

Herzlich willkommen beim
sicheren Cloudspeicher
made in Germany!

Datenverschlüsselung
in der luckycloud

Datenverschlüsselung bei luckyStorage

Beim luckyStorage wird zwischen zwei Arten von Verschlüsselungen unterschieden:

1. https-Verschlüsselung:

Die TLS-Transport-Verschlüsselung wird **automatisch beim Datentransfer** eingesetzt und verhindert das Abgreifen von Daten auf dem Übertragungsweg durch Dritte („Man in the Middle“).

2. Ende-zu-Ende Verschlüsselung:

Durch das Zero-Knowledge-Cloud Prinzip und echter Ende-zu-Ende Verschlüsselung, geben wir unseren **Nutzern die Hoheit über Ihre Daten zurück**. Nur durch Einsatz von OpenSource Software können wir plausiblen Datenschutz anbieten und garantieren, dass nicht einmal luckycloud-Mitarbeiter in Ihre Daten einsehen können.

Wenn Sie Ihre Daten verschlüsseln, wird eine 32 Byte lange, kryptographisch starke Zufallszahl erzeugt. Diese wird als Dateiverschlüsselungsschlüssel verwendet. Dieser sog. Dateischlüssel wird mit einem Passwort zusätzlich verschlüsselt. luckycloud verwendet zunächst den PBKDF2-Algorithmus (1000 Wiederholungen von SHA256), um von dem Passwort ein Schlüssel/IV-Paar abzuleiten. Sämtliche Daten der Datei werden durch den Dateischlüssel mit AES 256/CBC verschlüsselt. Das Ergebnis wird als verschlüsselter Dateischlüssel bezeichnet.

Nach der Verschlüsselung werden die Daten auf den Server hochgeladen und dort gespeichert. Wenn der Nutzer auf die Daten zugreifen möchte, können die Daten nur mit dem passenden Dateischlüssel entschlüsselt werden.

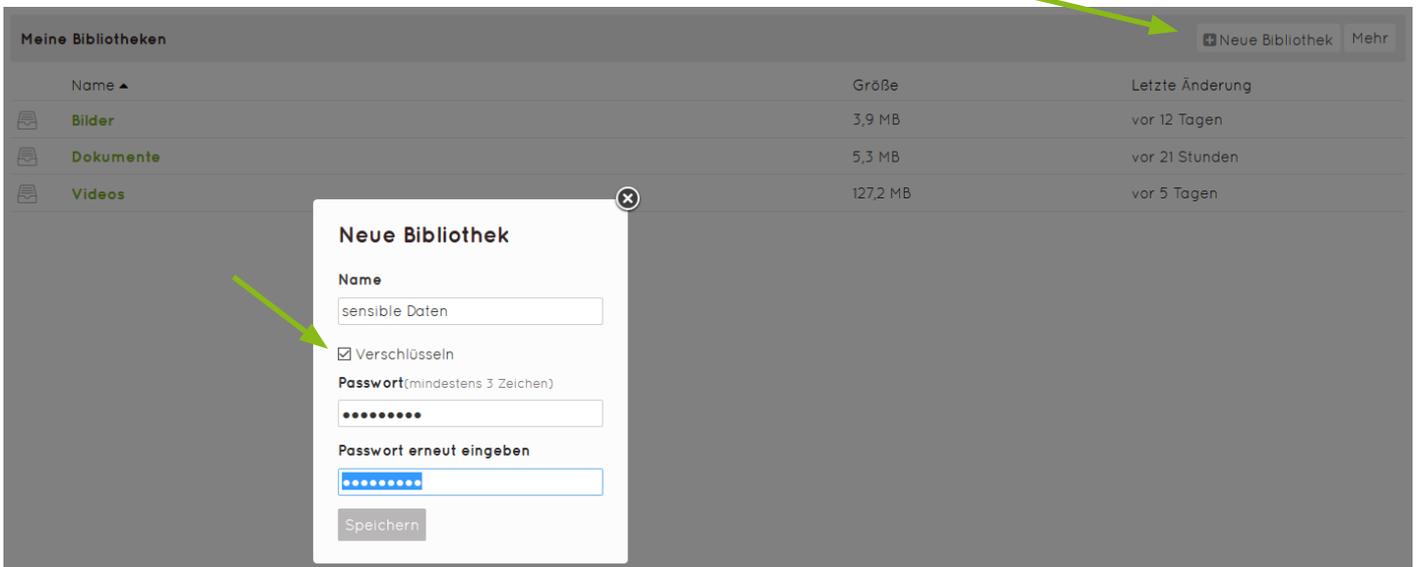
Um maximale Sicherheit zu gewährleisten, wird das Klartext-Passwort niemals auf dem Server gespeichert, sondern nur auf Ihrer Client-Seite.

Wie verschlüssele ich meine Daten?

Alle Ihre Daten werden **automatisch mit TLS** verschlüsselt. So können Dritte Ihre Daten nicht ausspähen.

Die Ende-zu-Ende Verschlüsselung können Sie im Webinterface unter **<https://storage.luckycloud.de>** bei der Erstellung einer Bibliothek einsetzen.

Gehen Sie dafür auf „**Neue Bibliothek**“ und setzen Sie danach ein Hacken bei „**Verschlüsseln**“.



