

# Datenschutz

afm Anleitung zur Verschlüsselung  
mobiler Datenträger/Endgeräte

Stand 03-2019

Liebe Kolleginnen und Kollegen,

der Umgang mit den Daten von Interessenten und Kunden ist Bestandteil des täglichen Geschäftsprozesses. Dabei werden sensible Daten immer intensiver verarbeitet.

Eine geeignete Sicherheit zum Schutz vertraulicher Daten wie zum Beispiel personenbezogene Informationen ist zwingend erforderlich. Dadurch werden die Daten im Rahmen der Zugriffskontrolle auch im Falle eines Angriffs oder Datenlecks geschützt.

Die afm Richtlinien zum Datenschutz beschreiben besondere Sicherungsmaßnahmen und Verhaltensweisen auch zum Umgang mit sensiblen Daten auf Datenträgern bzw. Endgeräten.

Wir möchten Ihnen zusätzlich mit dieser Anleitung Wege der Datenverschlüsselung aufzeigen, mithilfe derer Sie eine Zugriffskontrolle für Unternehmensdaten auf Ihren mobilen Datenträgern einrichten könnten.

Die mit der Verschlüsselung erfüllte Anforderung an den Datenschutz ist von jedem Berater und Mitarbeiter unseres Unternehmens in den aufgeführten Ansätzen oder adäquaten Lösungen umzusetzen.

Die Geschäftsleitung

### **Ansprechpartner IT-Administration**

Heiko Hallmann  
Kaiser-Wilhelm-Str. 9  
20355 Hamburg  
Tel. 040 532886-132  
hallmann@afm-gruppe.de

Stephan Tomfohrde  
Kaiser-Wilhelm-Str. 9  
20355 Hamburg  
Tel. 040 532886-136  
tomfohrde@afm-gruppe.de

Mail-Postfach der IT-Abteilung:

**hotline@afm-gruppe.de**

## **Inhalt**

- 1. Verschlüsselung von Laptops**
- 2. Verschlüsselung von USB-Sticks**

# 1. Verschlüsselung von Laptops

Damit ein Fremder die Daten auf Ihrem Notebook bei Verlust oder Diebstahl nicht lesen kann, helfen weder Anmeldekennwort noch Zugriffsrechte – notfalls startet er von einem USB-Stick einfach ein anderes Betriebssystem, das sich um die Windows Zugriffsrechte nicht kümmert.

Das einzige, was wirklich hilft, ist das Verschlüsseln der Daten, und zwar am besten vollständig, sprich das komplette Laufwerk. Dazu dient unter Windows die bordeigene Laufwerksverschlüsselung BitLocker.

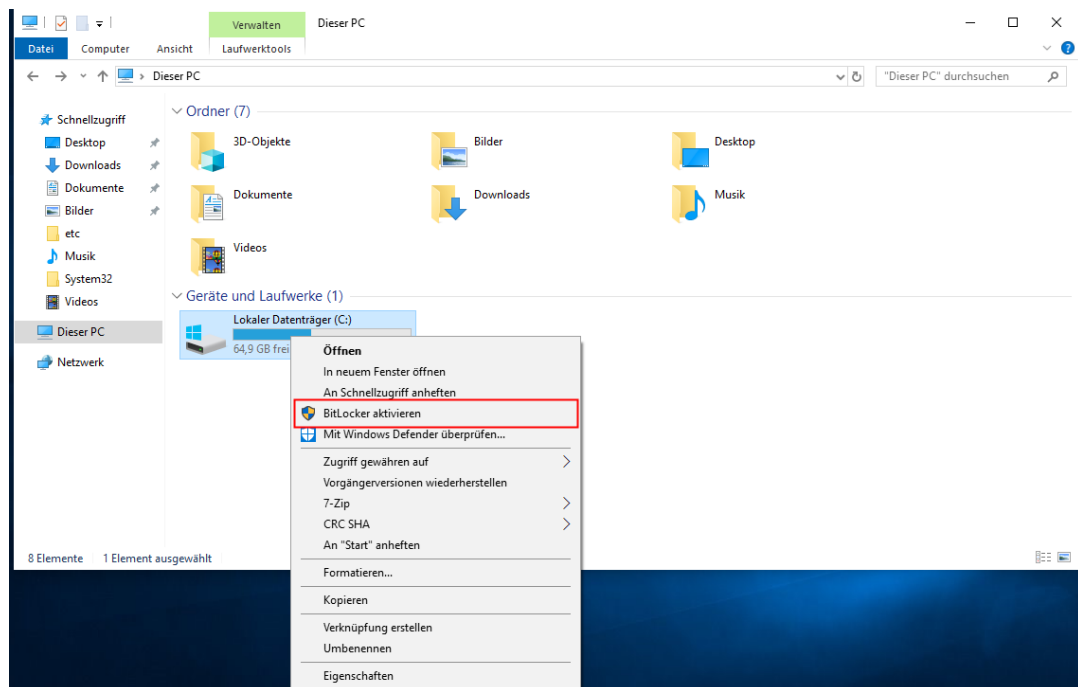
Um BitLocker auf Ihrem Notebook mit **Windows 10 Pro** zu aktivieren, gehen Sie bitte folgendermaßen vor:

