

Anmerkungen zu systemisch vorgegebenen Nutzungseinschränkungen und zur Datenschutzoptimierung bei OneDrive

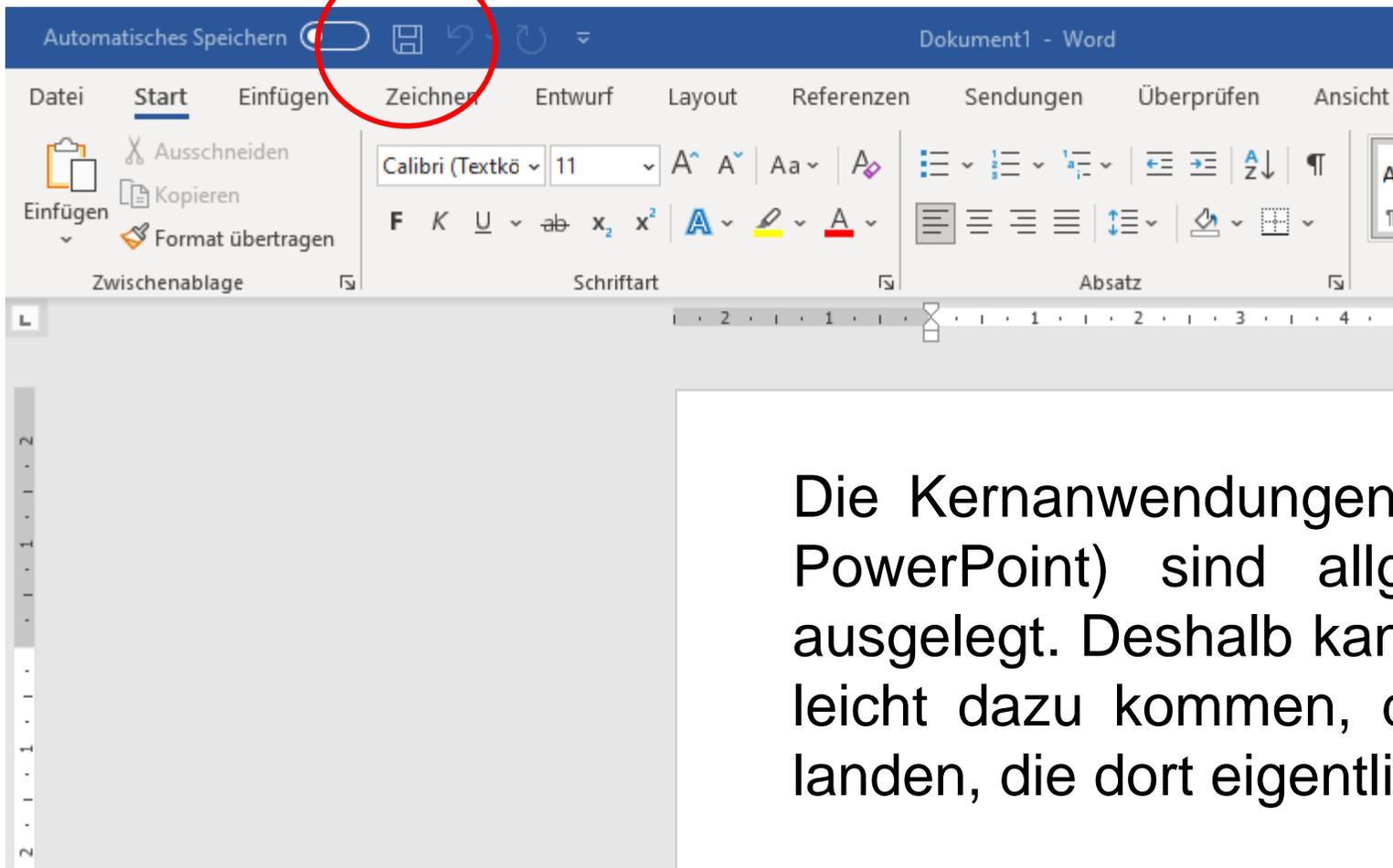
Office 365 besteht aus verschiedensten Programmen und Diensten. Die allermeisten davon dürfen verwendet werden. Einzelne stehen aus verschiedenen Gründen nicht zur Verfügung, dürfen nicht genutzt werden oder es gibt Auflagen:

Microsoft Teams, eine Plattform zum kollaborativen Arbeiten (Chat, Besprechung (Video/Audio), Anhänge ...), darf aus datenschutzrechtlichen Gründen nicht verwendet werden. Das Programm, das auf Windows und Mac separat zum Kernpaket installiert wird, kann also direkt nach Installation des Gesamtpaketes wieder deinstalliert werden.



