



VERSIEGELTE CLOUD

Benutzerhandbuch Versiegelte Cloud

Zusätzliche Tipps und Tricks
bei der Nutzung als Datenraum

© 2018 uniscon GmbH. All rights reserved.

Haftungshinweis/Disclaimer

Der Inhalt dieses Handbuchs dient lediglich zu Informations- und Dokumentationszwecken für das Produkt Versiegelte Cloud und kann jederzeit ohne Vorankündigungen geändert werden. Für Fehler oder Ungenauigkeiten übernehmen wir keine Verantwortung oder Haftung. Aufgrund technischer Weiterentwicklungen behält sich der Hersteller jederzeit vor, den Funktionsumfang des Produkts zu ändern.

Stand: Februar 2019

Inhaltsverzeichnis Abschnitt VII

Inhaltsverzeichnis Abschnitt VII.....	2
1 Einführung	3
1.1 Begriffsdefinition Menüs.....	4
2 Anlegen eines Datenraums.....	4
3 Umwandeln einer Privacy Box in einen Datenraum.....	6
4 Das Journal	7
4.1 Einsichtnahme in ein Journal.....	8
4.2 Exportieren eines Journals	9
5 Zutrittskontrolle	9
6 Box-Mitgliederverwaltung – Nutzer zu einen Datenraum hinzufügen und entfernen	10
7 Arbeiten mit dem Datenraum	10
7.1 Anbindung über WebDAV und Produktivitätswerkzeug	10
7.2 Hochladen und Herunterladen von Dateien und Verzeichnissen über den Browser ..	11
8 Schutz gegen unautorisierte Weiterverbreitung von Inhalten	11
8.1 Schutz vor untypischen Downloads.....	11
8.2 Herunterladen unterbinden/“Nur lesen“	12
8.3 PDF Dateien mit Wasserzeichen versehen	14
9 Zeitlich begrenzter Datenraum Zugriff.....	14
9.1 Anwendungsbeispiel.....	16
10 Datenraum in ein Archiv umwandeln	16

1 Einführung

Versiegelte Cloud ist ein Cloud-Dienst, mit dem Daten vertraulich innerhalb von Organisationen und über Organisationsgrenzen hinweg ausgetauscht werden können. Sie gewährleistet, dass die Daten bereits beim Transfer verschlüsselt werden und durch die Sealed Cloud unzugänglich bleiben. Selbst Telekom, der Betreiber des Dienstes Versiegelte Cloud, kann zu keinem Zeitpunkt die Nutzerdaten einsehen oder entschlüsseln.

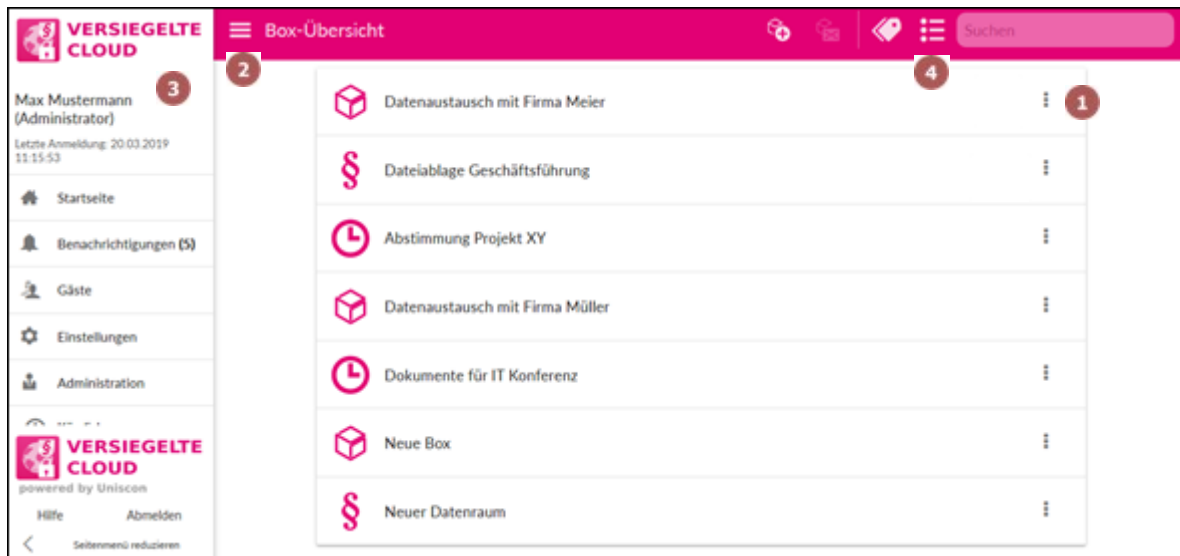
Obwohl die Daten, die in den Privacy Boxen abgelegt werden, mehrfach redundant gespeichert werden, bietet Versiegelte Cloud keine dauerhafte Garantie für die Verfügbarkeit der in den Privacy Boxen und Datenräumen gespeicherten Daten. Daher wird Versiegelte Cloud nicht als alleiniges Medium für die Verwahrung von Sicherungskopien empfohlen.

