

Installationsanleitung

Verschlüsselter Cloud-Datenaustausch

von: Marc Friedrich
DLRG OV Wartenberg
Cloud, Tools: **Nextcloud**, ownCloud und CrypSync
Ort und Datum: Wartenberg, 3. Oktober 2018

Vorwort

Die vorliegende Installationsanleitung „Verschlüsselter Cloud-Datenaustausch“ entstand beim Einrichten unseres *neuen* Laptops bevor es die DLRG.Cloud gab.

Es wird zum einen anhand einer eigenen „ownCloud“ [OWNCLOUD] Cloud gezeigt, wie auf eine einfache Art und Weise – „datenschutzkonform“ – Dateien über eine öffentliche Cloud im Internet Daten ausgetauscht werden können. Die dargestellte Methode lässt sich auch auf andere öffentliche Clouds übertragen, bspw. Dropbox, OneDrive, usw..



Mit der Freischaltung der DLRG.Cloud, welche auf Nextcloud [NEXTCLOUD] (ein Fork der ownCloud) basiert, wurde die Anleitung zum anderen darauf angepasst (die Aussagen zu ownCloud sind weitgehend alle auf die Nextcloud übertragbar). Zum besseren Verständnis wird aber auch die Installation der Nextcloud Schritt für Schritt erklärt.



Datenschutzkonform

Die Konformität zum Datenschutz bezieht sich in diesem Dokument nur auf die technischen und organisatorischen Maßnahmen (TOM) der sicheren Datenübertragung bzw. -speicherung über/auf unsicheren Medien (Internet/Cloud-Server). Die Übertragung über das Internet ist ohne Verschlüsselung unsicher. Das gleiche gilt für die Speicherung in einer Cloud, über die man selbst nicht die volle Kontrolle hat – das gilt bis zu einem bestimmten Grad auch für die DLRG.Cloud.

Es wird in diesem Dokument davon ausgegangen, dass die Daten/Dateien, die übertragen und gespeichert werden sollen, aus Datenschutzsicht übertragen und gespeichert werden dürfen. Diese Prüfung muss ggf. vorab für jede Datei oder Datensammlung, welche personenbezogene Daten enthält, gemacht werden. Das ist aber ein anderes Thema und wird nicht in diesem Dokument behandelt (vgl. bspw. <https://atlas.dlrg.de/confluence/display/AN/Datenschutz>).

Inhaltsverzeichnis

Vorwort	2
Datenschutzkonform	2
Inhaltsverzeichnis	3
Aufgabenstellung	4
Datenschutzkonformer Austausch von Daten über eine öffentlich Cloud-Lösung	4
Zielgruppe	4
Architektur	5
Erläuterung	6
Installation und Einrichtung öffentliche ownCloud	7
1. Cloud-Dienst beim Dienstanbieter einrichten	7
2. Lokales Transportverzeichnis einrichten	7
3. Lokales Arbeitsverzeichnis einrichten	7
4. Synchronisation zur Cloud einrichten	7
5. Lokale Synchronisation und Ver-/Entschlüsselung einrichten	10
Installation und Einrichtung DLRG.Cloud (Nextcloud)	15
1. DLRG.Cloud auf der Serverseite (DLRG) einrichten	15
DLRG-Account	15
2. Lokales Transport-/Arbeitsverzeichnis einrichten	15
3. Synchronisation zur DLRG.Cloud einrichten	15
4. Ggf. einzelne Dateien mit Office-Tools verschlüsseln	19
Fazit	21
Abbildungsverzeichnis	22
Abkürzungsverzeichnis / Glossar	22
Literatur- und Quellenverzeichnis	22

Aufgabenstellung

Datenschutzkonformer Austausch von Daten über eine öffentlich Cloud-Lösung



Die Rahmenbedingung dabei sind folgende:

1. Einhaltung gesetzlicher Rahmenbedingungen, insbesondere der DSGVO.
2. Einfache Einrichtung.
3. Datenaustausch über Ortsgruppen hinweg.
4. Gemeinsames Arbeiten an Dokumenten.
5. Kostengünstiger und einfacher Betrieb.

Da weder Bundes- noch Landesverband eine solche Lösung zur Verfügung stellen, ist hier Eigeninitiative gefragt.

Die o.g. Forderungen werden durch die Verwendung von

1. Verschlüsselung (Ende-zu-Ende),
2. Installationsanleitung,
3. Cloud-Lösung mit Rechte- und Rollenkonzept,
4. Zeitnahe automatische Synchronisation und
5. Verwendung von lizenzfreien oder kostenlosen Open Source bzw. Public Domain Tools

erreicht.

Zielgruppe

Alle interessierten.

Architektur

Nachfolgend wird der Aufbau der Lösung gezeigt. Dabei wollen die beiden fiktiven Mitglieder Alice und Bob gemeinsam an einem Dokument arbeiten – zeitversetzt, nicht exakt zur selben Zeit.

Exemplarisch ist hier die „Seite“ von Alice bis zum Internet in die (own)Cloud dargestellt¹.



Abbildung 1: Dateiaustausch von Alice mit der Cloud

¹ Die Icons sind aus dem Tango Desktop Project [TANGO].

Erläuterung

Arbeitsverzeichnis (unverschlüsselt)

Das *Arbeitsverzeichnis* ist die lokale Verzeichnisstruktur auf dem Computer von Alice oder Bob, in dem die Daten zum Bearbeiten unverschlüsselt vorliegen.



Beispiel Alice, im Benutzerverzeichnis auf dem Laufwerk C:\:

```
C:\USERS\ALICE\OWNCLOUD_LOKAL
+---(R-)Schwimmausbildung_WB_insecure
|  \---Rundschreiben
+---Datenschutz_insecure
|  +---DLRG-Intranet-Datenschutz
|  +---Literatur
|  \---OV_Wartenberg
\---Training_ED-WB_insecure
```

Beispiel Bob, auf einem zusätzlichen Laufwerk D:\:

```
D:\WARTENBERG-DLRG.DE_BOB_LOKAL
+---(R-)Schwimmausbildung_WB_insecure
|  \---Rundschreiben
+---Datenschutz_insecure
|  +---DLRG-Intranet-Datenschutz
|  +---Literatur
|  \---OV_Wartenberg
\---Training_ED-WB_insecure
```

Transportverzeichnis (verschlüsselt)

Das *Transportverzeichnis* ist die lokale Verzeichnisstruktur auf dem Computer von Alice oder Bob, in dem die Daten verschlüsselt vorliegen, so wie sie in die Cloud kopiert werden.