OneDrive ist ein Clouddienst von Microsoft, der zur Onlinespeicherung von Daten zur Verfügung steht. Dieser darf genutzt werden, **aber nur für Dateien, die keine personenbezogenen Daten enthalten** (Arbeitsmaterial, Präsentationen, Dokumentvorlagen, ...). Um diesen Dienst soll es hier etwas näher gehen.





Die Kernanwendungen von Office 365 (Word, Excel, PowerPoint) sind allgemein für den Cloudbetrieb ausgelegt. Deshalb kann es bei Standardeinstellungen leicht dazu kommen, dass doch Daten in der Cloud landen, die dort eigentlich nicht hingehören.

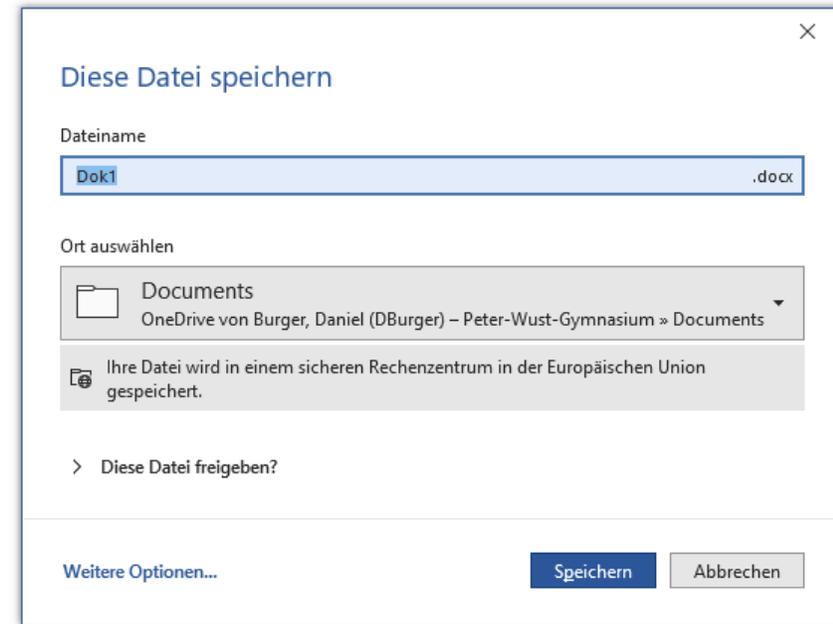
Hier ein kurzes Beispiel aus Word unter Windows 10: Nach Erstellen eines neuen Dokuments und Klick auf das Speichersymbol (roter Kreis) ...

... wird einem standardmäßig angeboten, die Cloud für die Speicherung zu nutzen.

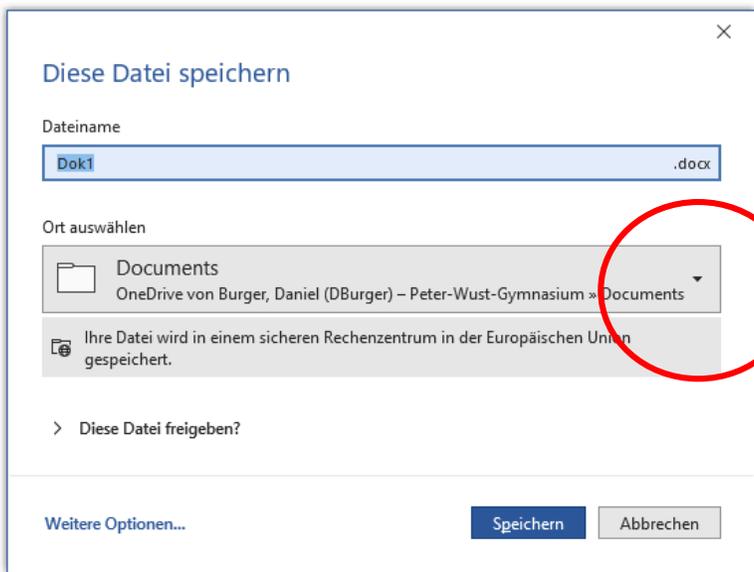
An diesem Punkt wäre zu überlegen, ob das Dokument in der Cloud gespeichert werden darf. Bei Dokumenten ohne personenbezogene Daten besteht kein Problem und es darf weitergehen.

