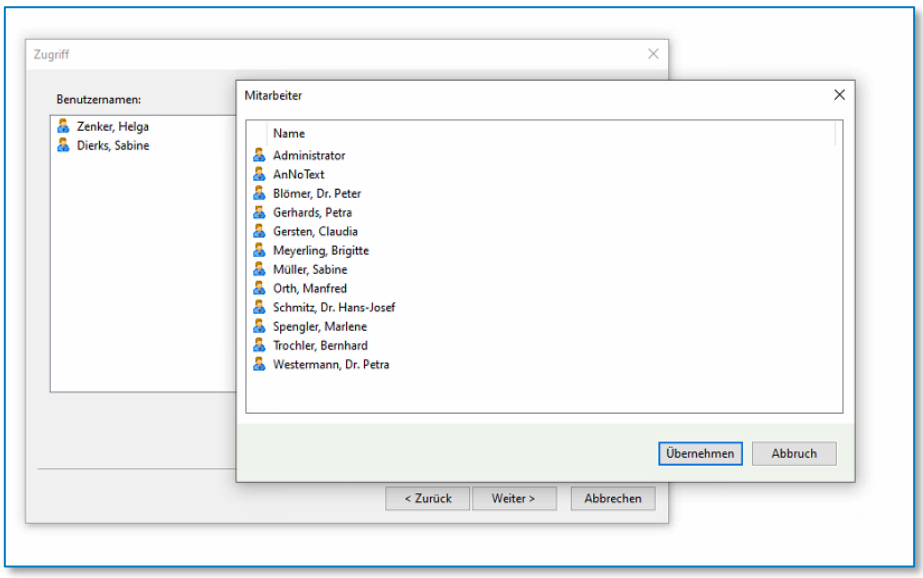

Abbildung 3: Mitarbeitergruppe anlegen

Die Mitarbeiter-Gruppe **Jeder**. Dieser Mitarbeiter-Gruppe werden alle Mitarbeiter der Kanzlei automatisch zugeordnet. Als Grundlage werden der Gruppe „**Jeder**“ alle Berechtigungen entzogen. Berechtigungen, die man in dieser Gruppe definiert gelten automatisch für alle Benutzer, denen einen bestimmtes Recht nicht explizit entzogen wurde.

Im Bereich der Gruppenbearbeitung kann im unteren Bereich definiert werden, ob der Mitarbeiter-Gruppe bestimmte Aktionen (z.B. Neuanlage von Akten, Neuanlage von Adressaten, Neuerstellung von Maßnahmen/Dokumenten) automatisch hinzugefügt werden sollen:

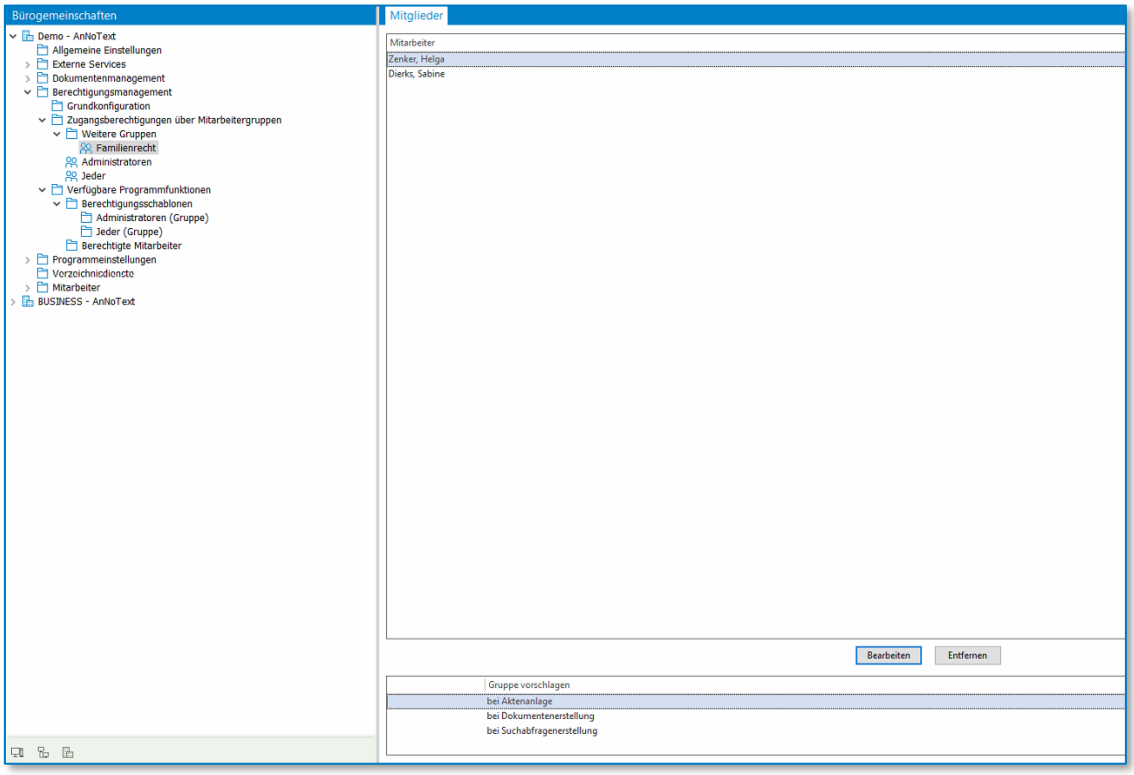

Abbildung 4: Aktionsvorschlag bei Mitarbeitergruppe anlegen

4.3 Berechtigungsschablonen

Über Berechtigungsschablonen lassen sich Zugriffsrechte zu einem Funktionsbereich strukturiert organisieren. Der Vorteil besteht darin, dass entsprechend eine Berechtigungsschablone nicht jedem Mitarbeiter einzeln zugeordnet werden muss. Für die Mitarbeiter-Gruppen kann im weiteren Verlauf eine Berechtigungsschablone, die ggf. bereits angelegt ist oder noch neu angelegt wird, zugeordnet werden.