Versiegelte Cloud Privacy Boxen erfüllen die generellen Sicherheitsanforderungen. Bei bestimmten Anwendungen wie Vertragsverhandlungen und bei besonders sensiblen Projekten sollen Dokumente jedoch oft zusätzlich geschützt werden. Bei Versiegelte Cloud ist ein Datenraum deshalb eine Privacy Box mit zusätzlichen Funktionen zum Schutz von Dokumenten gegen unerwünschte Weiterverbreitung und Protokollierung aller Aktivitäten. In diesem Handbuch werden nur die zusätzlichen Funktionen des Datenraums beschrieben. Möchten Sie die Grundlagen im Umgang mit Privacy Boxen kennenlernen, nutzen Sie bitte das Handbuch „Abschnitt II Beschreibung der Funktionen des Dienstes. Anleitung zur Nutzung mit dem Browser.“



Hinweis: nicht alle in diesem Handbuch beschriebenen Features sind für alle Pakete der Versiegelten Cloud verfügbar. Bei zusätzlichem Bedarf wenden Sie sich bitte an Ihren persönlichen Kundenberater.

1.1 Begriffsdefinition Menüs



1. „3-Punkte“-Menü: Das „3-Punkte“-Menü ermöglicht den Zugriff auf verschiedene Anwendungen einer Box (z.B. Einstellungen, Löschen, Teilen).
2. „Burger“-Menü: Mithilfe des „Burger“-Menüs lässt sich das Seitenmenü (Punkt 3) ein- und ausklappen.
3. „Seiten“-Menü: Das Seitenmenü gibt eine Übersicht über verschiedene Reiter (z.B. Startseite, Benachrichtigungen, Gäste, Einstellungen, usw.)
4. „Sortier“-Menü: Das „Sortier“-Menü eröffnet die Möglichkeit die Boxen nach Ansicht, Sortierrichtung und entweder nach Namen oder nach Benachrichtigungen zu sortieren.

2 Anlegen eines Datenraums

Datenräume können nur von einem Volllizenz-Nutzer angelegt werden, der auch über das entsprechende Recht verfügt. Des Weiteren muss die entsprechende Lizenz für den Datenraum vom Administrator Ihres Accounts gebucht sein.

In der Box-Übersicht wählen Sie die Funktion „neue Box erstellen“.



Wählen Sie den Datenraum aus.

Bitte wählen Sie den geeigneten Box-Typ

Temporäre Privacy Box

Privacy Box

Datenraum

Eigenschaften

- Revisions sicheres Journal
- Dynamische Wasserzeichen für Dokumente
- Konfigurierbare Zugriffs- und Darstellungsoptionen

Ideal für

- Due-Diligence-Prüfungen
- Jahresabschlussprüfungen
- Projekte mit hohem Nachweisbedarf

DATENRAUM ERSTELLEN

Tragen Sie den Namen entsprechend den Regeln für zulässige Zeichen ein und speichern Ihre Eingaben ab

Neue Box erstellen

ALLGEMEIN* EIGENSCHAFTEN DER BOX VOREINGESTELLTE BERECHTIG... DATENRAUM

Name
Neuer Datenraum

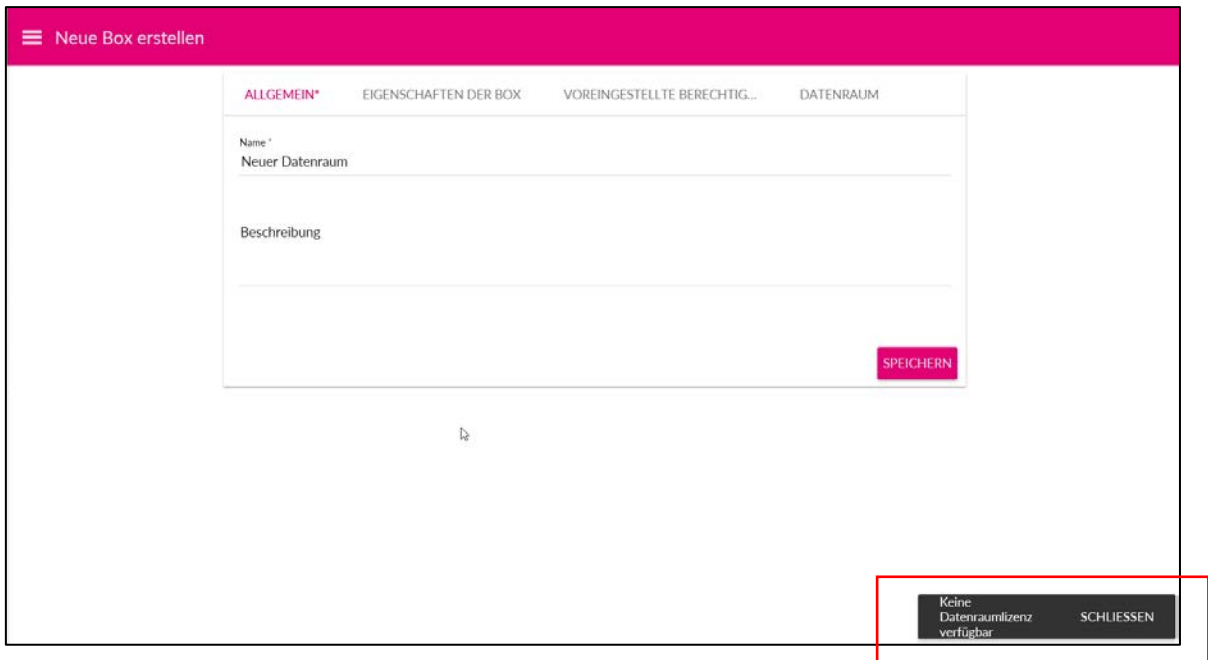
Beschreibung

SPEICHERN

Bezüglich der Bezeichnung des Datenraums gelten dieselben Regeln wie für Privacy Boxen. Sie finden nähere Angaben im Handbuch „Abschnitt II Beschreibung der Funktionen des Dienstes. Anleitung zur Nutzung mit dem Browser.“