Beispiel Alice:

```
C:\USERS\ALICE\OWNCLOUD
+---Documents
|  +---(R-)Schwimmausbildung_WB_secure
|  |  \---Rundschreiben
|  +---Datenschutz_secure
|  |  +---DLRG-Intranet-Datenschutz
|  |  +---Literatur
|  |  \---OV_Wartenberg
|  \---Training_ED-WB_secure
```

Beispiel Bob:

```
D:\WARTENBERG-DLRG.DE_BOB
+---Documents
|  +---(R-)Schwimmausbildung_WB_secure
|  |  \---Rundschreiben
|  +---Datenschutz_secure
|  |  +---DLRG-Intranet-Datenschutz
|  |  +---Literatur
|  |  \---OV_Wartenberg
|  \---Training_ED-WB_secure
```

Cloud-Verzeichnis (verschlüsselt)

Das *Cloud-Verzeichnis* ist die Verzeichnisstruktur in der Cloud.

Die Verzeichnisstruktur wird z.T. vom Dienst vorgegeben oder von der lokal angelegten Struktur.



Installation und Einrichtung öffentliche ownCloud

Reihenfolge der Installations- und Einrichtungsschritte:

1. Cloud-Dienst beim Dienstanbieter einrichten.
2. Lokales Transportverzeichnis einrichten.
3. Lokales Arbeitsverzeichnis einrichten.
4. Synchronisation zur Cloud einrichten.
5. Lokale Synchronisation und Ver-/Entschlüsselung einrichten.

1. Cloud-Dienst beim Dienstanbieter einrichten

Das Vorgehen ist von Cloud zu Cloud unterschiedlich und wird hier nicht näher beschrieben. Ebenso wird auf die Beschreibung der Benutzerverwaltung sowie auf die des Rechte- und Rollenkonzepts verzichtet und auf die Anleitung des jeweiligen Anbieters verwiesen.

2. Lokales Transportverzeichnis einrichten

Das lokale Transportverzeichnis wird ganz normal mit dem Windows Explorer oder einem anderen Tool angelegt. Der Ort kann frei gewählt werden, s. die Beispiele von Alice und Bob. Es wird bei der täglichen Arbeit nur von den Tools benötigt. Alice und Bob benutzen es i.d.R. nicht direkt.

3. Lokales Arbeitsverzeichnis einrichten

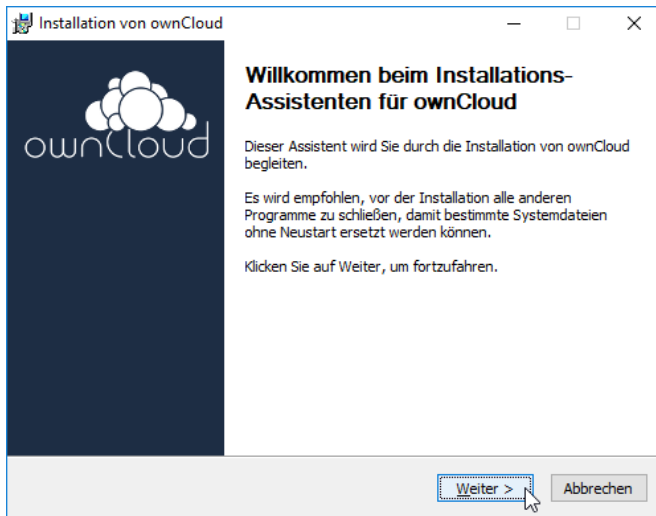
Das lokale Arbeitsverzeichnis wird wie das lokale Transportverzeichnis angelegt. Der Ort kann ebenfalls frei gewählt werden, allerdings wird es – wie es der Name schon sagt – bei der täglichen Arbeit benötigt. Alice und Bob können direkt in diesem Verzeichnis arbeiten, bspw. ein Word-Dokument erstellen, an dem sie wechselseitig arbeiten. Es ist dabei allerdings darauf zu achten, dass immer nur einer das Dokument offen hat, da es ansonsten bei der Synchronisierung zu Versionskonflikten kommt.

4. Synchronisation zur Cloud einrichten

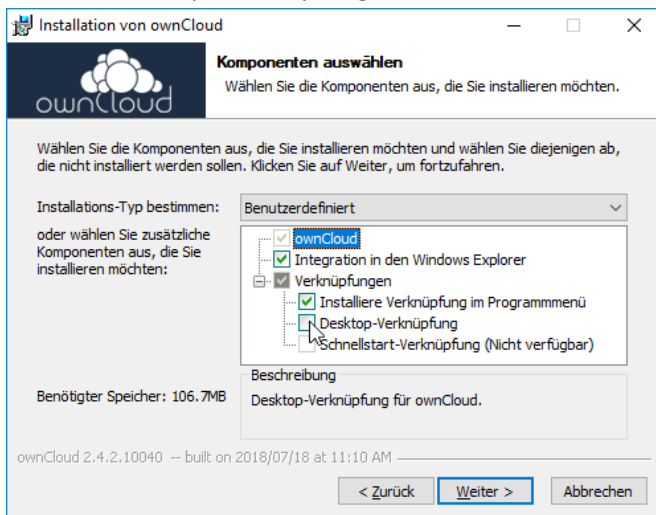
Das Einrichten der Synchronisation mit dem Speicher in der Cloud ist von der verwendeten Cloud abhängig. Die hier vorgestellte Schritt-für-Schritt-Anleitung bezieht sich auf die ownCloud des OV Wartenberg. Prinzipiell ist das Vorgehen aber für alle Clouds ähnlich. Die Angaben passen nicht ganz zu den Beispielen von Alice und Bob, daher sind ein paar Details verpixelt. Diese Details sind von der jeweiligen Installation abhängig und müssen zwischen den beteiligten Personen abgestimmt werden.

1. ownCloud Desktop Client von der Webseite herunterladen, die „production“ Version:
<https://owncloud.org/download/#owncloud-desktop-client-windows>

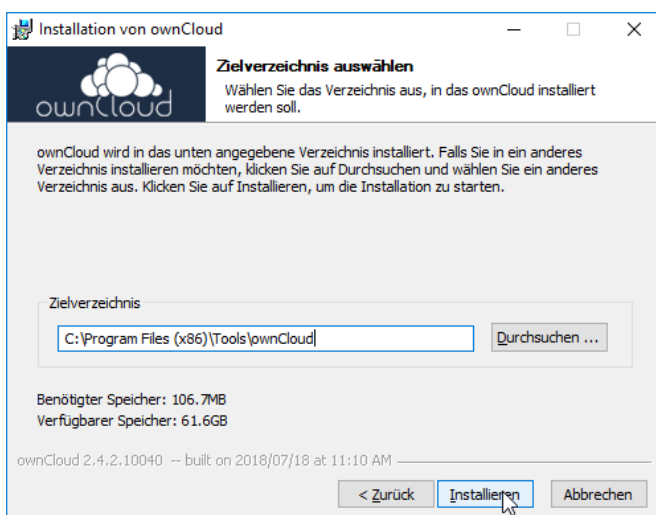
2. Installer starten und den Willkommensdialog mit weiter bestätigen:



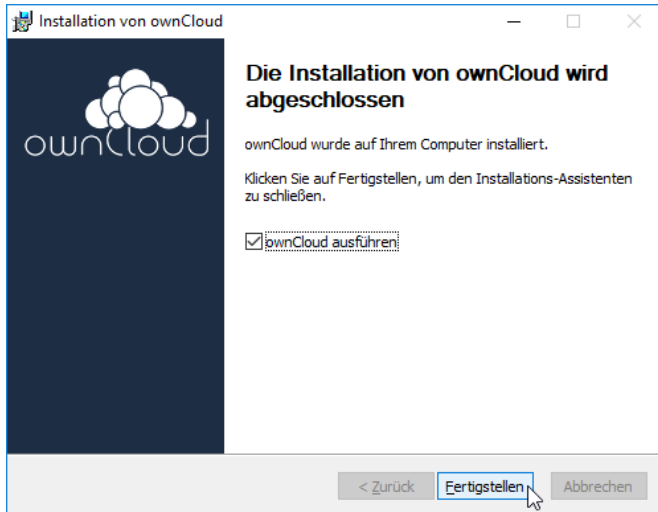
3. Evtl. die Desktop-Verknüpfung ausschalten und mit weiter bestätigen:



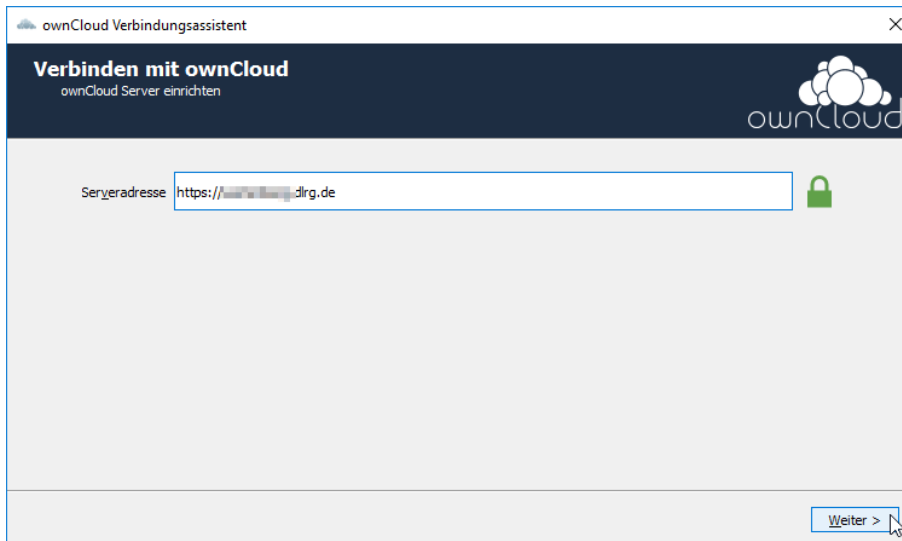
4. Den Ort für die Installation auswählen und mit Installieren bestätigen:



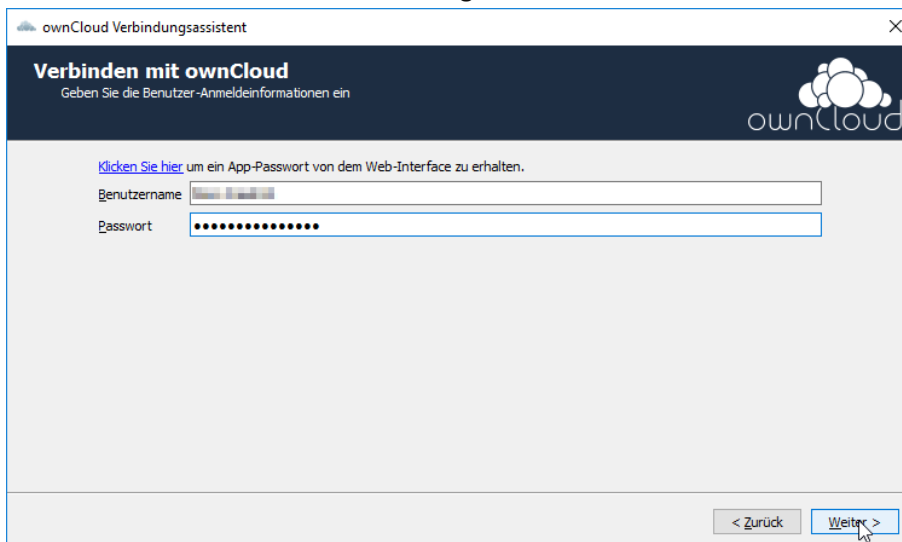
5. ... und erstellen:



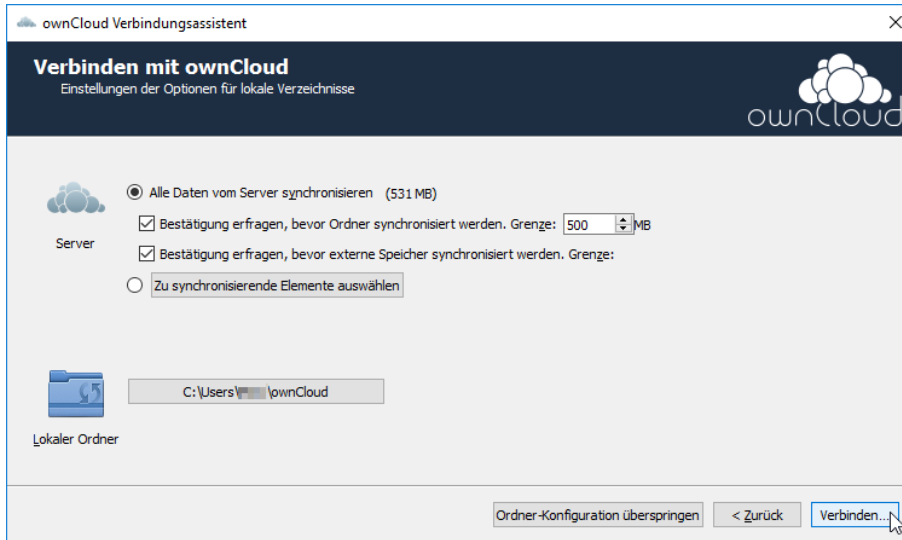
6. Es sollte der Verbindungsassistent starten, in dem die Serveradresse einzutragen ist:



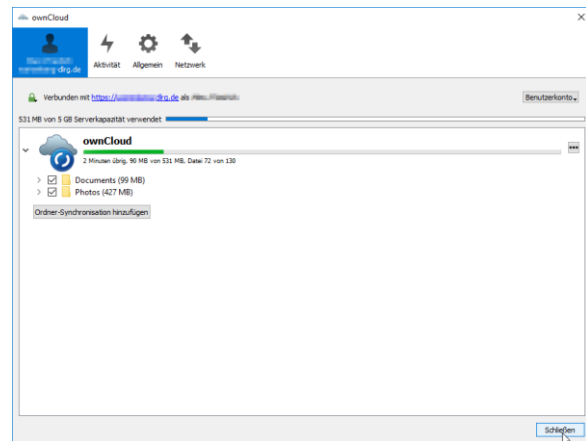
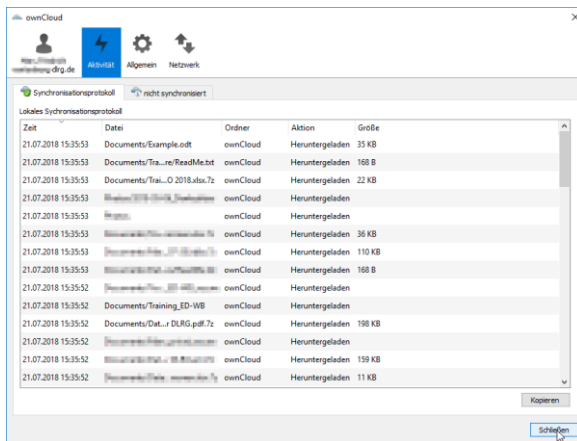
7. Dann sind User und Passwort einzutragen:



8. ... und vor dem ersten Verbinden ist das lokale Transportverzeichnis auszuwählen:



Ab jetzt läuft die Synchronisation zwischen dem Transportverzeichnis mit dem Cloud-Verzeichnis. Wenn schon etwas in der Cloud gespeichert ist, wird das noch leere Transportverzeichnis gefüllt – da können auch Beispieldateien des Cloud-Anbieters dabei sein:



5. Lokale Synchronisation und Ver-/Entschlüsselung einrichten

Abschließend folgt die Einrichtung der Synchronisation mit der automatischen Ver-/Entschlüsselung zwischen Transportverzeichnis und Arbeitsverzeichnis. Die hier vorgestellte Schritt-für-Schritt-Anleitung passt nicht ganz zu den Beispielen von Alice und Bob, daher sind ein paar Details verpixelt. Diese Details sind von der jeweiligen Installation abhängig und müssen zwischen den beteiligten Personen abgestimmt werden.

1. Die aktuelle Version von CryptSync (<https://tools.stefankueng.com/CryptSync.html>) muss heruntergeladen werden, die *.msi Version verwenden, ggf. die 64-Bit Version für ein 64 Bit Windows:

<https://github.com/stefankueng/CryptSync/releases>

2. Wenn über die Cloud mehrere Gruppen Daten und Dateien austauschen wolle/sollen, so macht es Sinn für jede Gruppe ein eigenes Verzeichnis anzulegen, so wie es Alice und Bob für
 - a. „(R-)Schwimmausbildung_WB_insecure“,
 - b. „Datenschutz_insecure“ und
 - c. „Training_ED-WB_insecure“

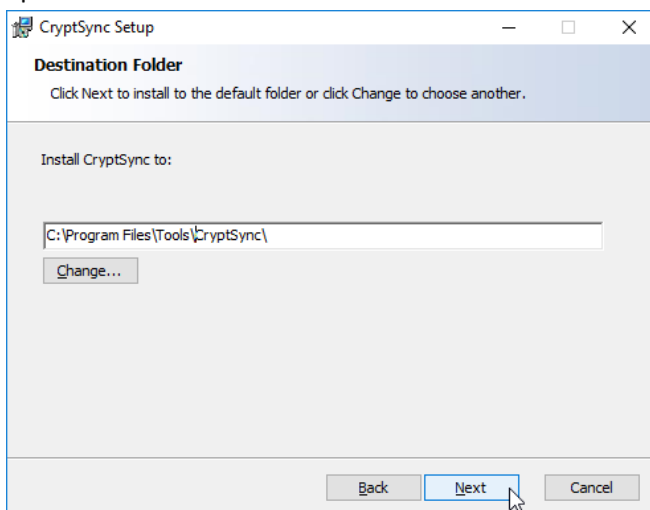
gemacht haben.

Das bietet auch den Vorteil, dass man – wenn man möchte – auch für jede Gruppe bzw. jedes Verzeichnis ein eigener Schlüssel für die Verschlüsselung gewählt werden kann. Wenn man sich allerdings nur vor „unberechtigten Dritten“ schützen möchte, bspw. Hacker oder Administratoren der Cloud, reicht auch ein Passwort. Der Zugriffsschutz erfolgt dann über das Rechte- und Rollenmodell der Cloud, bspw. wird ein Order mit einer Person oder Gruppe „geteilt“ und diese kann dann darauf zugreifen.

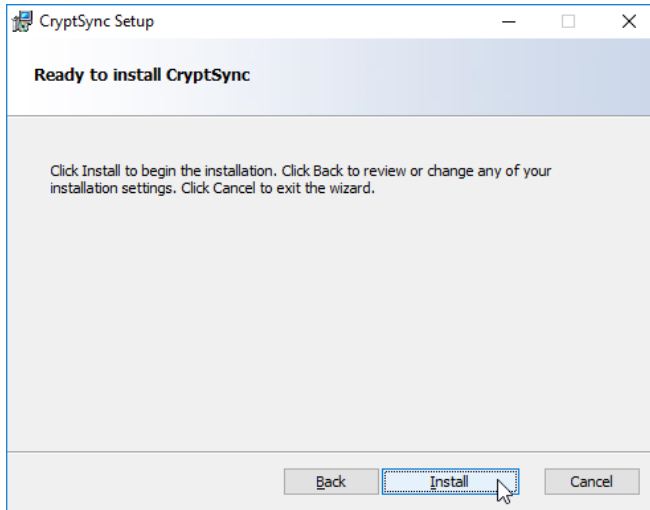
3. Doch nun zum Einrichten von CryptSync. Den Installer starten und mit Next bestätigen:



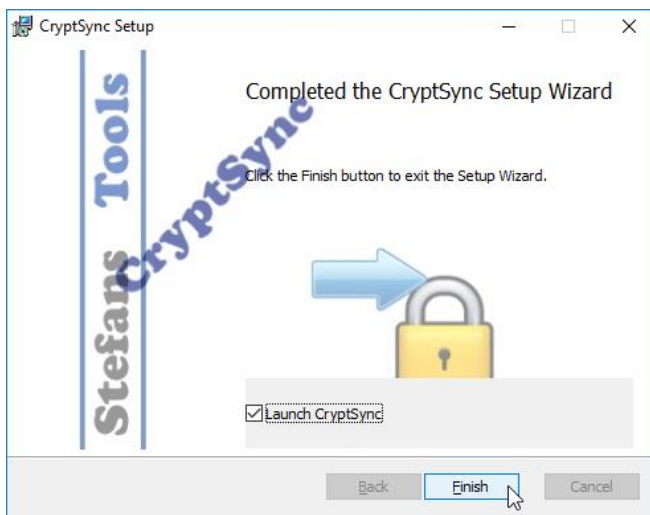
4. Speicherort der Software auswählen:



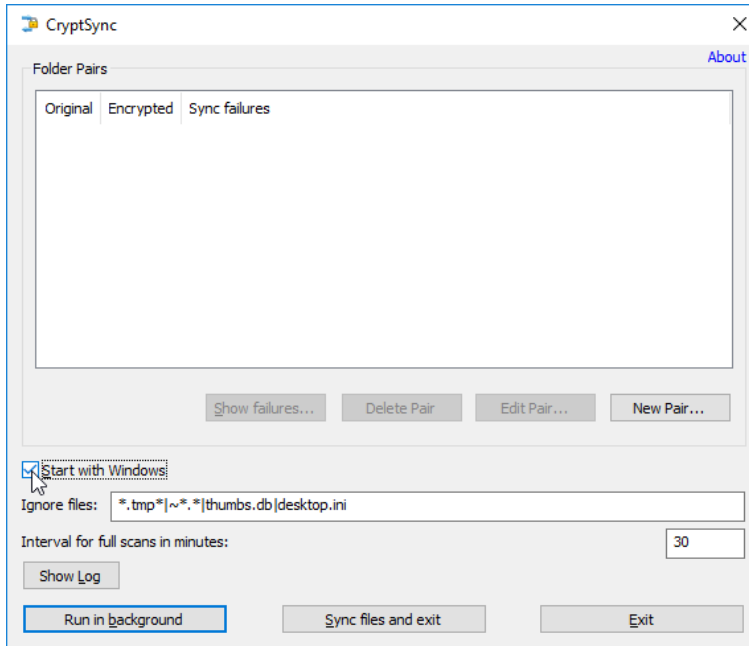
5. Die Installation abschließen:



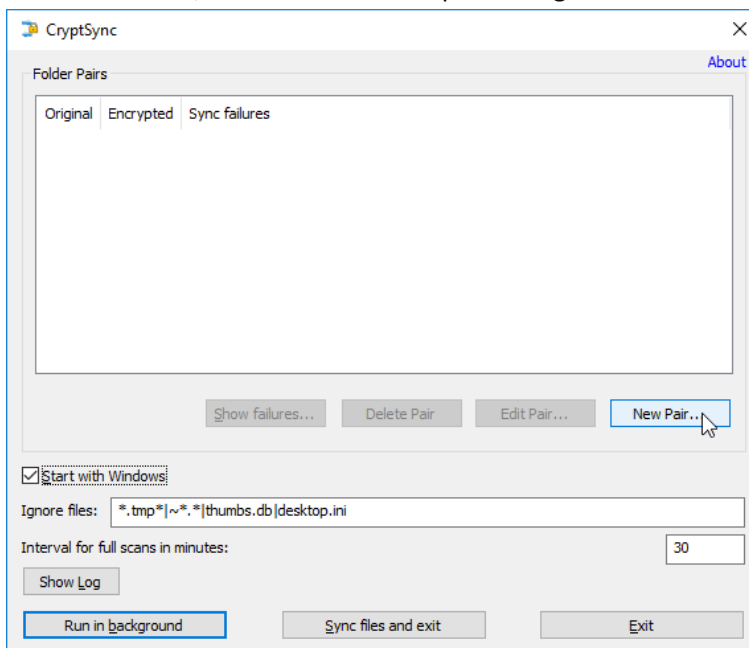
6. ... und das Tool starten:



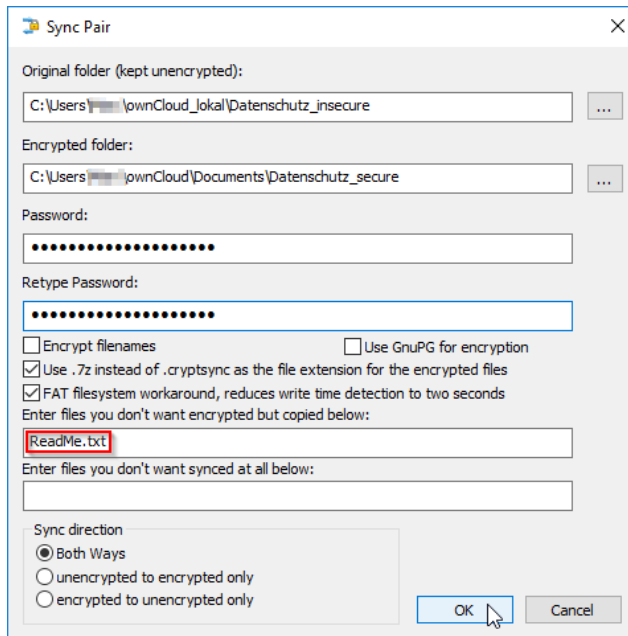
7. Den Haken für den automatischen Start mit Windows setzen:



8. ... und das erste/nächste Verzeichnispaar anlegen:



9. Die Parameter für die Verzechnissynchronisation und Ver-/Entschlüsselung angeben:



Hier am Beispiel des Datenschutz-Verzeichnisses² für den Vorstand und den Referenten Datenschutz.

Daher wir eine ReadMe.txt Datei als Erklärung in jedem Ordner liegen haben wollen, wird diese von der Verschlüsselung explizit ausgenommen und ist immer im Klartext vorhanden (s. rot umrandeter Text).

10. Wiederholen des Schrittes 8 und 9 für alle Verzeichnisse.

Fertig!

² Analog der Datenstruktur, die auch Alice gewählt hat.

Installation und Einrichtung DLRG.Cloud (Nextcloud)

1. DLRG.Cloud auf der Serverseite (DLRG) einrichten

Die Einrichtung der DLRG.Cloud ist auf <https://atlas.dlrg.de/confluence/display/AN/DLRG-Cloud> beschrieben. Es gibt dort aber (bis jetzt) keine Schritt für Schritt Anleitung des Synchronisations-Clients auf der Windows-/Client-Seite.

DLRG-Account

Für die Verwendung der DLRG.Cloud muss jeder Benutzer einen eigenen DLRG-Account besitzen (vgl. <https://atlas.dlrg.de/confluence/display/AN/DLRG-Account>).