Darüber hinaus besteht die Möglichkeit, für einen bestimmten Mitarbeitenden eine spezielle Berechtigungsschablone zu erstellen und diese Schablone nur diesem Mitarbeiter:in zuzuordnen.

Eine Berechtigungsschablone steht für alle Programmunterpunkte zur Verfügung:

- Adressmanagement
- Aktenmanagement
- Allgemein
- Dokumentenmanagement
- Elektronischer Rechtsverkehr
- Finanzbuchhaltung u. STATus
- Forderungsmanagement
- Honorarabrechnung
- Kostenberechnung
- Leistungserfassung
- Rechnungswesen
- Todomanagement-Aktivitäten
- Unfallprogramm

Für einzelne Berechtigungen können mit einem Rechtsklick ausgeführt werden: „Berechtigung hinzufügen“, „Berechtigung entziehen“ oder den „Zugriff verweigern“. Die Berechtigungsvergabe in einer individuellen Schablone hat Vorrang vor den hinterlegten Berechtigungen aus einer Gruppen-Schablone.

Hinweis:
Gemäß der Sicherheitsphilosophie von AnNoText sind standardmäßig alle Berechtigungen bei Neuanlage entzogen und müssen ergänzt werden.

Dieses Konzept folgt den in der DSGVO festgeschriebenen Grundsätzen “Privacy by Default” und “Privacy by Design”.

Beim Hinzufügen eines Benutzers oder einer Gruppe werden generell die Rechte aus der zugeordneten Schablone übertragen, beim Erstellen einer Akte verfügt der Besitzer einer Akte bzw. eines Dokuments über alle Rechte und kann dementsprechend den zugefügten Benutzern / Gruppen weitere Rechte zu ihren vorhandenen erteilen.

Eine Schablobe ist flexibel löschbar. Vorab prüft AnNoText jedoch, ob die Schablone noch einem Benutzer oder einer Gruppe zugewiesen ist und Sie erhalten einen Hinweis.

Beispiel: In der nachfolgenden Darstellung ist der Mitarbeiterin Dierks die spezielle Berechtigungsschablone **Familienrecht** zugeordnet, die Mitarbeiterin Dierks ist gleichzeitig aber auch in der Mitarbeiter-Gruppe **Jeder** (welcher die Nutzung des Programms Buchhaltung untersagt ist) zusammengeführt:

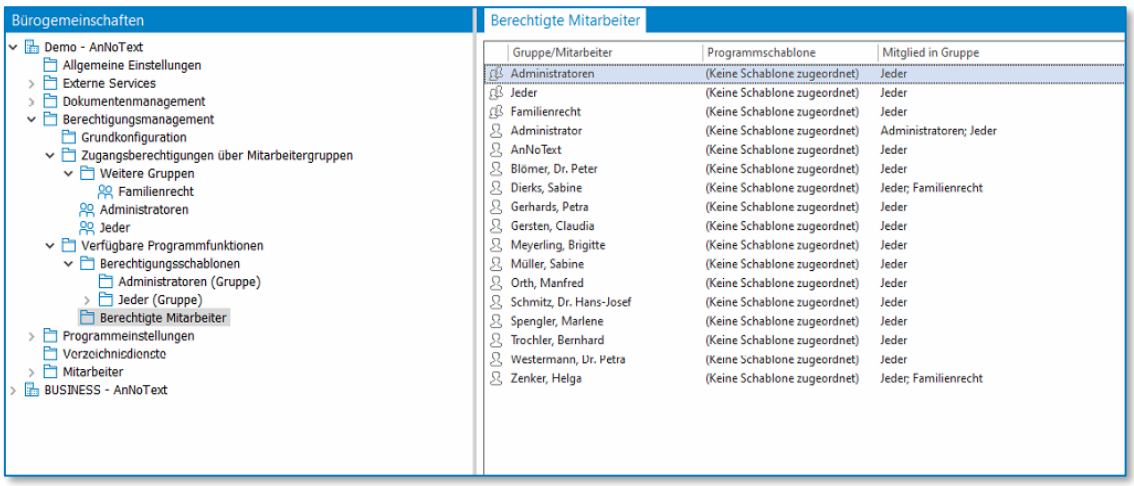

Abbildung 5: Zuordnung einer Schablone zu einem Benutzer

4.4 Standort- / Anwalts-Gruppen

Ähnlich zu den Mitarbeiter-Gruppen können Sie in AnNoText Standort- und Anwalts-Gruppen anlegen.

Dazu gehen Sie zur Grundkonfiguration und klicken den entsprechenden Haken an und bestätigen mit dem Button „Aktivieren“. Nach dem Speichern werden zu jedem Standort bzw. jedem Anwalt die Gruppe angelegt.

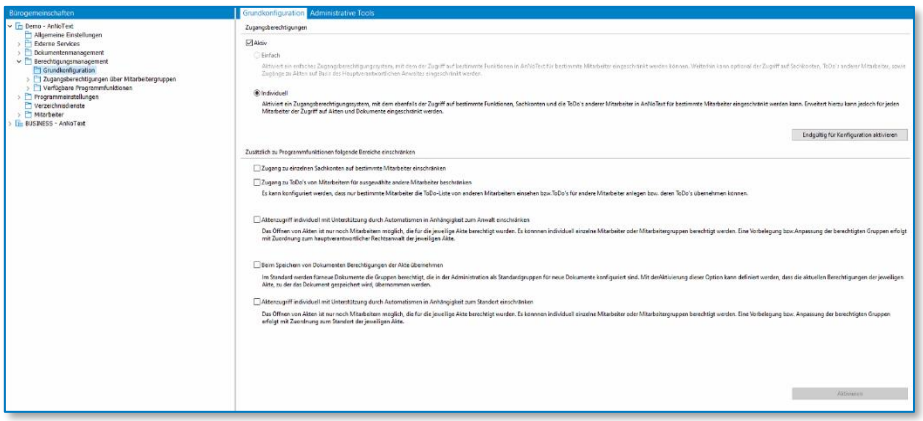

Abbildung 6: Grundkonfiguration

Danach werden in den „Zugangsberechtigungen über Mitarbeitergruppen“ im Menü „Vorauswahl über“ die jeweiligen Anwalts- / Standorts-Gruppen angelegt. Im gleichen Schritt werden auch Schablonen für Standort / Anwalt angelegt.