Falls das Dokument personenbezogene Daten enthält, dann darf auch der Hinweis, dass die Datei in einem Rechenzentrum in der EU gelagert wird, nicht dazu verleiten, das Dokument doch dort zu speichern. Das ist aus verschiedenen datenschutzrechtlichen Gründen (zumindest momentan) nicht zulässig.

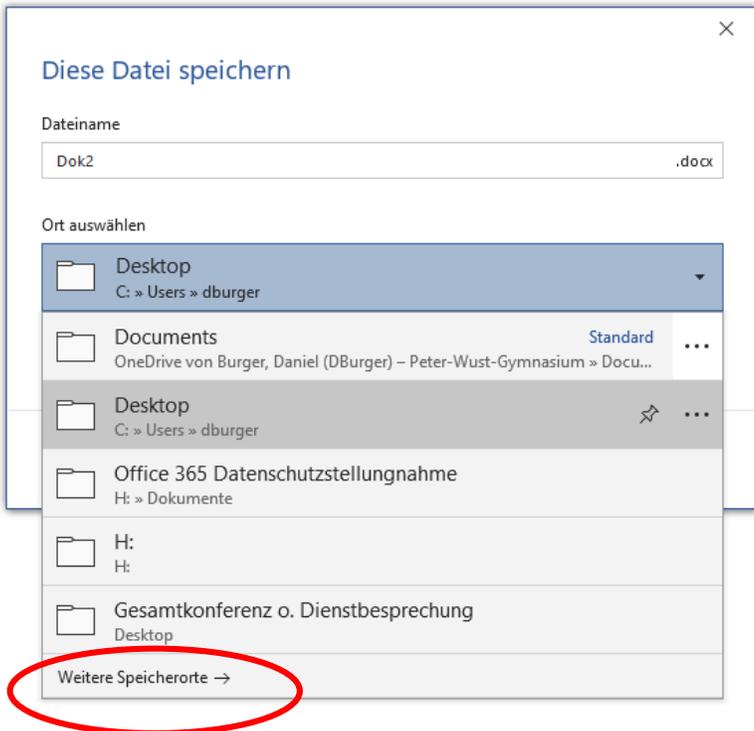
Dateien mit personenbezogenen Inhalten gehören nicht auf OneDrive.



Das Feature „Diese Datei freigeben“ sollte natürlich ebenfalls nicht für entsprechende Dokumente genutzt werden, denn die Freigabe erfolgt über die Cloud!