2. Lokales Transport-/Arbeitsverzeichnis einrichten

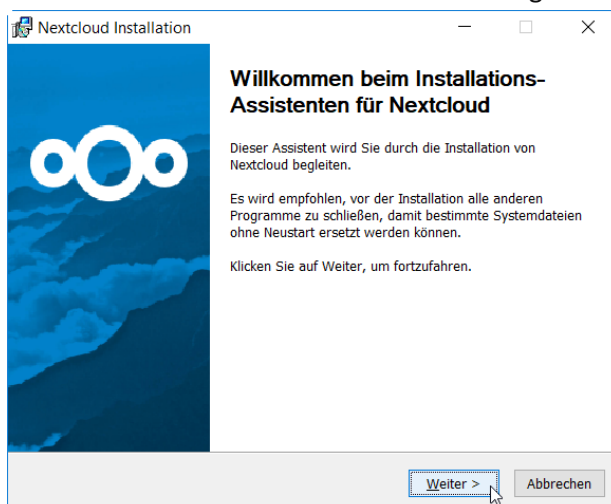
Das lokale Transportverzeichnis wird ganz normal mit dem Windows Explorer oder einem anderen Tool angelegt. Der Ort kann frei gewählt werden, s. die Beispiele von Alice und Bob.

Auf Grund der anderen Vertrauensstellung des Betreibers der DLRG.Cloud (Bundesverband der DLRG) mit dem eine DVIA bestehen sollte (vgl. Rundschreiben)

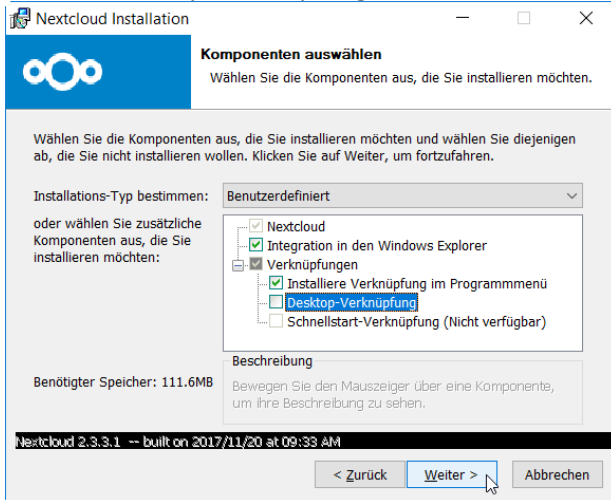
Es wird bei der täglichen Arbeit nur von den Tools benötigt. Alice und Bob benutzen es i.d.R. nicht direkt.

3. Synchronisation zur DLRG.Cloud einrichten

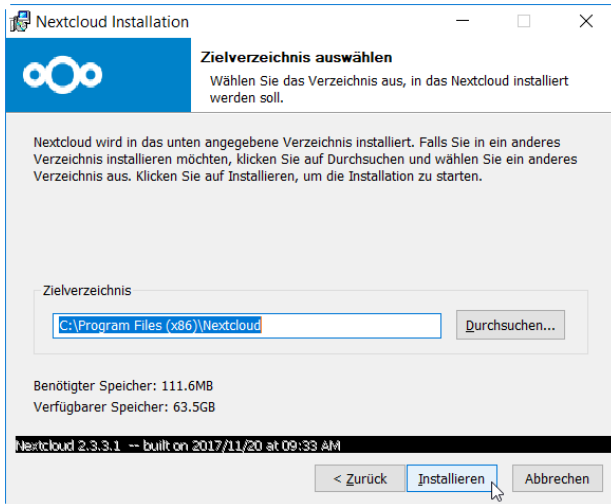
1. Nextcloud „Desktop Client“ von der Webseite herunterladen, „Sync your data“:
<https://nextcloud.com/de/install/#install-clients>
s. auch Anleitung unter <https://atlas.dlrg.de/confluence/display/AN/DLRG-Cloud>
2. Installer starten und den Willkommensdialog mit weiter bestätigen:



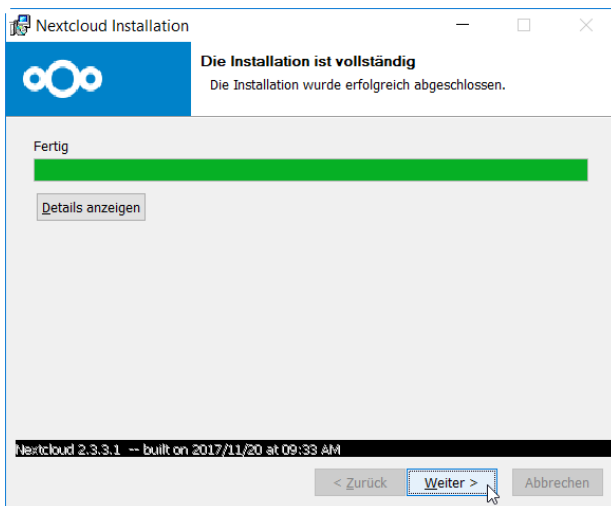
3. Evtl. die Desktop-Verknüpfung ausschalten und mit weiter bestätigen:



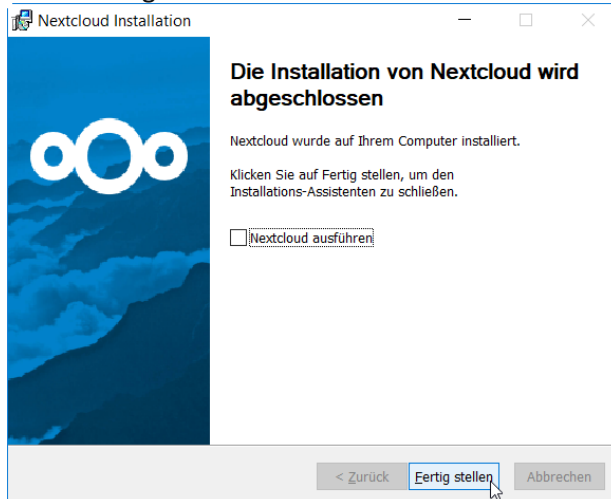
4. Den Ort für die Installation auswählen und mit Installieren bestätigen:



5. ... installieren:



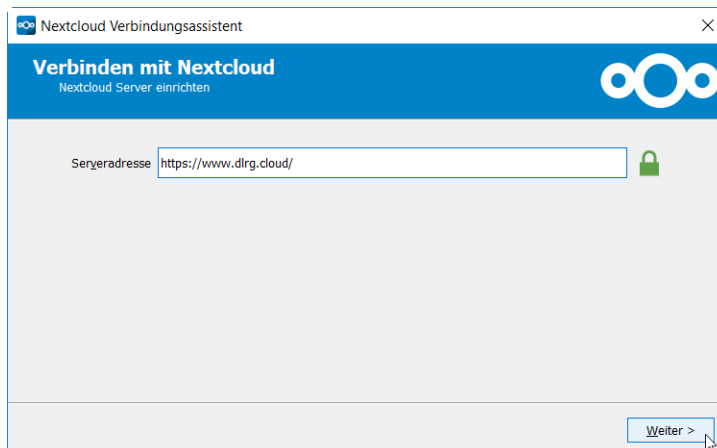
6. ... und Fertig stellen:



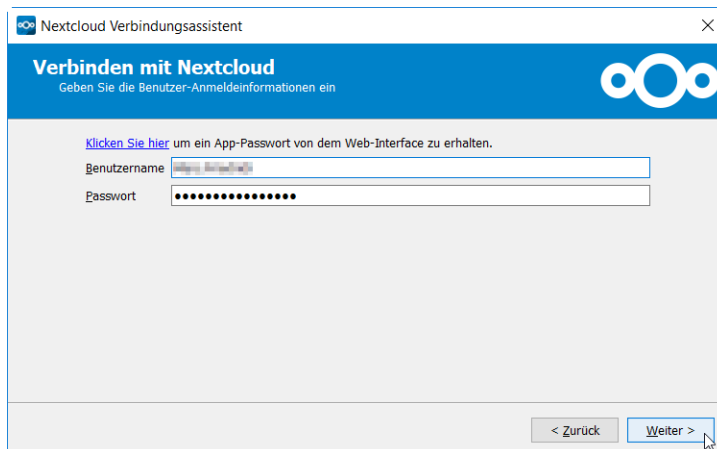
7. Das Nextcloud-Tool aus dem Windows-Start starten:



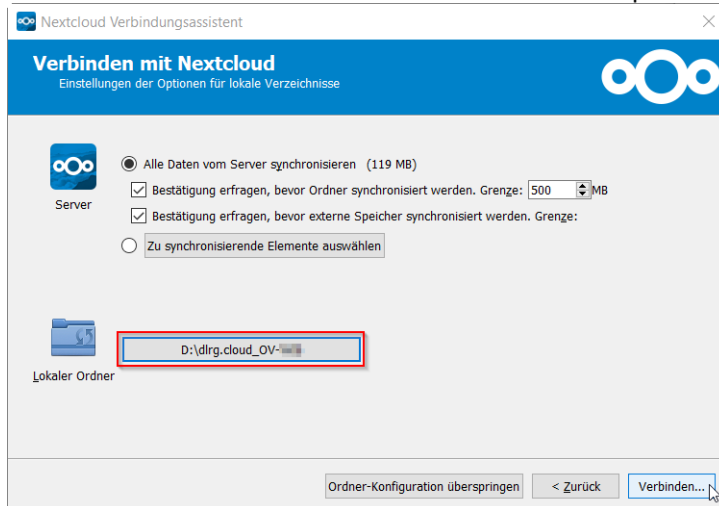
8. Es sollte der Verbindungsassistent starten, in dem die Serveradresse einzutragen ist:



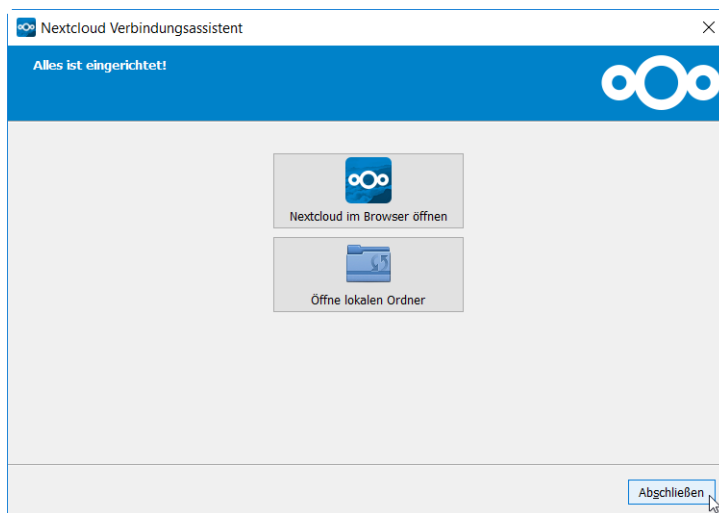
9. Dann sind User und Passwort des DLRG-Accounts einzutragen (das sind die selben wie im ISC):



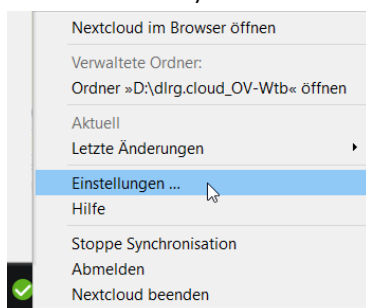
10. ... und vor dem ersten Verbinden ist das lokale Transportverzeichnis auszuwählen:



11. Installation abschließen:

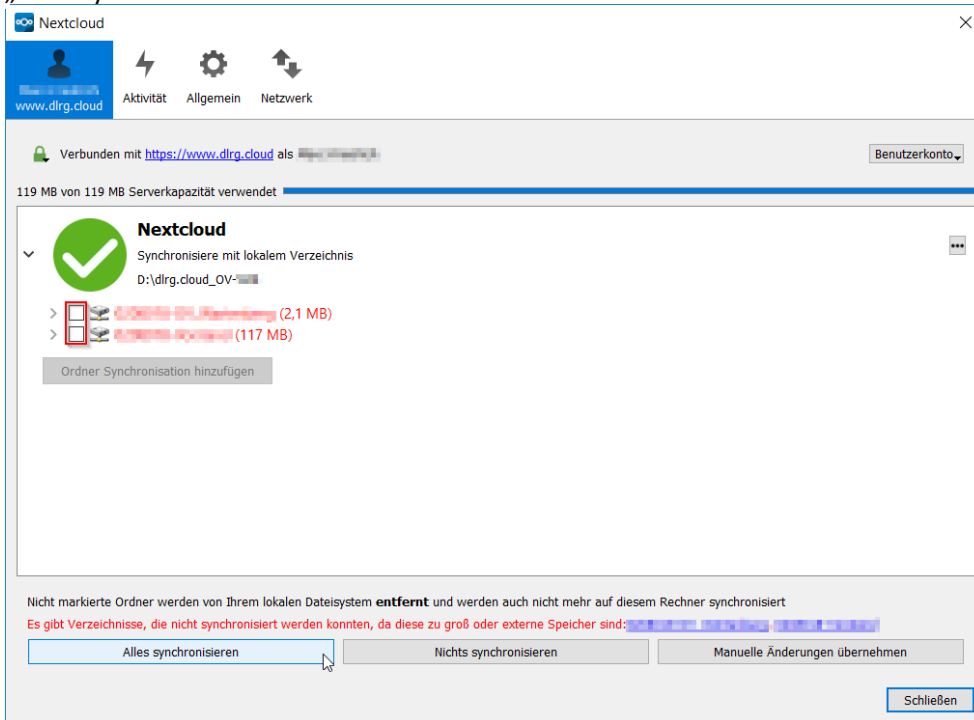


12. Öffnen aus dem Sys-Tray, grüner Kreis mit Haken (rechts unten die kleinen Icons beim Datum und der Uhrzeit):

