

# Windows verschlüsseln mit Bitlocker

Diese Anleitung beschreibt, wie du einen Computer mit Windows verschlüsseln kannst. Es ist immens wichtig, dass du dir auch die [allgemeinen Informationen zum Thema Festplattenverschlüsselung](#) durchliest.

Wir empfehlen aktuell die in Windows integrierte Verschlüsselung, die "Bitlocker" genannt wird.

Bitlocker funktioniert nur auf Pro und Enterprise Editionen von Windows. In dieser Anleitung wird beschrieben, wie du herausfindest, welche Edition du hast und wie du sie umwandeln kannst.

Wenn dein Gerät verschlüsselt ist, lies bitte auch [diesen wichtigen Hinweis](#).

## Ist die Verschlüsselung schon aktiv?

Es kann gut sein, dass dein Rechner schon verschlüsselt ist. Um das herauszufinden, drücke die Windows-Taste auf der Tastatur und gebe "Bitlocker" ein. Dann:

- kommt eine Bing-Suche, wenn deine installierte Windows-Edition nicht ausreicht (siehe unten für mehr Details)
- falls Bitlocker unterstützt wird, klicke auf das Bitlocker-Symbol. Dann siehst du
  - den Text „Bitlocker deaktiviert“, wenn nichts verschlüsselt ist
  - „aktiviert“, wenn deine Festplatte bereits verschlüsselt ist

## Windows-Edition herausfinden

1. Windowstaste und X gleichzeitig drücken
2. Menüpunkt „System“ auswählen.
3. Unter der Überschrift „Windows Spezifikationen“ steht die Windows-Edition. Wenn da steht „Windows 10 Home“ dann folge bitte weiter dieser Anleitung. Wenn da „Windows 10 Pro“ oder „Windows 10 Enterprise“ steht kannst du zu „Verschlüsselung aktivieren (1. Schritt)“ springen.



# Windows-Edition ändern

Bitte einen entsprechenden Key kaufen. Die IT-AG kann dich dabei unterstützen.

## Verschlüsselung aktivieren (1. Schritt)

1. Windowstaste drücken, "Bitlocker" eingeben und "Bitlocker verwalten" anklicken.



2. Nun kann es sein, dass du die folgende Meldung erhältst:

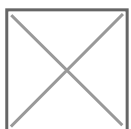


Wenn das der Fall ist, folge bitte dieser Anleitung weiter. Wenn das nicht der Fall ist springe zu "Verschlüsselung aktivieren (2. Schritt)".

## Verschlüsselung aktivieren (TPM-Fehler beheben)

Um diesen Fehler zu beseitigen bitte folgendes tun:

1. "Abbrechen" klicken.
2. Windowstaste zusammen mit R drücken und in das Dialogfeld "gpedit.msc" und Enter drücken.



2. Links folgendes auswählen: “Administrative Vorlagen”, “Windows Komponenten”...



3. ... “Bitlocker-Laufwerksverschlüsselung”, “Betriebssystemlaufwerke”.



4. Auf der rechten Seite “Zusätzliche Authentifizierung beim Start anfordern” doppelklicken:



5. Im folgenden Dialogfeld sicherstellen, dass links oben “Aktiviert” ausgewählt ist und weiter unten “BitLocker ohne kompatibles TPM zulassen [...]”. Danach auf OK drücken.



6. Das Gruppenrichtlinienfenster schließen.

7. Im Bitlocker-Fenster nochmal “Bitlocker aktivieren” anklicken.

8. Laufwerke sollten nur mit Passwort entsperrt werden, entsprechendes anklicken:



9. Jetzt ein Kennwort vergeben. Bitte lies dir unseren [allgemeinen Hinweise zum Thema Verschlüsselung](#) durch - das ist wichtig, damit dein Computer auch wirklich geschützt ist.



## Verschlüsselung aktivieren (2. Schritt)

1. Windows zwingt dich nun, Wiederherstellungsschlüssel für die Festplatte zu speichern - auch wenn du das gar nicht willst. Lies dir bitte zum Thema Wiederherstellungsschlüssel unsere [allgemeinen Hinweise zum Thema Verschlüsselung](#) durch. Speichere den Wiederherstellungsschlüssel auf keinem Fall in deinem Microsoft-Konto oder auf einem USB-Stick! Wähle stattdessen "Wiederherstellungsschlüssel drucken". Hinweis: es kann sein, dass hier weitere Optionen angezeigt werden, die nicht auf dem Screenshot unten zu sehen sind.