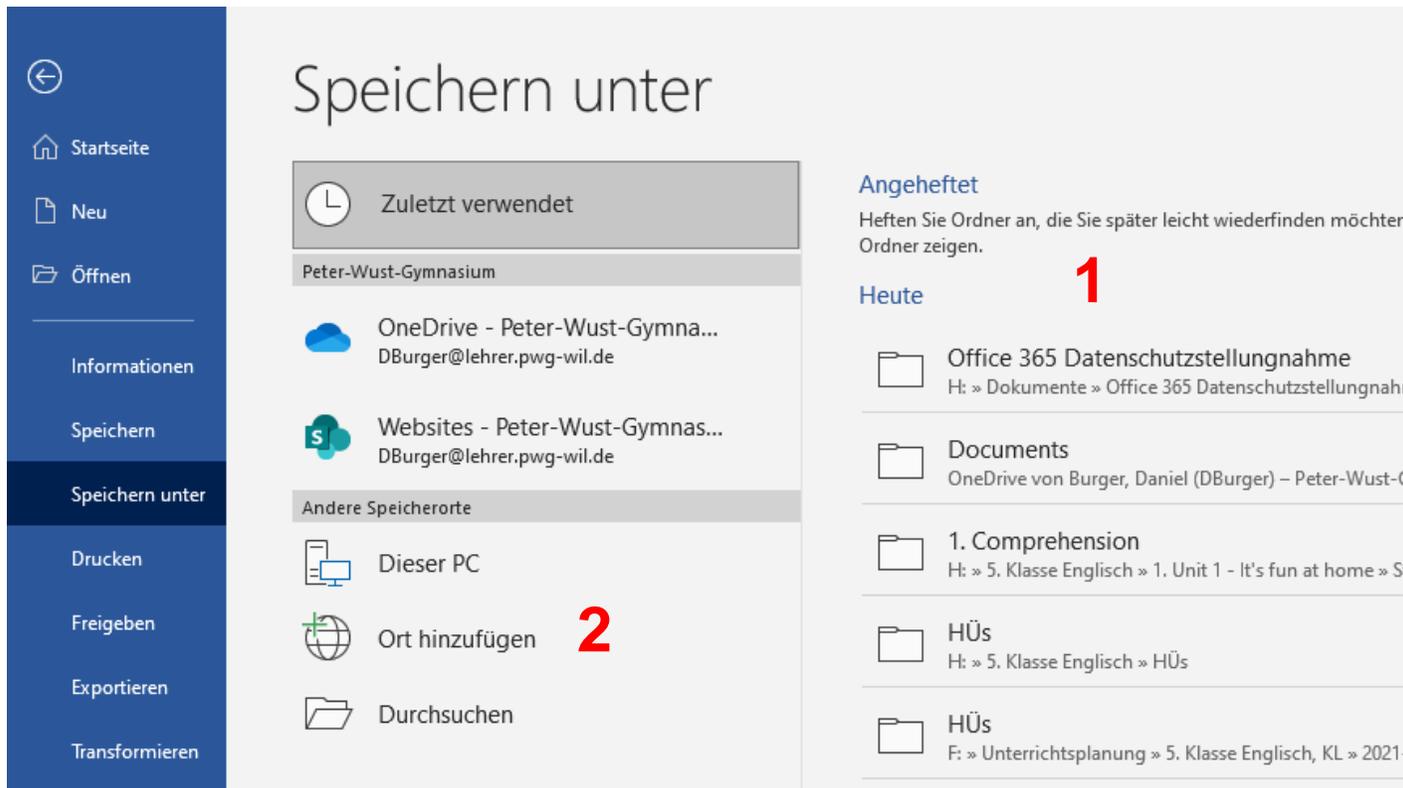


Falls das Dokument personenbezogene Daten enthält wäre also ein lokaler und idealer Weise verschlüsselter Speicherort zu wählen. Einen solchen Speicherort kann man hier im Menu mit Klick auf das umgekehrte Dreieck auswählen (siehe roter Kreis).



Angezeigt werden dann die zuletzt genutzten lokalen Speicherorte. Mit Klick auf „weitere Speicherorte“ (siehe rote Ellipse) erweitert sich die Liste der Möglichkeiten.

Mehr dazu auf der nächsten Folie.