- 1.1. Laden Sie sich auf ihrem Laptop die BitLocker-Konfiguration von dieser Seite herunter

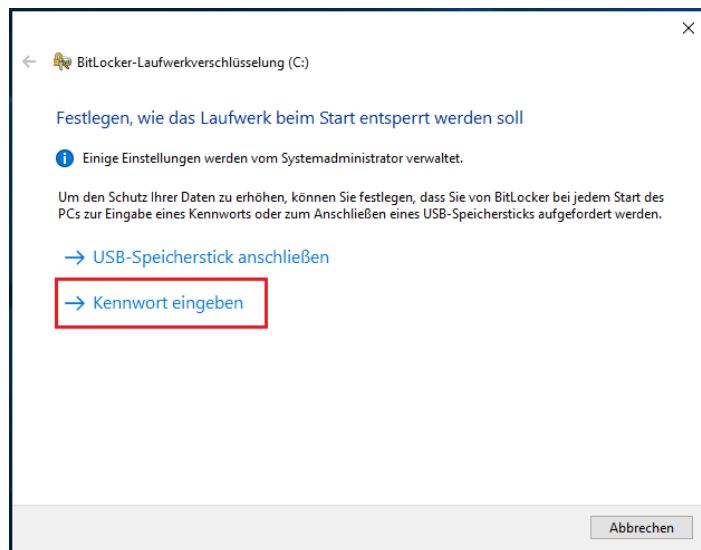
<http://ts.afm-update.de>

Hierdurch werden alle notwendigen Einstellungen für die Bitlocker-Verschlüsselung Ihres Notebooks automatisch vorgenommen

- 1.2. Nachdem Sie die Datei ausgeführt haben, startet Ihr Notebook einmal neu
- 1.3. Im Anschluss an den Neustart öffnen Sie den Datei-Explorer mit der Ansicht „Dieser PC“ (eine direkte Verknüpfung zu „Dieser PC“ ist auf den meisten Desktops zu finden) und führen Sie einen Rechtsklick auf Ihr Laufwerk C: aus
- 1.4. Wählen Sie „BitLocker aktivieren“ aus



- 1.5. Im darauffolgenden Fenster klicken Sie auf „Kennwort eingeben“ um den PC mit Hilfe eines Kennworts zu ver-/entschlüsseln