1. Wähle als Drucker "Microsoft Print to PDF".



1. Vergebe einen Namen und speichere die PDF auf dem Desktop.



Wenn du die Wiederherstellungsschlüssel nicht an einen vertrauenswürdigen Menschen geben willst, dann lösche sie gleich wieder. Halte dich ansonsten an die [Regeln aus den allgemeinen Hinweisen zur Verschlüsselung](#).

Klicke auf "Weiter".

Wähle im folgenden Dialogfenster "Gesamtes Laufwerk verschlüsseln", dann "Weiter":



1. Den Verschlüsselungsmodus auf "Neuer Verschlüsselungsmodus" lassen, "Weiter" klicken:

Verschlüsselungsmodus

1. "Bitlocker-Systemüberprüfung ausführen" muss ausgewählt sein, wieder "Weiter" drücken:

Jetzt verschlüsseln bestätigen

1. Und nun den Computer "Jetzt neu starten".



1. Der Computer wird jetzt verschlüsselt. Das dauert eine Weile, er kann jedoch dabei weiter verwendet werden, wobei er am Anfang etwas langsam sein kann. Wenn Bitlocker dir ein weiteres Festplattenlaufwerk zum Verschlüsseln anbietet, dann verschlüssele auch das.

## Siehe auch

VeraCrypt ist eine Alternative zum Verschlüsseln von Windows. Der Vorteil ist, dass keine Pro-Lizenz von Windows nötig ist. Leider birgt die Verschlüsselung bei VeraCrypt das Risiko, dass durch das Verschlüsseln der Rechner unwiederbringlich unbenutzbar wird. Daher ist es wichtig, vor dem Verschlüsseln des Rechners ein Backup zu machen.

# wichtiger Hinweis: Recovery Key im Microsoft Account

Es gibt einen Recovery Key, mit dem die Festplatte entschlüsselt werden kann. Den brauchst du, wenn dein Laptop kault ist, du die Festplatte ausbauen möchtest und an einen anderen Rechner anschließt/einbaust und von da auf deine Daten zugreifen möchtest. Dieser Recovery/Wiederherstellungs-Key ist bei vielen im Microsoft Account gespeichert. Wenn ihr den Laptop verschlüsselt werdet ihr danach gefragt, wo ihr den Recovery-Key speichern wollt. Eine Option ist "in der Microsoft Cloud". Wir empfehlen, den Key auszudrucken und an einem Sicheren Ort zu verwahren (Freunde/Familie, auf jeden Fall außerhalb der Wohnung).

Falls die Polizei euren Rechner beschlagnahmt und die Festplatte verschlüsselt ist, kann die Polizei nicht auf die Daten zugreifen. Theoretisch kann sie aber bei Microsoft fragen, ob ihr den Recovery Key bei ihnen gespeichert habt (wir wissen nicht, ob das passiert).

Dementsprechend empfehlen wir, zu schauen, ob ihr den bei Microsoft gespeichert habt. Wenn ja, dort bitte löschen. Hier gibt's zwei Anleitungen, um den den Recovery Key im Microsoft Account zu löschen (bislang ungetestet, gerne Rückmeldung geben):

1. [How to find your BitLocker recovery key](#) -> im Video ist ein löschen/delete Button zu sehen
2. Ansonsten ist der Key wohl auch im OneDrive zu finden, siehe dazu:
  - <https://www.thewindowsclub.com/delete-bitlocker-recovery-key-from-onedrive-in-windows-10>

Prozessvorschlag für die Verschlüsselung ist demnach:

- beim Verschlüsseln neuer Systeme mit Bitlocker: den Recovery Key nicht im Microsoft Account speichern, sondern ausdrucken/aufschreiben und nicht-LG-Menschen geben
- wenn Menschen schon verschlüsselte Windows-Rechner haben: checken, ob der Recovery Key im Microsoft Account hinterlegt ist; wenn ja: löschen

---

Version #1

Erstellt: 5 Juli 2025 15:15:38 von RAZ Migration Bot

Zuletzt aktualisiert: 5 Juli 2025 15:15:38 von RAZ Migration Bot