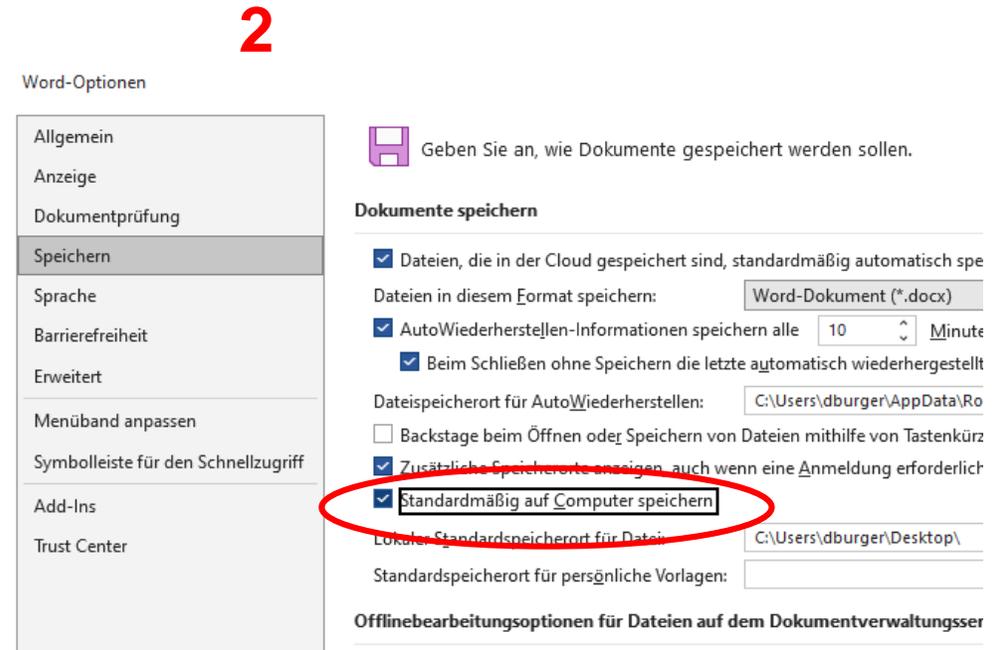
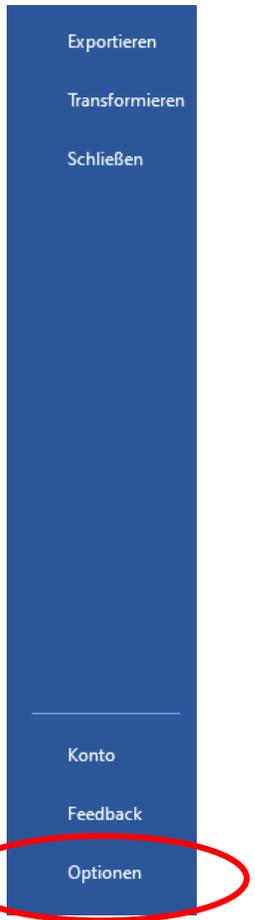


Falls der gewünschte Speicherort zuvor in der Kurzliste nicht angezeigt wurde, bekommt man nun eine längere Liste präsentiert (1) oder hat die Möglichkeiten, den Computer nach diesem zu durchsuchen (2).

Dieses Menu kann man durch Klick auf „Datei“ und dann auf „Speichern Unter“ auch direkt aufrufen.

Es anzuraten, die Standardeinstellungen so zu verändern, dass für neuerstellte Dateien beim Klick auf das Speichersymbol nicht standardmäßig die Cloud verwendet wird. Das kann man bei Word wie folgt einstellen (funktioniert bei den anderen Anwendungen analog):

1. In der Hauptanwendung zunächst ein Klick auf „Datei“.
2. Dann unten links ein Klick auf „Optionen“ (1, rote Ellipse).
3. Im Menu (2) dann Klick auf „Speichern“ und ein Häkchen bei „Standardmäßig auf Computer speichern“ setzen (rote Ellipse).
4. Jetzt wird einem beim Erstspeichern ein lokaler Speicherort zuerst vorgeschlagen.



Ungeachtet der vorgestellten Möglichkeiten zur Datenschutzoptimierung bleibt die Verwechslungsgefahr von lokalen Speicherorten und Speicherorten in der Cloud präsent.

Auch ist zu bedenken, dass bei Verwendung von Apps (Android, iOS, iPadOS) die Schritte zur Angabe bzw. Veränderung des Speicherortes anders sind und sich auch anders grafisch darstellen.

Bitte deshalb bei der Verwendung achtsam sein. Gleiches gilt bei Verwendung der OneCloud-Anwendung unter Windows. Auch hier sollte darauf geachtet werden, dass keine Dateien mit personenbezogenen Daten aus Versehen in der Cloud abgelegt werden.