4.5 Anwendungsbeispiele

4.5.1 Insider-Mandat

In unserem Beispiel hat eine Kanzlei mehrere Standorte und trennt die Akten in der Regel standortbasiert. Spezielle Fälle sollen jedoch nur für einen Anwalt und seine Gruppe einsehbar sein.
Dazu müssen wir in der Administration die beiden Punkte der Anwaltsgruppe und der Standort-basierten Trennung aktivieren.

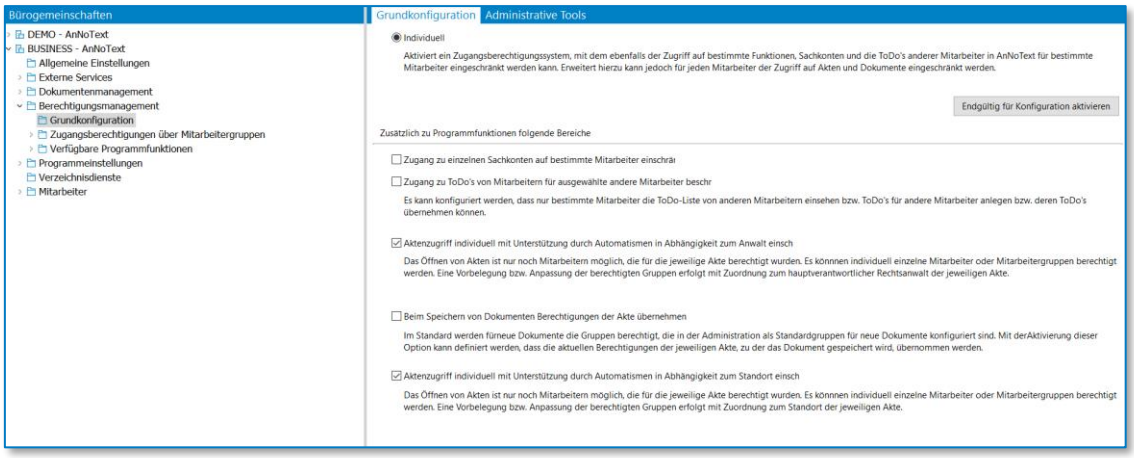

Abbildung 7: Grundkonfiguration Insider-Mandat

Danach legen wir die beiden Anwaltsgruppen fest; für den Standort Berlin fassen wir die beiden Anwaltsgruppen von den Anwälten Freitag & Burkhardt zusammen.

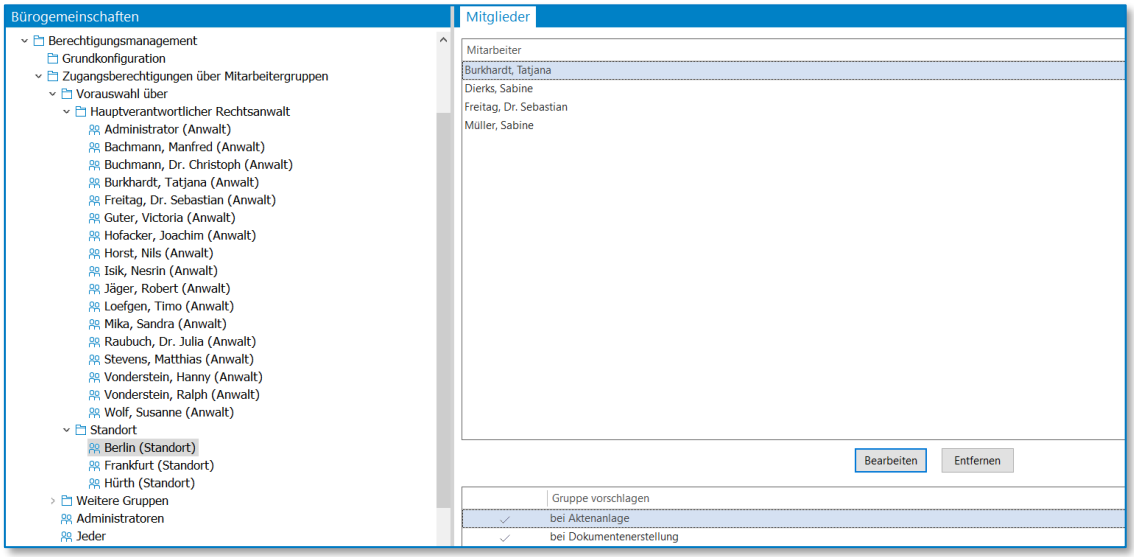

Abbildung 8: Standort-Gruppen

Anschließend legen wir die Berechtigungsschablonen für die Rechtsanwälte fest – hierbei ist zu beachten, dass Rechte wie z.B. die Aktenanlage nicht einer Gruppe zugeordnet werden können, sondern einer individuellen Person. Nach dem Anlegen der Berechtigungsschablonen erfolgt die Zuordnung; für die Sachbearbeiter ist die Anlage der Schablonen identisch.

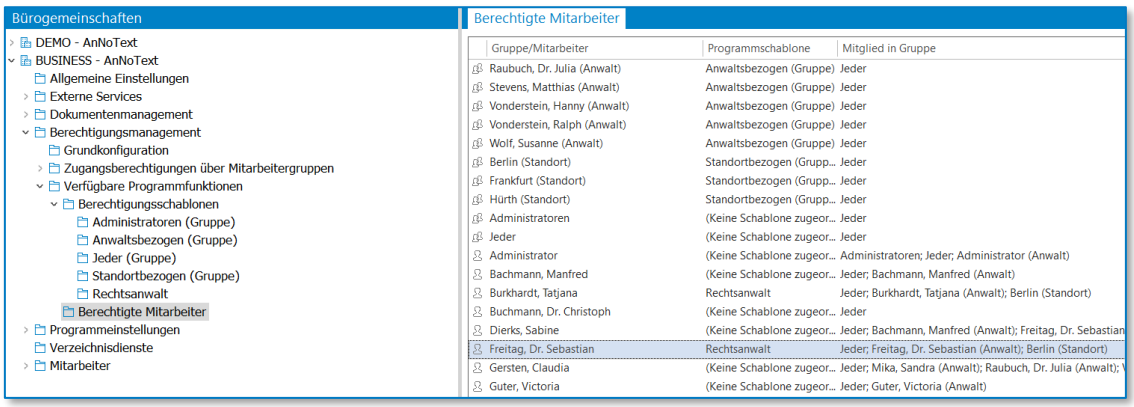

Abbildung 9: Berechtigte Mitarbeiter

Zum Schluss muss die Konfiguration des Berechtigungsmanagements noch aktiviert werden.