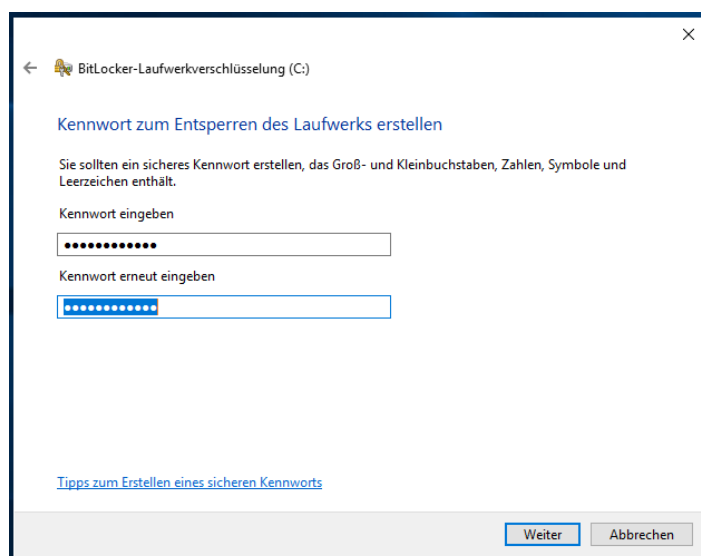
- 1.6. Überlegen Sie sich nun ein sicheres Kennwort zur Verwendung von BitLocker

### **Achtung!**

Bitte verwenden Sie in Ihrem Kennwort keine Umlaute, kein y, kein z, kein ß und lediglich diese **Sonderzeichen**: ! , . \$ %

Auch Zahlen sind problemlos möglich.

Grund hierfür ist, dass viele Notebooks beim Start stets von einer englischen Tastaturbelegung ausgehen und sich diese vom deutschen Tastaturlayout unterscheidet, sodass Sie Ihr BitLocker-Kennwort unwissentlich falsch eingeben könnten.



- 1.7. Im nächsten Schritt müssen Sie angeben wo Sie Ihren Wiederherstellungsschlüssel speichern wollen

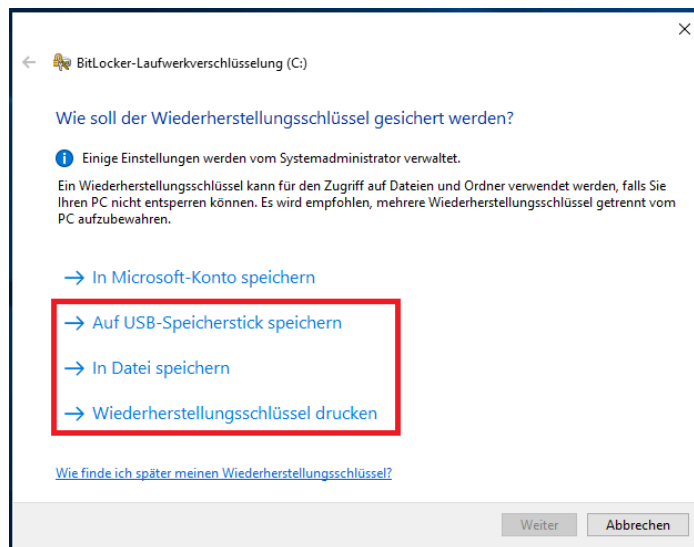
Mit diesem Schlüssel können Ihre Daten doch noch entschlüsselt werden, sollten Sie Ihr zuvor vergebenes Kennwort vergessen haben.

**Entsprechend wichtig ist dieser Schlüssel!**

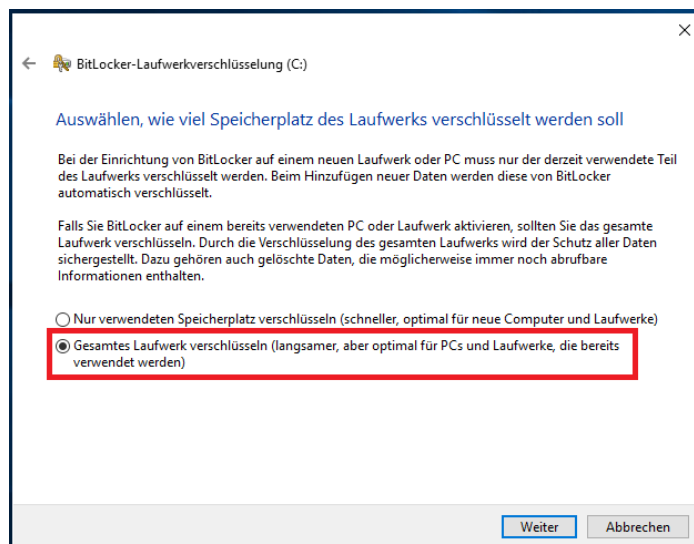
Drucken Sie ihn am besten aus und lagern den Ausdruck an einem räumlich getrennten Ort, notfalls als PDF über den Drucker „Microsoft Print to PDF“.