The screenshot shows the 'Meine Bibliotheken' interface. At the top right, there is a button labeled 'Neue Bibliothek' and a 'Mehr' button. Below this is a table with columns for 'Name', 'Größe', and 'Letzte Änderung'. The table lists three libraries: 'Bilder' (3,9 MB, vor 12 Tagen), 'Dokumente' (5,3 MB, vor 21 Stunden), and 'Videos' (127,2 MB, vor 5 Tagen). A modal dialog box titled 'Neue Bibliothek' is open in the foreground. It contains a 'Name' field with the text 'sensible Daten', a checked checkbox for 'Verschlüsseln', a 'Passwort (mindestens 3 Zeichen)' field with masked characters, and a 'Passwort erneut eingeben' field also with masked characters. A 'Speichern' button is at the bottom of the dialog.

Wählen Sie nun ein **Passwort bzw. Schlüssel für Ihre Bibliothek** aus und geben Sie es in das entsprechende Feld ein. Dieses Passwort benötigen Sie dann bei der Entschlüsselung der Bibliothek.

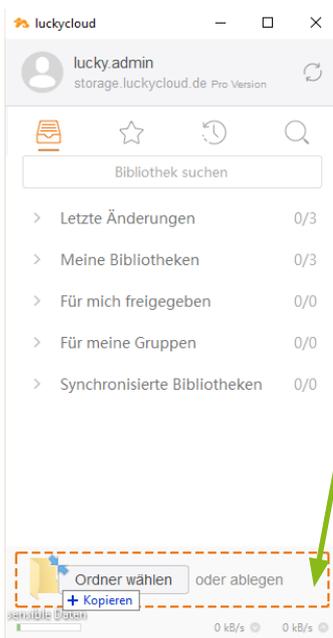
Wenn Sie die Bibliothek mit Ihren Benutzern teilen möchten, müssen Sie den Benutzern den Schlüssel mitteilen.

Hinweis:

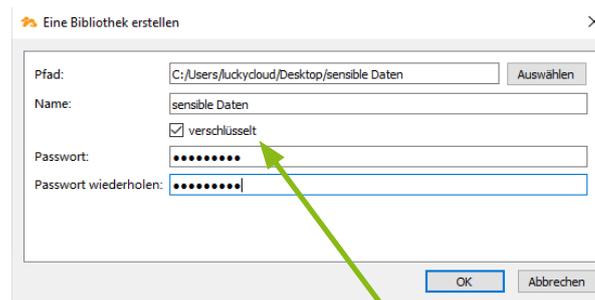
Um Ihnen die volle Schlüsselhoheit zu geben, werden die Schlüssel bzw. die Bibliothekspasswörter nicht auf unseren Servern gespeichert. Eine Passwortwiederherstellung ist somit nicht möglich, sofern Sie den Schlüssel verlieren sollten.

Wie verschlüssele ich meine Daten?

Im **Sync-Client** sieht die Erstellung einer Ende-zu-Ende verschlüsselten Bibliothek ähnlich aus:



Um eine verschlüsselte Bibliothek zu erstellen, müssen Sie den gewünschten Ordner einfach in das **entsprechende Feld** ziehen.



Setzen Sie dann einen Hacken bei „**verschlüsselt**“ und geben ein Bibliothekspasswort in die entsprechenden Felder ein.

Hinweis:

Eine Bibliothek kann **nachträglich nicht wieder entschlüsselt** bzw. verschlüsselt werden. Der Zustand einer Bibliothek ist irreversibel. Eine Bibliothek ist vergleichbar mit einem Fingerprint: Jede Bibliothek hat eine einmalige ID, die nicht geändert werden kann.

Wie erkenne ich eine echte Ende-zu-Ende Verschlüsselung?

Eine **echte** Ende-zu-Ende Verschlüsselung erkennen Sie daran, dass Sie selbst den Schlüssel wählen und Ihr Schlüssel nicht auf den Servern gespeichert wird (nur das dazu passende Schlüssel-paar). Nur so behalten Sie die Schlüsselhoheit über Ihre Daten!

Wann ist es sinnvoll zu verschlüsseln?

Anders als bei anderen Cloudanbietern, handelt es sich bei luckycloud um eine der wenigen **Zero Knowledge Clouds** aus Deutschland. Bei uns sind Sie Kunde - nicht das Produkt! Bei luckycloud bezahlen Sie nur mit Geld - nicht mit Ihren Daten. Wir scannen, analysieren oder verkaufen Ihre Daten **nicht**.

Da wir Ihre Daten in Ruhe lassen, ist es nicht immer sinnvoll alle Daten zu verschlüsseln, da mit der Ende-zu-Ende Verschlüsselung einige Funktionseinschränkungen mit eingehen:

Hinweis:

Aktuell können verschlüsselte Bibliotheken noch **nicht** mit dem **Drive Client** verwendet werden.

Bei verschlüsselten Bibliotheken ist es **nicht möglich Freigabelinks** zu erstellen, denn für die Entschlüsselung der Bibliothek wird ein luckycloud Benutzeraccount erfordert.

Es ist ebenfalls **nicht** möglich **einzelene Dateien oder Unterordner einer verschlüsselten Bibliothek** an Benutzer freizugeben, denn bei der Entschlüsselung wird die gesamte Bibliothek entschlüsselt.

Deswegen ist es umso wichtiger, sich vorher eine sinnvolle Ordnerstruktur zu überlegen.

Falls Sie sich nicht sicher sind, welche Daten Sie verschlüsseln sollten oder Hilfe bei der Ordnerstruktur benötigen, kann Sie unser Supportteam gerne **beraten**.

Vielen Dank, dass Sie sich für
luckycloud entschieden haben!



Haben Sie alles verstanden?

☞ Schauen Sie sich doch unsere
anderen Hilfestellungen an!

Wir freuen uns über Ihr Feedback!

☞ Google ☞ trustpilot ☞ trusted

luckycloud GmbH
Solmsstraße 18
10961 Berlin

+49(0) 30 89634840
websupport@luckycloud.de
www.luckycloud.de