Sollten Sie keinen Datenraum erstellen können, weil die Auswahl grau hinterlegt ist, fehlt Ihnen das entsprechende Recht. Der Administrator Ihres Accounts kann Ihnen die Berechtigung einen Datenraum zu erstellen zuweisen.

Ist die Berechtigung vorhanden, fehlt jedoch die Lizenz um einen Datenraum zu erstellen, können Sie zwar die Funktion „Datenraum erstellen“ aufrufen, den Datenraum jedoch nicht anlegen. Wenden Sie sich an Ihren Administrator und bitten Sie ihn eine entsprechende Lizenz zu buchen.



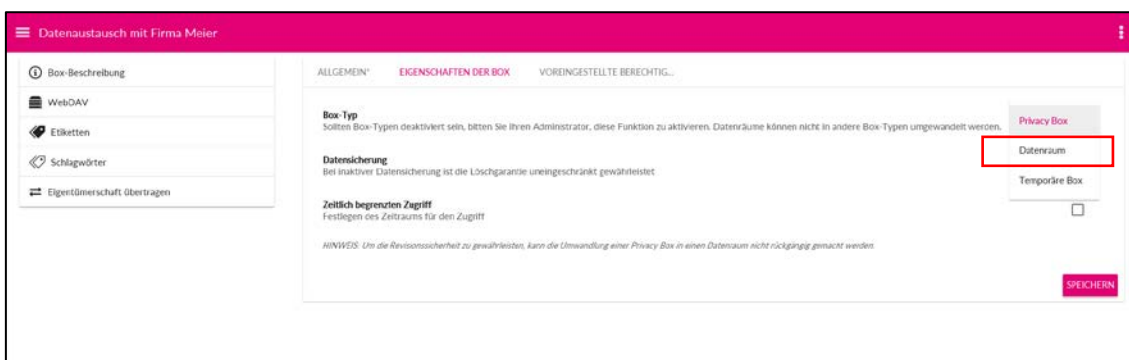
3 Umwandeln einer Privacy Box in einen Datenraum

Nur mit einer vorhandenen Lizenz und dem Recht für einen Datenraum kann eine Privacy Box in einen Datenraum umgewandelt werden.

In der Listenansicht: Öffnen Sie die entsprechende Privacy Box und aktivieren Sie im Box Menü mit den „3-Punkten“ den Befehl „Box-Einstellungen“. Über diesen Befehl öffnen Sie die Box Beschreibungen.

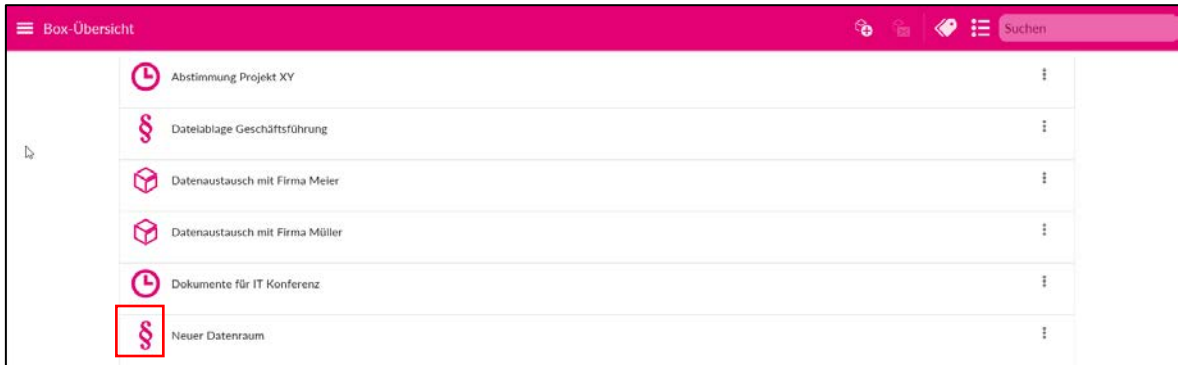


In den Box-Beschreibungen wechseln Sie in das Fenster mit den Eigenschaften der Box.

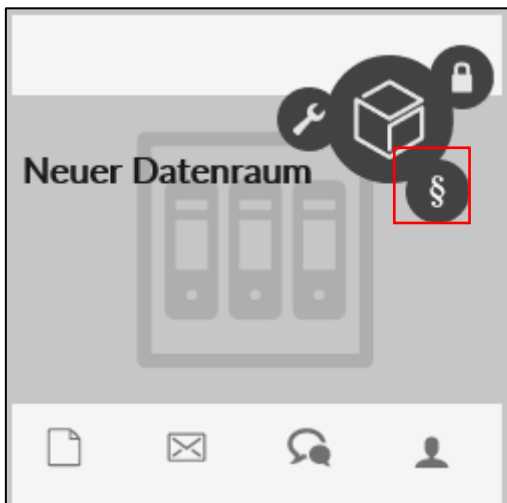


Ändern Sie den Box-Typ von Privacy Box auf Datenraum und speichern Sie die Eingaben ab.