Alternativ speichern Sie ihn auf einem separaten USB-Stick und verwahren den USB-Stick an einen sicheren, räumlich getrennten Ort!

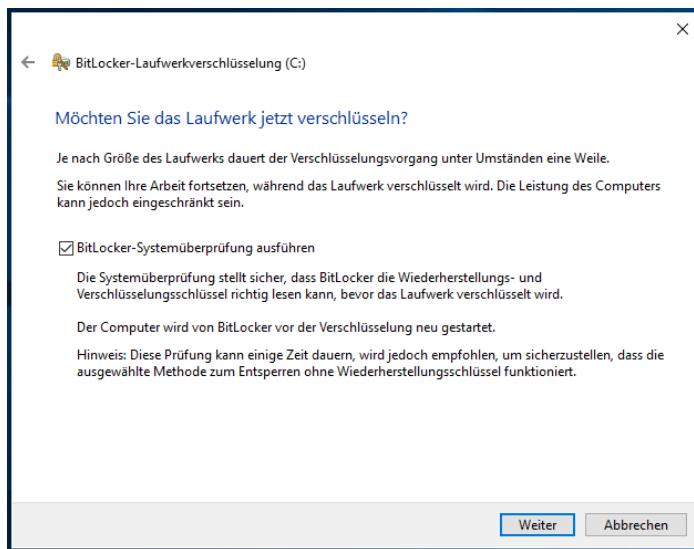
**Ohne diesen Wiederherstellungsschlüssel kann niemand Ihre Daten wiederherstellen!**



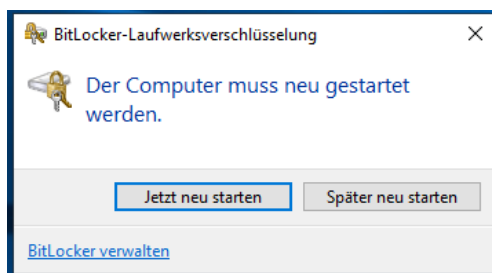
- 1.8. Wählen Sie im nächsten Schritt aus, dass das gesamte Laufwerk verschlüsselt werden soll



1.9. Den letzten Schritt können Sie einfach mit „Weiter“ bestätigen



1.10. Nach einem Neustart des Notebooks wird die Bitlocker-Verschlüsselung gestartet



Die schlussendliche Verschlüsselung des Laufwerks kann je nach Notebook-Performance mehrere Stunden dauern. Dies geschieht allerdings im Hintergrund und Sie können das Notebook normal weiternutzen.

Von nun an werden Sie beim Start Ihres Notebooks stets aufgefordert das zuvor vergebene Kennwort zum Entschlüsseln des PCs einzugeben.