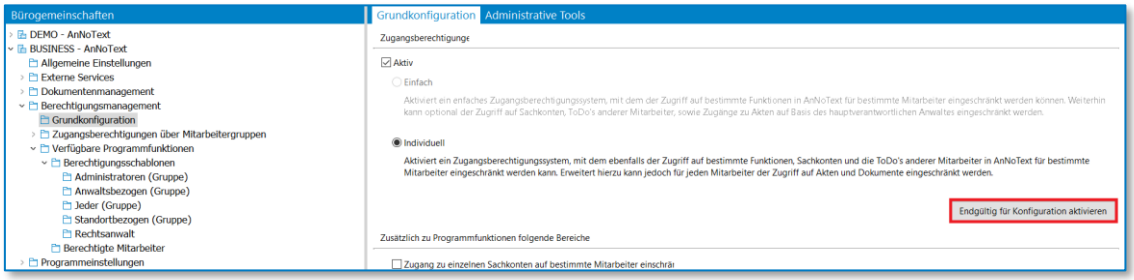

Abbildung 1: Konfiguration aktivieren

In der Auskunft legen Sie eine neue Akte an und nach den üblichen Einträgen von Mandanten, Gegner und Rubren sehen Sie einen neuen Reiter „Sicherheit“. Dort können Sie nun festlegen, wer oder welche Gruppe(n) diese Akte überhaupt sehen können.

In unserem Fall soll nur die Gruppe vom Rechtsanwalt Freitag Einblick in die Akte haben.

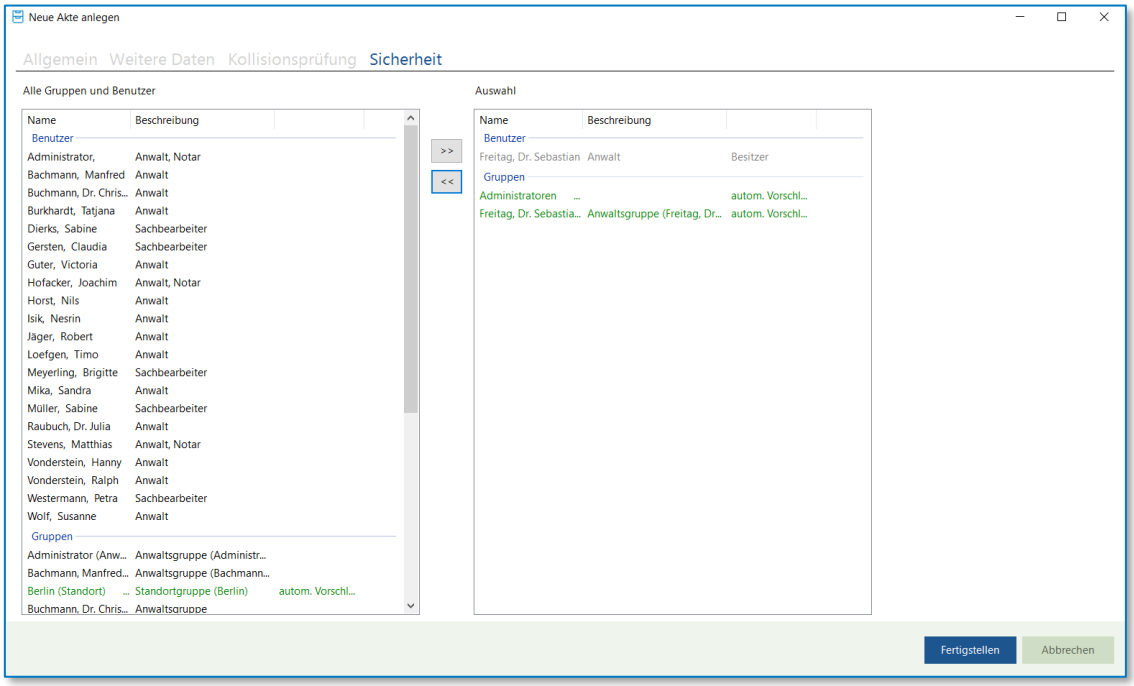

Abbildung 11: Akte anlegen

Nun soll diese Akte noch als Insider-Mandat gekennzeichnet werden. Dazu klicken Sie mit Rechtsklick auf die Akte und öffnen den Punkt „Akte als Insider-Mandat kennzeichnen“ im Kontextmenü aus.