In der Box-Übersicht wird sich die Privacy Box „Transaktion Übernahmeziel Muster AG“ als Datenraum darstellen. Sie erkennen einen Datenraum an dem „Paragrafen“ Symbol.



Das „Paragrafenzeichen“ weist auf die besonderen Funktionen eines Datenraums hin. In der Rasteransicht zeigt sich Datenraum auf diese Weise:



➡ Hinweis: Die Umwandlung einer Privacy Box in einen Datenraum ist nicht umkehrbar. Ein einmal erstellter Datenraum bleibt aus Gründen der Revisionsicherheit immer ein Datenraum, bis er komplett gelöscht wird.

4 Das Journal

Das Journal ist für jeden Ersteller und dem Verwalter eines Datenraums einsehbar. Andere Mitglieder des Datenraums können das Journal nur sehen, wenn ihnen in der Mitgliederverwaltung das entsprechende Recht gewährt wurde.

Jeder Datenraum verfügt automatisch über ein eigenes Journal. Im Journal wird jede Aktion im Datenraum unveränderbar und damit revisionsicher aufgezeichnet,

um im Bedarfsfall Zugriffe und Änderungen an Datenrauminhalten nachvollziehen zu können.

Das erstreckt sich über das Hochladen und Herunterladen eines jeden Dokuments, Lesezugriffe, Löschen von Dokumenten, Schreiben von Nachrichten und Zustimmung sowie Ablehnung zu den Nutzungsregeln. Über das „3-Punkte“ Menü gelangen Sie zum Journal.



Beispiel für Journaleinträge:



4.1 Einsichtnahme in ein Journal

Der Datenraum Ersteller und Verwalter können in der Mitgliederverwaltung einem Volllizenz-Mitglied das Recht auf Einsichtnahme des Journals geben. Nutzer mit einer Gastlizenz können das Journal nicht öffnen.

Der Umgang und Arbeiten mit der Mitgliederverwaltung finden Sie im Handbuch „Abschnitt II Beschreibung der Funktionen des Dienstes. Anleitung zur Nutzung mit dem Browser beschrieben.“

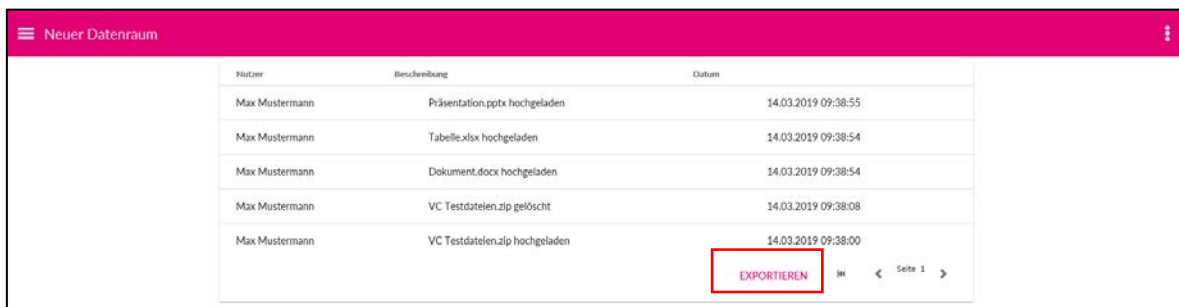


Nur wenn das Recht „Journal“ in der Zeile eines Datenraum Mitglieds gesetzt ist, kann derjenige das Journal öffnen. Jedoch ist einem Gastlizenz-Nutzer nicht möglich, das Recht auf Einsicht eines Journals zu bekommen.

4.2 Exportieren eines Journals

Nur der Datenraum Ersteller und die Verwalter des Datenraums können das Journal exportieren.

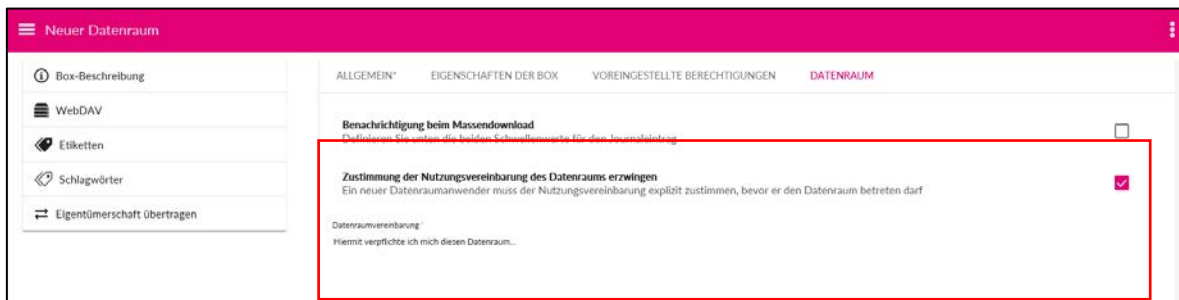
Sie können am Ende eines Projekts das Journal exportieren, sofern Sie dieses zu Dokumentationszwecken auf ein anderes Medium (z.B. DVD) archivieren möchten.