## 2. Verschlüsselung von USB-Sticks

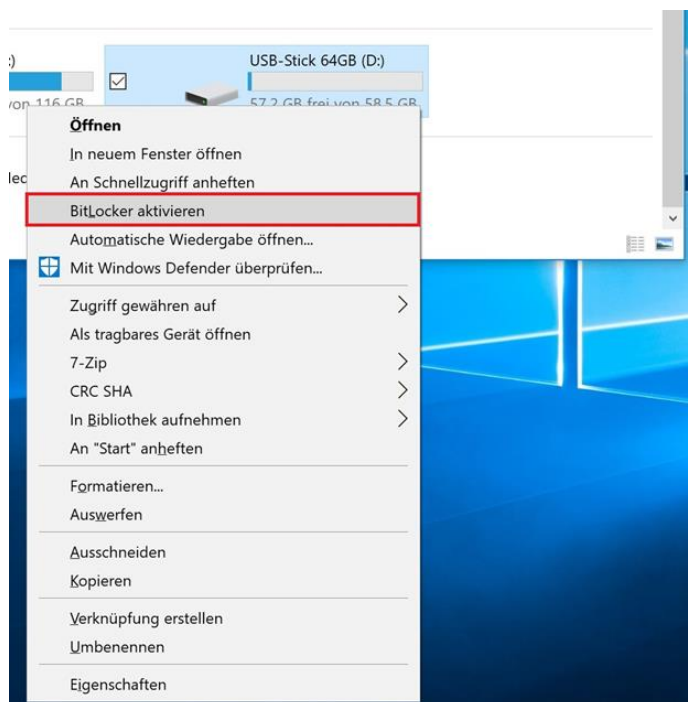
Um mit Hilfe von BitLocker Ihren USB-Stick zu verschlüsseln, gehen Sie bitte folgendermaßen vor:

- 2.1. Sofern noch nicht geschehen, laden Sie sich auf ihrem Laptop die BitLocker-Konfiguration von dieser Seite herunter

<http://ts.afm-update.de>

Hierdurch werden alle notwendigen Einstellungen für die BitLocker-Verschlüsselung Ihres Notebooks automatisch vorgenommen

- 2.2. Nachdem Sie die Datei ausgeführt haben, startet Ihr Notebook einmal neu
- 2.3. Im Anschluss an den Neustart öffnen Sie den Datei-Explorer mit der Ansicht „Dieser PC“ (eine direkte Verknüpfung zu „Dieser PC“ ist auf den meisten Desktops zu finden) und führen Sie einen Rechtsklick auf Ihren USB-Stick aus
- 2.4. Wählen Sie „BitLocker aktivieren“ aus



- 2.5. Im darauffolgenden Fenster vergeben Sie ein Kennwort zum Ver-/Entschlüsseln des USB-Sticks

The screenshot shows the BitLocker 'Choose a method to unlock the drive' window. The title bar reads 'BitLocker-Laufwerkverschlüsselung (D:)'. The main heading is 'Methode zum Entsperren des Laufwerks auswählen'. There are two options: 'Kennwort zum Entsperren des Laufwerks verwenden' (selected with a checkbox) and 'Smartcard zum Entsperren des Laufwerks verwenden' (unchecked). The selected option includes a note: 'Kennwörter sollten Groß- und Kleinbuchstaben, Zahlen, Leerzeichen und Symbole enthalten.' Below this are two password input fields labeled 'Kennwort eingeben' and 'Kennwort erneut eingeben', both showing masked characters. The 'Smartcard' option includes a note: 'Sie müssen Ihre Smartcard einstecken. Die Smartcard-PIN ist erforderlich, wenn Sie das Laufwerk entsperren.' At the bottom right are 'Weiter' and 'Abbrechen' buttons.

- 2.6. Im nächsten Schritt müssen Sie angeben wo Sie Ihren Wiederherstellungsschlüssel speichern wollen

Mit diesem Schlüssel können Ihre Daten doch noch entschlüsselt werden, sollten Sie Ihr zuvor vergebenes Kennwort vergessen haben.