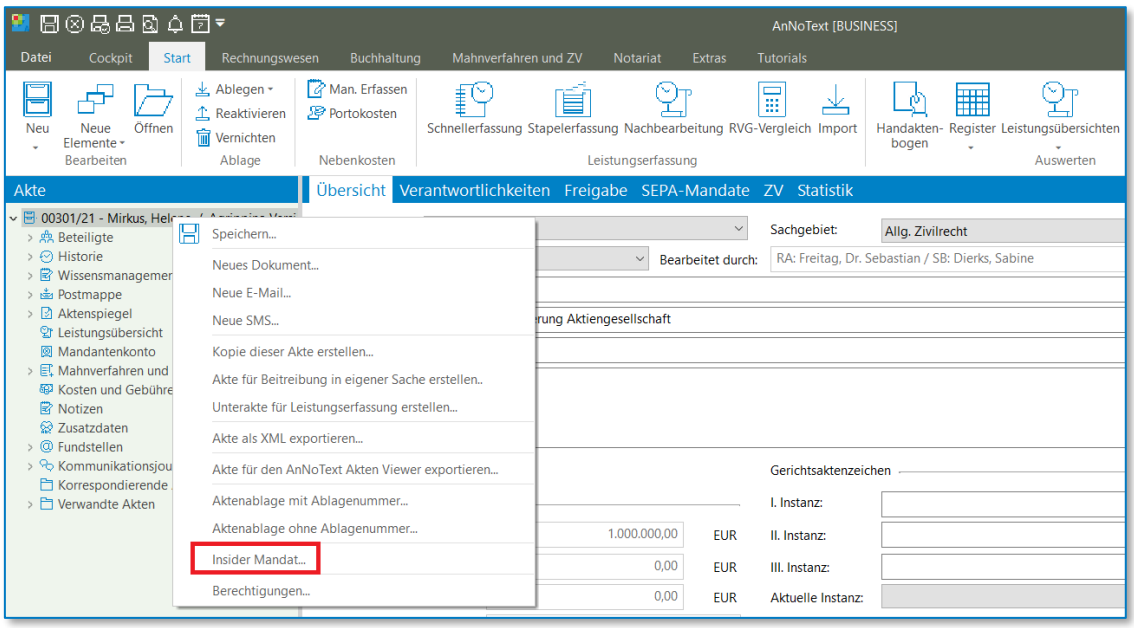

Abbildung 12: Insider Mandat

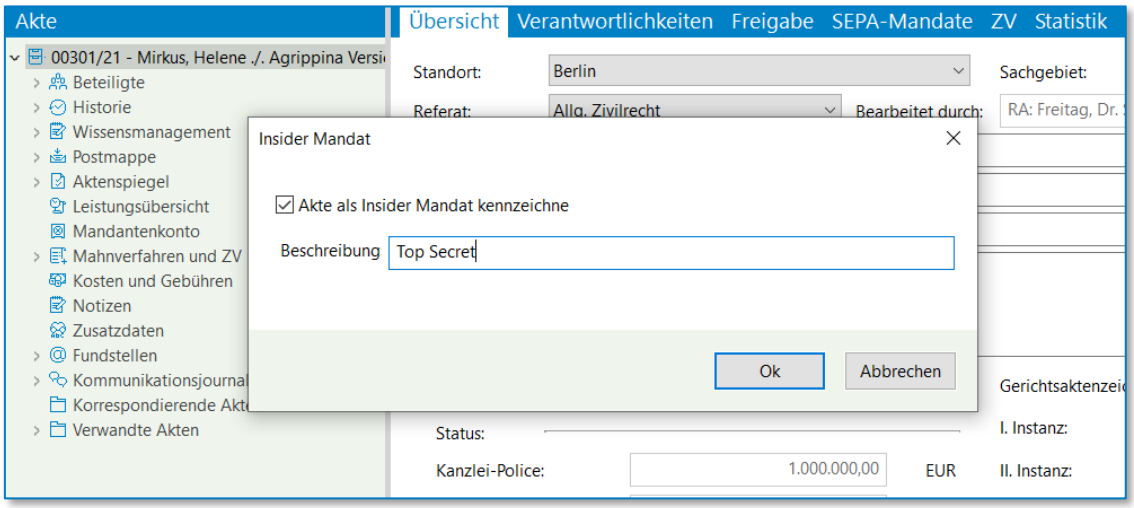

Abbildung 13: Insider Mandat II

Nachdem Sie den Haken gesetzt haben, können Sie einen Namen festlegen, mit dem die wichtigen Felder Rubrum Mandant, Rubrum Gegner und Wegen-Feld ersetzt werden sollen. Anschließend bestätigen Sie mit OK.

Bitte beachten Sie, dass auch für die berechtigten Benutzer diese Felder ausgeblendet sind, um z.B. bei einem Ausdruck keine Informationen über die Akte preiszugeben. Sie können allerdings in der Aktensuche nach Ihrem gewählten Projektnamen suchen.

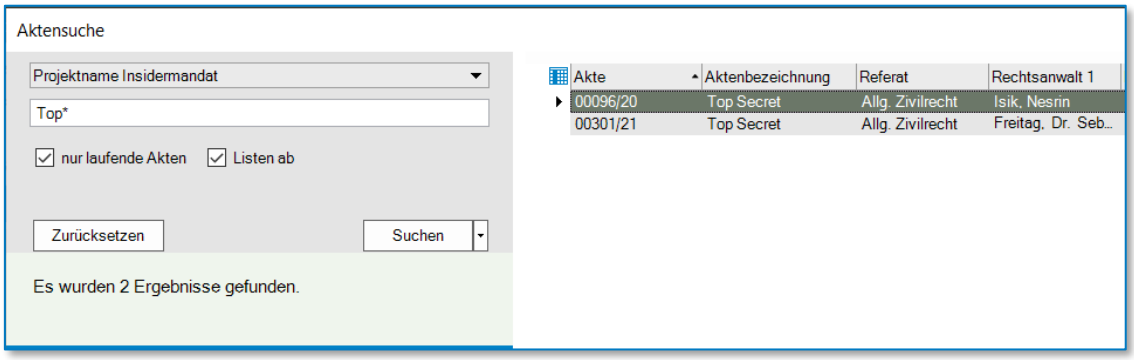

Abbildung 14: Aktensuche

Wenn Sie nun die Auskunft mit einem anderen Account öffnen und z.B. die Aktensuche öffnen, wird Ihnen die Insider-Akte mit dem gewählten Projektnamen gelistet. Bei einem Klick auf die Akte erhalten Sie als nicht-berechtigter Benutzer einen Hinweis.