Das exportierte Journal wird als .csv-Datei in Ihren Download-Verzeichnis gespeichert. Es kann dann anschließend konvertiert und in anderen Programmen weiterverarbeitet werden.

5 Zutrittskontrolle

Bevor dem Datenraum Mitglieder hinzugefügt wurden, kann der Ersteller und der Verwalter eines Datenraums für die zukünftigen Mitglieder individuelle Zugriffs- und Verhaltensregeln festlegen (click-through agreement CTA). Der entsprechende Text wird im Menü „Box Beschreibungen“ im Fenster „Datenraum“ eingegeben.



Jedes Mitglied des Datenraums muss diesen Regeln vor dem ersten Zutritt zustimmen, bevor der Zugriff auf Daten erhält. Die Zustimmung/Ablehnungen zu den Regeln werden im Journal protokolliert.

Meldet sich ein Mitglied des Datenraums an, bekommt er folgende Meldung:

Datenraumvereinbarung

Hiermit verpflichte ich mich diesen Datenraum...

NICHT ZUSTIMMEN ZUSTIMMEN

Nur, wenn das Datenraum Mitglied der Vereinbarung zustimmt, wird ihm Zugriff auf die Daten und Dokumente im Datenraum gewährt.

Journaleinträge:

Neuer Datenraum	
Nutzer	Beschreibung
Mitglied 1	Der Vereinbarungstext wurde akzeptiert
Max Mustermann	Der Vereinbarungstext wurde aktualisiert



Hinweis: Werden die Regeln eines Datenraums während der Lebenszeit verändert, ist von allen zugriffsberechtigten Nutzern eine neue Zustimmung erforderlich

6 **Box-Mitgliederverwaltung – Nutzer zu einem Datenraum hinzufügen und entfernen**

Der Datenraum verfügt über dieselbe Mitgliederverwaltung wie eine Privacy Box.

Für Fragen bezüglich des Einladens eines Nutzers oder dem zuweisen von Berechtigungen nutzen Sie das Handbuch „Abschnitt II Beschreibung der Funktionen des Dienstes. Anleitung zur Nutzung mit dem Browser.“

7 **Arbeiten mit dem Datenraum**

7.1 **Anbindung über WebDAV und Produktivitätswerkzeug**

Datenräume sind nicht per WebDAV sichtbar, da dieses Protokoll die Schutzfunktion eines Datenraums nicht versteht und deshalb dafür gesperrt ist.

Im Gegensatz hierzu kennt das Produktivitätswerkzeug die Eigenschaften von Datenräumen und kann kontinuierlich zur Arbeit mit Datenräumen verwendet werden. Das Hochladen und Herunterladen von Dateien und von Verzeichnisstrukturen erfolgt einfach per „drag & drop“ der Verzeichnisse in den entsprechenden Bereich des Produktivitätswerkzeugs. Diese Arbeit kann jederzeit vorgenommen werden.

Die einzige Einschränkung bezüglich des Produktivitätswerkzeugs besteht darin, dass ein Datenraum nicht synchronisiert werden darf. Diese Funktion ist gesperrt, da sie die Weiterverbreitungsschutzfunktionen verletzen würde.

7.2 Hochladen und Herunterladen von Dateien und Verzeichnissen über den Browser

Sie können in einen Datenraum ebenso wie in eine Privacy Box Daten hochladen. Nutzen Sie dafür die entsprechenden „Pfeil“-Symbole in der Dateiansicht eines Datenraums. Um ein gesamtes Verzeichnis hochzuladen, nutzen Sie den Experten-Upload. Genauere Angaben dazu lesen Sie bitte in dem Handbuch „Abschnitt II Beschreibung der Funktionen des Dienstes. Anleitung zur Nutzung mit dem Browser“ nach.

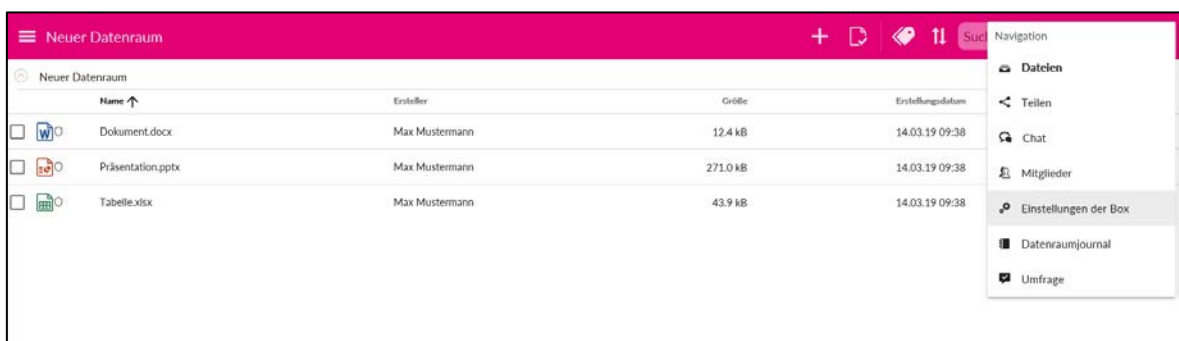
8 Schutz gegen unautorisierte Weiterverbreitung von Inhalten