**Entsprechend wichtig ist dieser Schlüssel!**

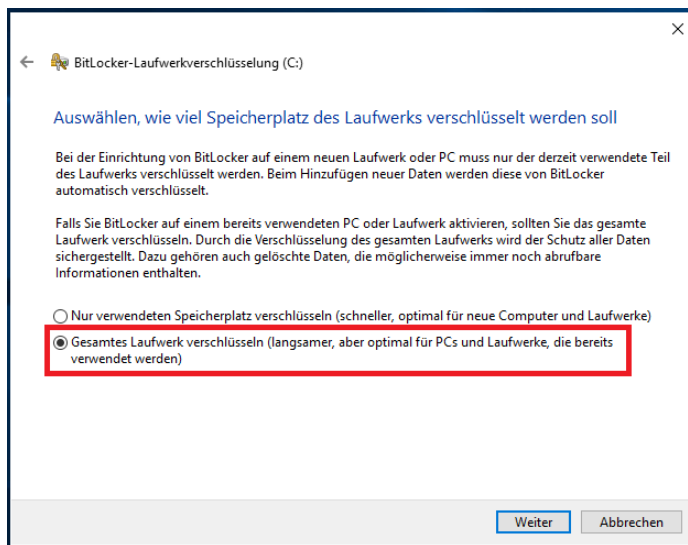
Drucken Sie ihn am besten aus und lagern den Ausdruck an einem räumlich getrennten Ort, notfalls als PDF über den Drucker „Microsoft Print to PDF“.

Alternativ speichern Sie ihn auf einem separaten USB-Stick und verwahren den USB-Stick an einen sicheren, räumlich getrennten Ort!

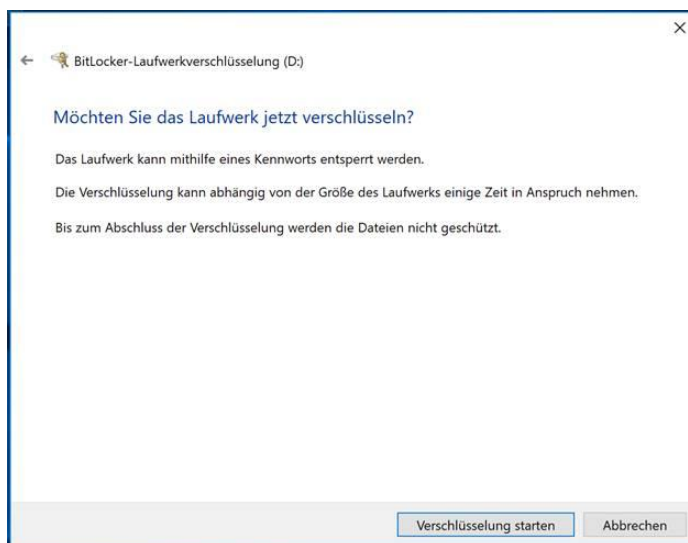
**Ohne diesen Wiederherstellungsschlüssel kann niemand Ihre Daten wiederherstellen!**

The screenshot shows the BitLocker 'How should the recovery key be secured?' window. The title bar reads 'BitLocker-Laufwerkverschlüsselung (D:)'. The main heading is 'Wie soll der Wiederherstellungsschlüssel gesichert werden?'. There is a note: 'Einige Einstellungen werden vom Systemadministrator verwaltet.' Below this is a paragraph: 'Wenn Sie das Kennwort vergessen oder die Smartcard verlieren, können Sie mithilfe eines Wiederherstellungsschlüssels auf das Laufwerk zugreifen.' There are three options with arrows: 'In Microsoft-Konto speichern', 'In Datei speichern' (highlighted with a red rectangle), and 'Wiederherstellungsschlüssel drucken'. At the bottom left is a link: 'Wie finde ich später meinen Wiederherstellungsschlüssel?'. At the bottom right are 'Weiter' and 'Abbrechen' buttons.

2.7. Wählen Sie im nächsten Schritt aus, dass das gesamte Laufwerk verschlüsselt werden soll



2.8. Den letzten Schritt können Sie einfach mit „Verschlüsselung starten“ bestätigen



Die Verschlüsselung des USB-Sticks kann je nach Speicherplatz und Performance einige Zeit in Anspruch nehmen.

Von nun an werden Sie, sobald Sie den USB-Stick an einen Rechner anschließen, aufgefordert das Kennwort zum Entsperren des USB-Sticks einzugeben.