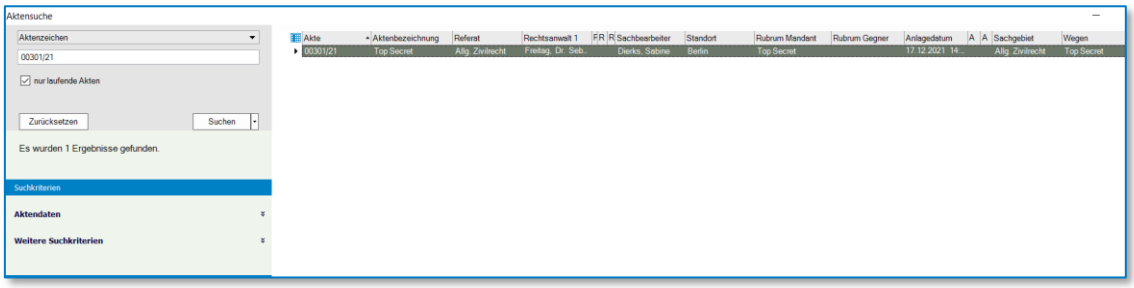

Abbildung 152: Aktensuche II

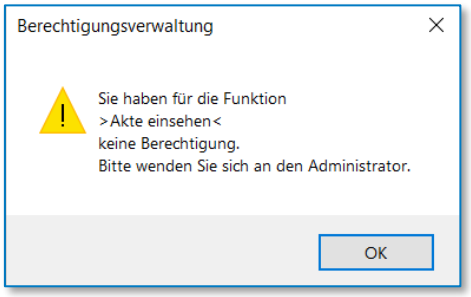

Abbildung 16: Hinweis zu fehlenden Berechtigungen

4.5.2 Urlaubsvertretung

Aufbauend auf unser erstes Beispiel soll die Rechtsanwältin Burkhardt die Urlaubsvertretung für die besagte Insider-Akte übernehmen.

Wie Sie gesehen haben, hat Sie aber kein Recht, die Akte aufzurufen. Dafür muss erst die Urlaubsvertretung aktiviert werden. Gehen Sie hierfür in die Administration und rufen den Benutzer Freitag auf; im Punkt „Mitarbeiter“ sehen Sie im unteren Bereich die Urlaubsvertretung. Hier tragen wir für den Rechtsanwalt Freitag die Rechtsanwältin Burkhardt ein. Bitte beachten Sie, dass Urlaubsvertretungen nur für die Gruppe Rechtsanwalt aktiv sind.

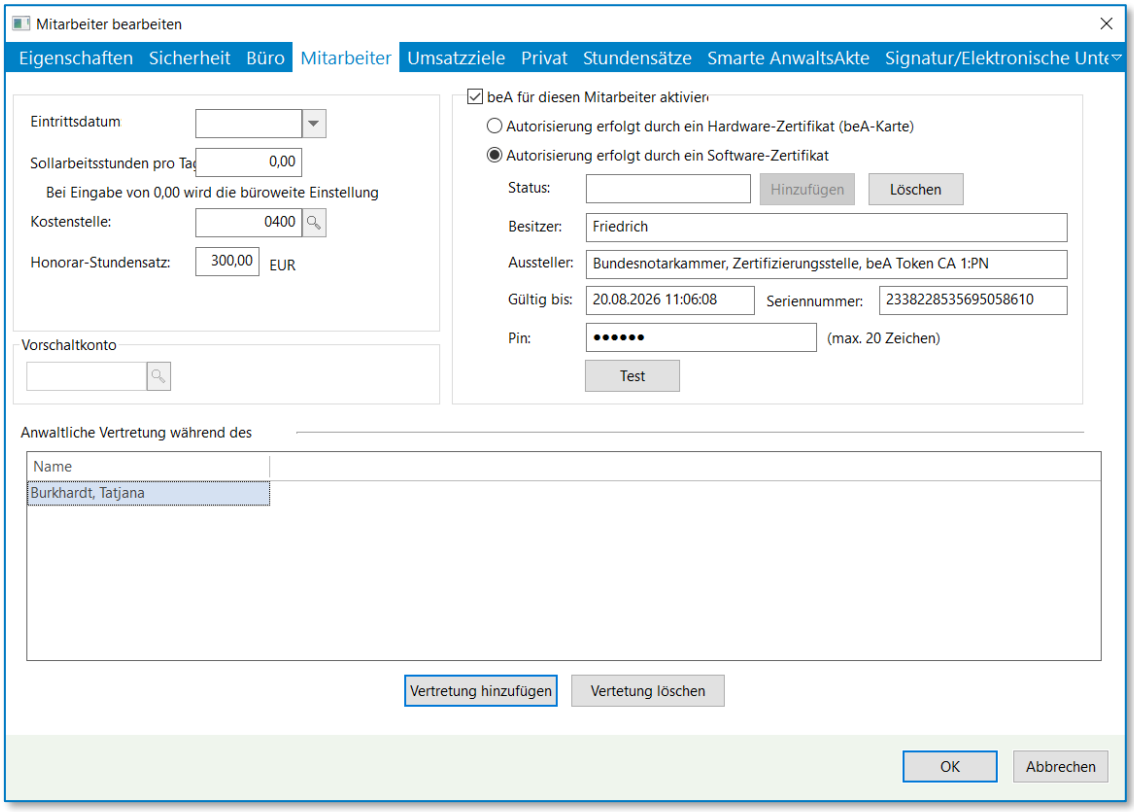

Abbildung 17: Mitarbeiter bearbeiten

Nachdem die Urlaubsvertretung gespeichert wurde, kann die Auskunft mit dem Benutzer Freitag gestartet werden. Bei Klick auf den Pfeil neben seinem Namen öffnet sich ein Kontextmenü, indem der Punkt „Stellvertretung aktivieren“ aufgelistet ist. Wenn Sie diesen Punkt anklicken, dann erscheint links neben seinem Namen „Stellvertretung aktiviert“.