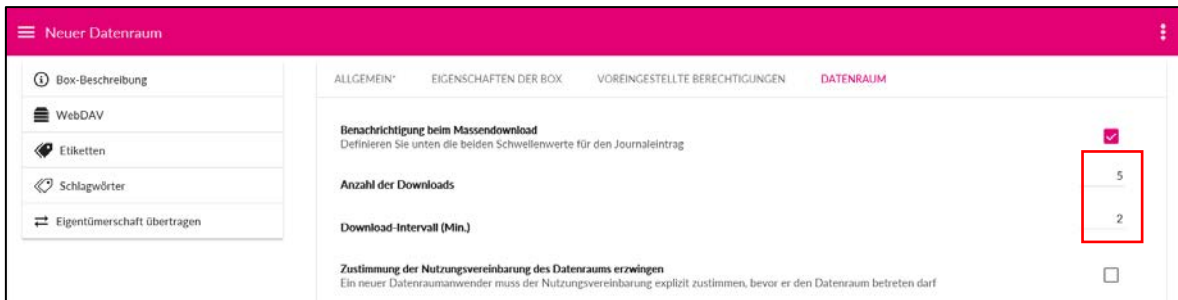
8.1 Schutz vor untypischen Downloads

Diese Einstellungen können nur vom Datenraum-Ersteller und -Verwalter vorgenommen werden.

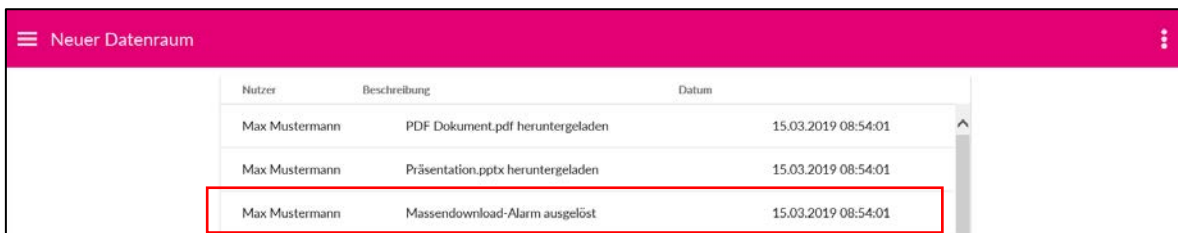
Um den Inhalt des Datenraums vor einen Massendownload von Dateien zu schützen, können Sie Maßzahlen (Anzahl, Intervall) für das Herunterladen von Dateien festlegen. Wird diese Regel verletzt, sehen Sie diese Aktion im Journal als Alarmmeldung dargestellt.

Sie finden diese Einstellungen im „3-Punkte“ Menü auf der magentafarbenen Leiste innerhalb des Datenraums.





Im obigen Beispiel ist es den Mitgliedern des Datenraums erlaubt, bis zu 5 Dateien innerhalb von 2 Minuten herunterzuladen.



Im Journal wird jedes Datenraum Mitglied unter seinem im System bekannten Namen geführt. Hat ein registrierter Nutzer die Regel des erlaubten Downloads verletzt, haben Sie die Möglichkeit mit diesem Nutzer über seine Daten im Nutzer-Profil in Kontakt zu treten.

Wird ein Dokument mit einer Funktion versehen, welches das Herunterladen unterbindet, also eine PDF Datei die mit der „Nur Lesen“ Funktion versehen, so wird auch jeder Aufruf des Dokuments als Download verzeichnet.

8.2 Herunterladen unterbinden/„Nur lesen“

Nur der Datenraum-Ersteller und der Datenraum-Verwalter können einer PDF Datei die Funktion „Nur Lesen“ zuweisen und wieder entnehmen.

Einer PDF-Datei, der die Funktion „Nur Lesen“ zugewiesen wurde, enthält ein Wasserzeichen und den Zeitstempel auf jeder einzelnen Seite. Mit der Funktion ist die PDF-Datei geschützt gegen

- Herunterladen
- Drucken
- Kopieren in die Zwischenablage des Computers

Öffnen Sie den Datenraum und markieren Sie die PDF-Datei in deren Checkbox.



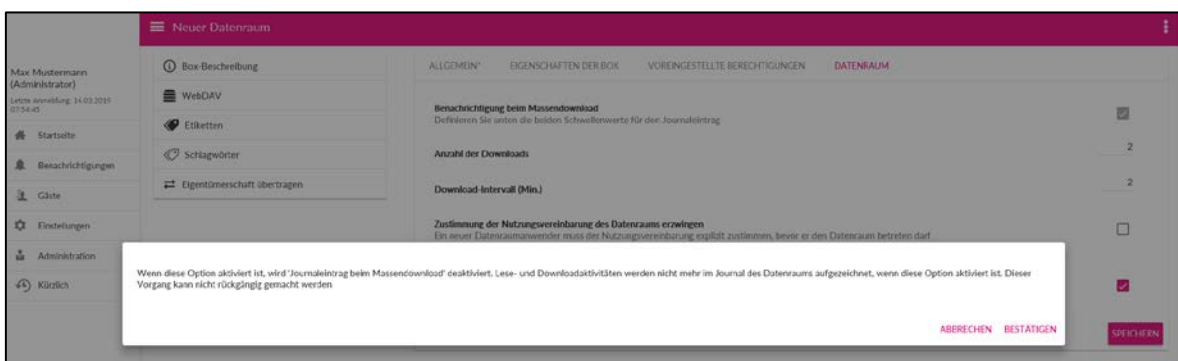
Es öffnet sich ein zusätzliches Menü in der grünen Leiste.