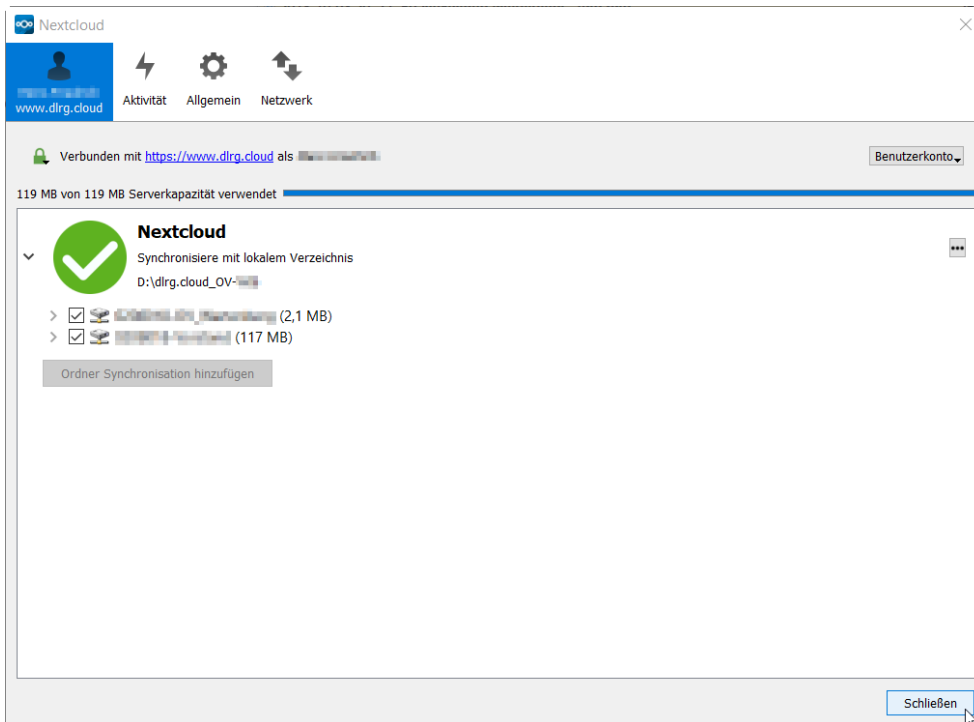


13. Ggf. Fehler beheben – Häkchen fehlen, keine Synchronisation

„Alles synchronisieren“ auswählen:



14. Nach dem Synchronisieren sollte es passen:

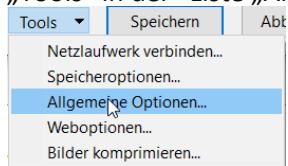


Fertig! Es sei denn, man möchte zusätzlich die Verschlüsselung einrichten (s.o. CryptSync).

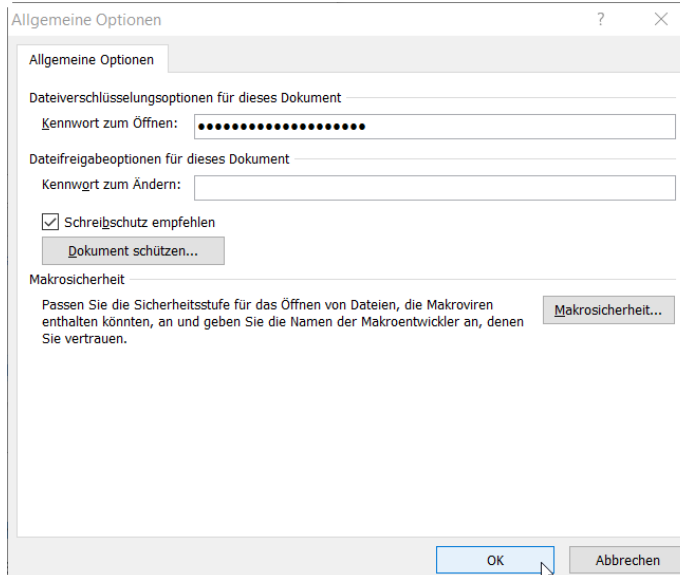
4. Ggf. einzelne Dateien mit Office-Tools verschlüsseln

Da diese Cloud aber eine höhere Vertrauensstellung hat und ein DVIA vorliegt, reicht es m.E., wenn einzelne Dateien mit personenbezogenen Daten oder mit vertraulichem Inhalt per Verschlüsselung der Office-Tools (bspw. Word oder Excel) geschützt werden:

1. „Datei“ / „Speichern unter“ auswählen und in dem Auswahldialog rechts unten bei „Tools“ in der Liste „Allgemeine Optionen“:



2. ... und dann das „Kennwort zum öffnen“ setzen.



Für Excel gilt ein analoges vorgehen.

ACHTUNG: „Dokument schützen“ alleine reicht nicht!

Die „geschützte“ Datei ist nur eine ZIP-Datei, die XML-Dateien enthält. Aus diesen XML-Dateien kann man ganz einfach den Schutz löschen.

Fazit

Es ist mit einfachen und kostenneutralen Mitteln möglich, einen datenschutzkonformen Daten und Dateiaustausch über das Internet zu ermöglichen, der auch ein gemeinsames Arbeiten an Dokumenten zulässt.

Abbildungsverzeichnis

Abbildung 1: Dateiaustausch von Alice mit der Cloud

Abkürzungsverzeichnis / Glossar

DSGVO Die **Datenschutz-Grundverordnung** (DSGVO) ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden. Dadurch soll einerseits der Schutz personenbezogener Daten innerhalb der Europäischen Union sichergestellt, und auch andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden.
[Wikipedia, 22.07.2018]

Literatur- und Quellenverzeichnis

[Wikipedia, Datum] Die Beschreibungen der Abkürzungen im Glossar sind i.d.R. der Wikipedia entnommen und im Glossar mit Abrufdatum angegeben. Suchkriterium war die Abkürzung. Wiedergegeben wird i.d.R. der erste Absatz.
<https://de.wikipedia.org/>

[NEXTCLOUD]

Nextcloud

Homepage: <https://nextcloud.com/>

Wikipedia: <https://de.wikipedia.org/wiki/Nextcloud>



[OWNCLOUD]

ownCloud

Homepage: <https://owncloud.org/>

Wikipedia: <https://de.wikipedia.org/wiki/OwnCloud>



[TANGO]

Das **Tango Desktop Project** ist ein freedesktop.org-Projekt mit dem Ziel, Benutzern eine einheitlichere grafische Benutzeroberfläche zu ermöglichen. Es stellt Entwicklern einen einheitlichen Iconsatz zur Verfügung, da die unterschiedliche Gestaltung der Desktop-Umgebungen von Microsoft Windows XP, macOS, KDE und Gnome es Entwicklern schwer macht, Programme optisch zu integrieren. Programme, die Icons benutzen, die dem Tango-Stil folgen, sollten sich trotz der verschiedenen Oberflächen äußerlich gut einpassen.

https://de.wikipedia.org/wiki/Tango_Desktop_Project

https://commons.wikimedia.org/wiki/Category:Tango_project