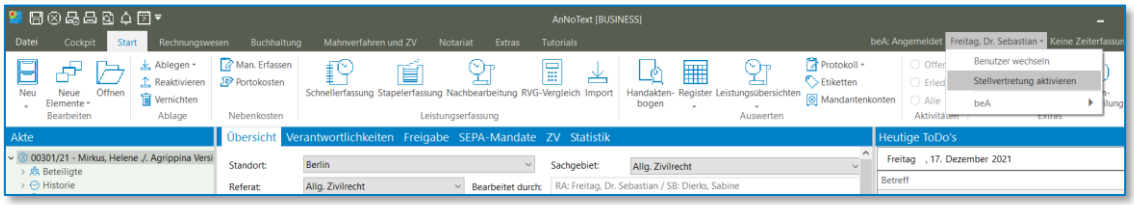

Abbildung 18: Stellvertretung aktivieren

Abbildung 19: Stellvertretung aktiviert

Wenn nun die Rechtsanwältin Burkhardt die Auskunft öffnet und die für Sie bislang gesperrte Insider-Akte aufruft, kann Sie darauf zugreifen und die Urlaubsvertretung wahrnehmen.
Nachdem der Rechtsanwalt Freitag aus seinem Urlaub zurückgekehrt ist, ruft er in der Auskunft in seinem Kontextmenü den Punkt „Stellvertretung deaktivieren“ auf und die Einblendung verschwindet wieder. Der Aktenzugriff ist nun wieder so geregelt wie vorher.

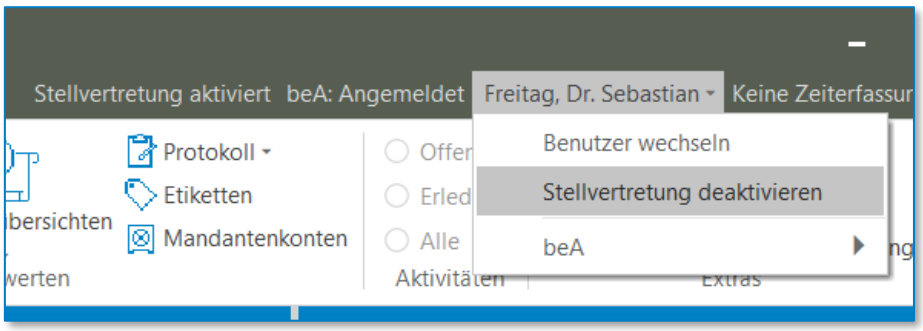

Abbildung 203: Stellvertretung deaktivieren

4.5.3 Dokumentenschutz

Ähnlich wie bei Akten können Sie auch bei Dokumenten den Zugriff einschränken. Wir legen hierfür eine Akte an, die vom Standort Berlin zugegriffen werden kann.

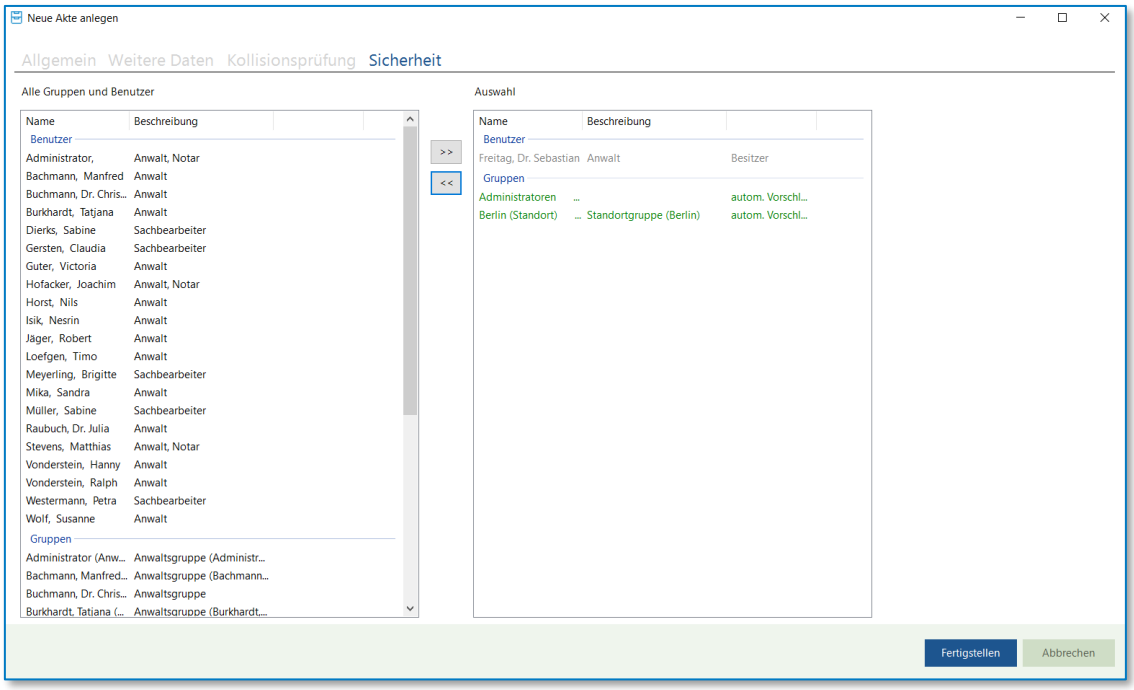

Abbildung 21: Akte anlegen

In dieser Akte fügt der Rechtsanwalt Freitag ein Dokument hinzu, welches er aber exklusiv bearbeiten möchte und welches die Gruppe der Rechtsanwältin Burkhardt nicht einsehen soll. Dafür legt er im Reiter „Sicherheit“ die berechtigten Gruppen fest.