Wählen Sie in den Datenraumeinstellungen den Befehl „Nur-lesen“ aus.

Der Aufruf jeder Seite eines Dokuments wird als Download im Journal verzeichnet und wird bei Anwendung der Regel zur Begrenzung des Downloads herangezogen. Es kann dazu kommen, dass ein vielfaches Blättern durch ein Dokument zu einer Alarmmeldung im Journal führt.

Sie können dieses jedoch verhindern, indem Sie das Blättern durch ein „Nur Lesen“-Dokument aus der Regel zur Aufzeichnung eines Massendownloads herausnehmen.

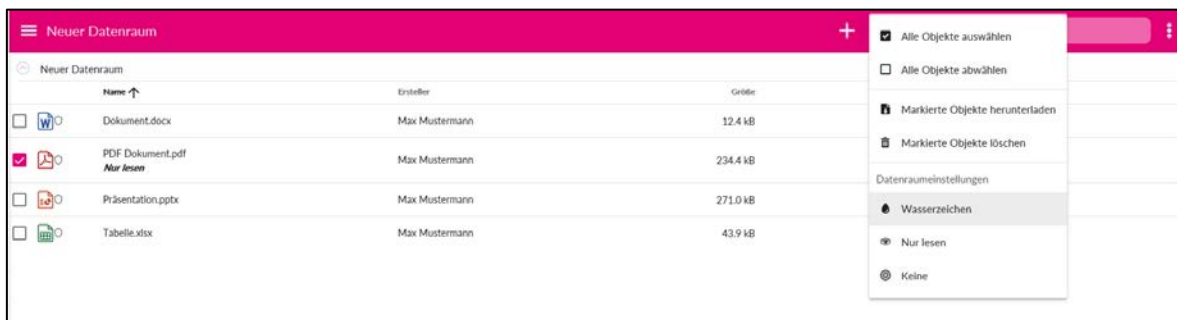


➡ Hinweis: Diese Einstellung ist ein einmaliger Vorgang innerhalb eines Datenraums und kann nicht mehr rückgängig gemacht werden.

8.3 PDF Dateien mit Wasserzeichen versehen

Nur der Datenraum-Ersteller und der Datenraum-Verwalter können einer PDF-Datei die Funktion „Wasserzeichen“ zuweisen und wieder entnehmen.

Das dynamisch generierte Wasserzeichen von Versiegelte Cloud kann nur einer PDF-Datei hinzugefügt werden. Das Wasserzeichen enthält den Namen des Nutzers und den Zeitstempel, an welchen diese Datei von einem Nutzer geöffnet und heruntergeladen wurde. Diese Kennzeichnung bietet einen Schutz gegen unberechtigte Weitergabe von Unterlagen. Wird diese Funktion einer PDF-Datei zugewiesen, so wird sie automatisch in jede Seite der Datei eingebettet.



Markieren Sie eine PDF Datei im Datenraum und öffnen Sie das Blatt in der magentafarbenen Leiste. Wählen Sie den Befehl „Wasserzeichen“ aus. Damit haben Sie dem PDF Dokument das Wasserzeichen zugewiesen.

9 Zeitlich begrenzter Datenraum Zugriff

Der Ersteller eines Datenraums kann für andere Mitglieder den Zugriff auf eine Box zeitlich begrenzen. Der Datenraum-Verwalter kann einmal gespeicherte Zugriffszeiten nicht ändern, aber auch außerhalb der Zugriffszeiten die Box öffnen.

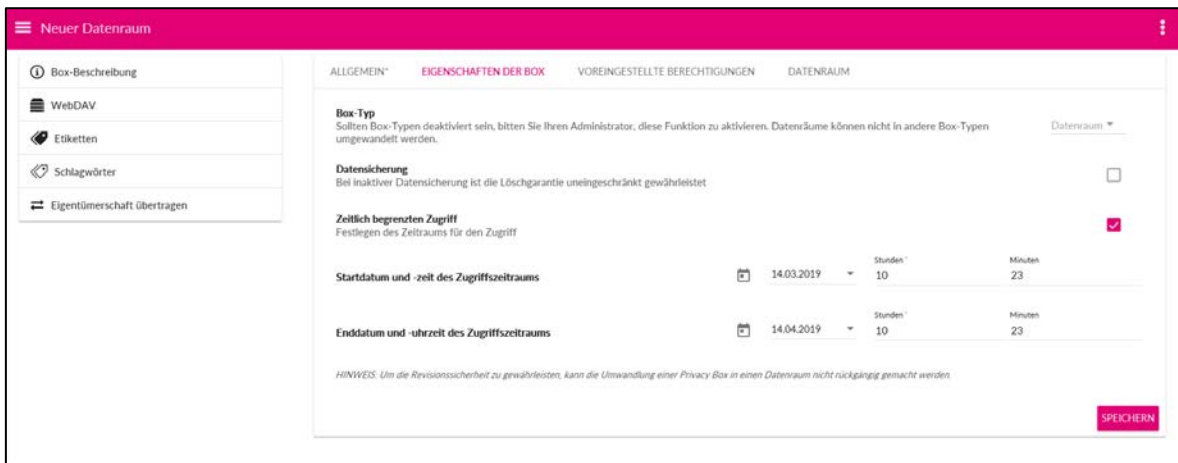
Oft benötigt ein Datenraum eine gewisse Vorbereitungszeit:

z.B. für den Upload der Verzeichnisstrukturen und Dokumente, Einstellung der Schutzfunktionen, Einladung der Mitglieder.

Unabhängig vom Vorbereitungsstand ist es komfortabel, Mitglieder einzuladen, bevor alle Arbeiten abgeschlossen sind. Damit die Mitglieder aber nicht auf den unfertigen Raum zugreifen, kann beispielsweise ein Freigabezeitpunkt („Eröffnungstag“) für den Datenraum festgelegt werden. Dies erfolgt in „Einstellungen der Box“.

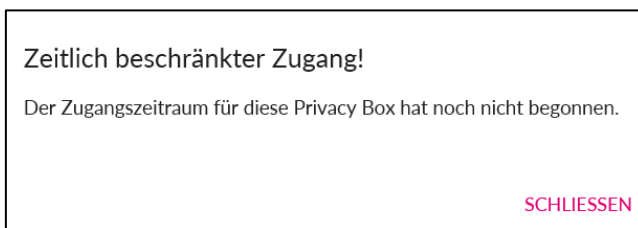


Öffnen Sie über das Menü „Informationen“ die Boboxbeschreibungen. Öffnen Sie das Fenster Eigenschaften der Box. Dort können Sie die Zugriffszeiten für die Mitglieder Ihres Datenraums festlegen.

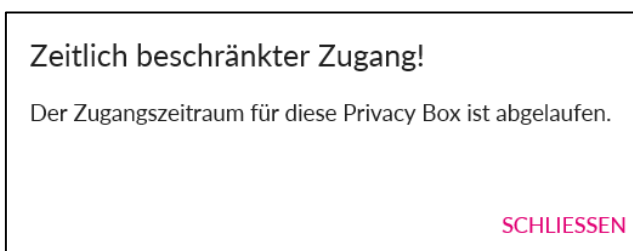


Fügen Sie die gewünschten Mitglieder Ihren Datenraum hinzu und stellen Sie den Zeitraum ein, in welchem diese Mitglieder auf den Datenraum zugreifen dürfen.

Möchte ein Mitglied **vor** der von Ihnen eingestellten Zeit auf die Box zugreifen, erscheint für dieses Mitglied folgende Meldung:



Ist die Zeit bereits **überschritten**, zu der Mitglieder auf die Box zugreifen durften, sieht die Meldung folgendermaßen aus:



9.1 Anwendungsbeispiel

Datenraum als Austausch- und Dokumentenplattform für ein Gremium:

In einem Beispiel möchte ein Gremium vertrauliche Dateien austauschen, jedoch von einem Sekretär die Sitzungstermine des Gremiums verwalten lassen. Die Anforderung an das Rechtemanagement ist also, dass die Mitglieder des Gremiums als Gruppe alle Dokumente sehen und lesen, sowie eigene Beiträge schreiben bzw. hochladen dürfen. Der Sekretär darf jedoch nur den Ordner „Sitzungstermine“ sehen und darin schreiben.

Hierzu legen Sie zwei Gruppen an: Gremiumsmitglieder und Sekretär. Sie geben beiden Gruppen auf der obersten Ebene alle Rechte, schließen jedoch bei den darunter liegenden Ordnern, außer vom Ordner „Sitzungstermine“, den Sekretär aus.

10 Datenraum in ein Archiv umwandeln

Nach Abschluss eines Projektes wird das Archivieren des Datenraums empfohlen. Anschließend kann der Datenraum gelöscht werden. Bei Löschung wird die entsprechende Lizenz frei und kann wieder neu verwendet werden.

Die Archivierung erfolgt in wenigen Schritten:

- Alle Dokumente auf „normal“ einstellen, d.h. kein Wasserzeichen und kein „Nur lesen“.
- Alle Verzeichnisse des Datenraums auf der obersten Verzeichnisebene markieren.
- Download aktivieren.
- Der gesamte Datenraum wird als eine ZIP-Datei auf den PC-geladen.
- Das Archiv wird anschließend entsprechend der Regeln Ihrer Organisation bzw. Ihres Unternehmens gespeichert.

Sollten Sie keine Antworten auf Ihre Fragen bezüglich der Bedienung von Versiegelte Cloud in diesem Handbuch gefunden haben, kontaktieren Sie bitte unseren Versiegelte Cloud Support unter:



Service Desk, Telefonischer-Support über das Customer Interaction Center:

- Kunden-Hotline: 0800 33 04444
- Service-Zeiten: Mo-Fr von 8-20 Uhr
- Problem Management und Produkt-Sales



Hinweis: nicht alle in diesem Handbuch beschriebenen Features sind für alle Pakete der Versiegelten Cloud verfügbar. Bei zusätzlichem Bedarf wenden Sie sich bitte an Ihren persönlichen Kundenberater.