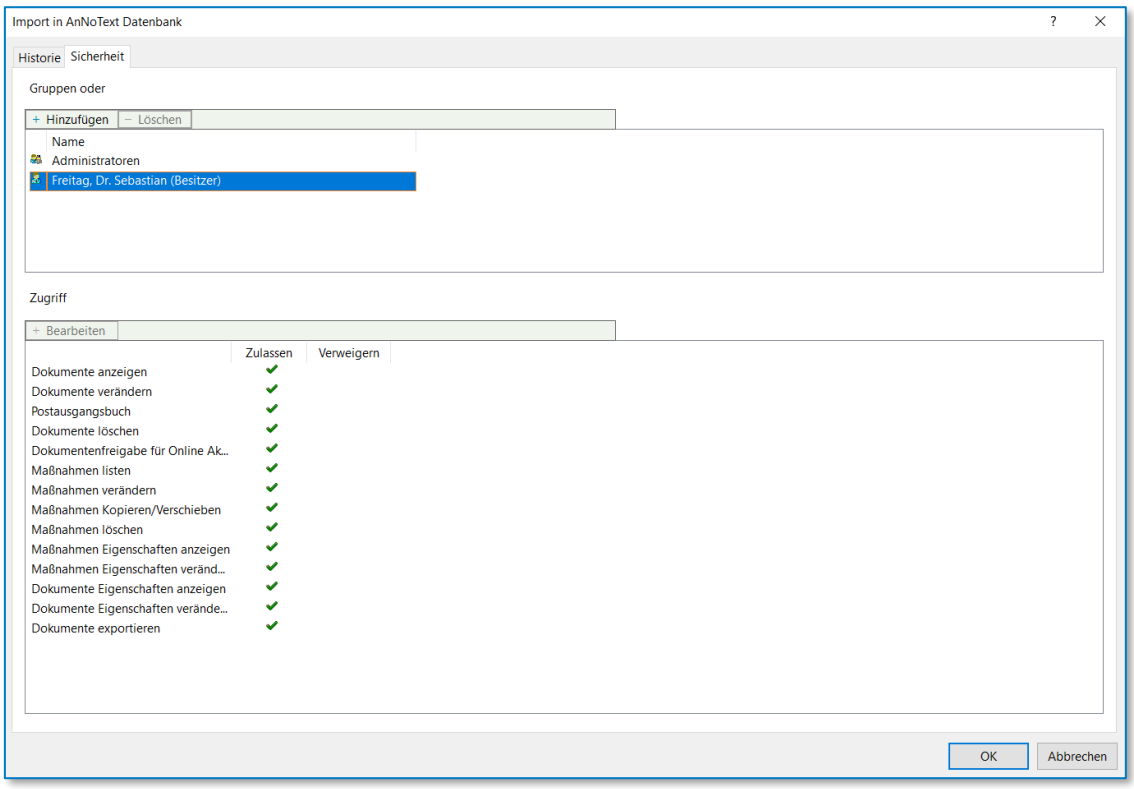

Abbildung 22: Dokument importieren

Im Anschluss rufen wir die Auskunft mit dem Benutzer Burkhardt auf und sehen beim Klick auf das Dokument, dass wir weder in der Vorschau noch anderweitig Zugriff auf das Dokument erlangen.

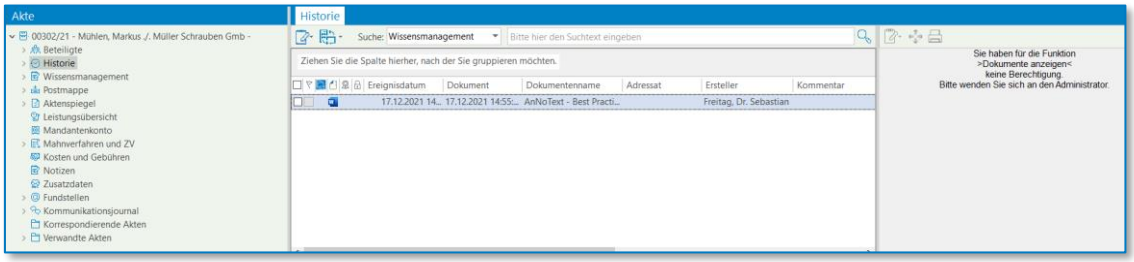

Abbildung 23: Vorschau Dokument

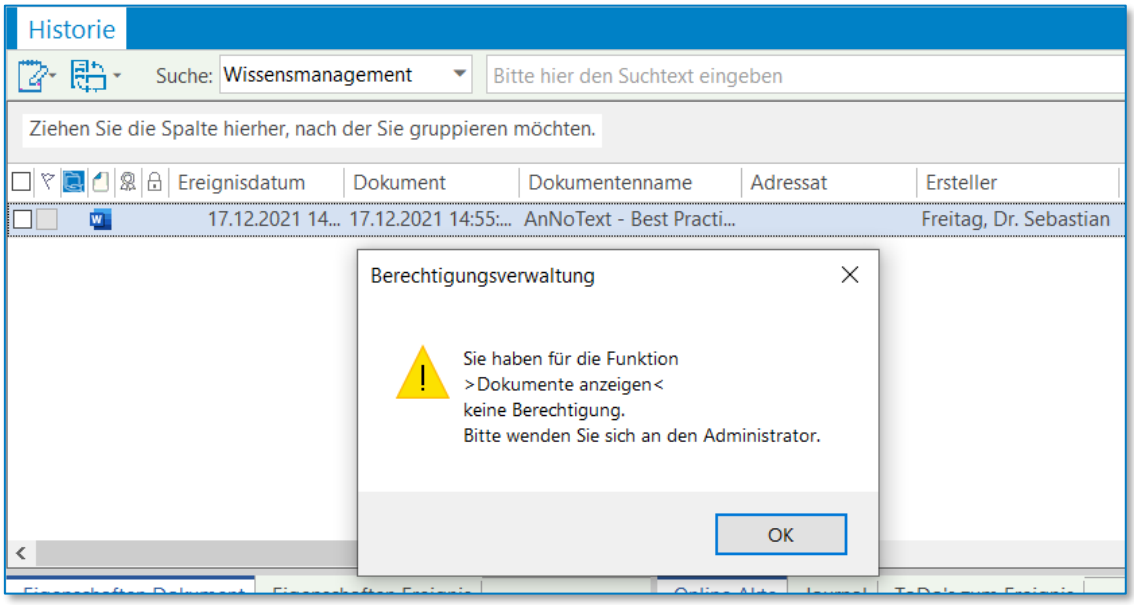

Abbildung 4: Hinweis zu fehlenden Berechtigungen

Wolters Kluwer Deutschland GmbH
Geschäftsbereich Legal Software

Wolters-Kluwer-Straße 1
D-50354 Hürth

Tel.: +49 (2233) 3760 - 6000
Fax: +49 (2233) 3760 - 16000
E-Mail: vertrieb.software-recht@wolterskluwer.com

AnNoText