Datenverlust vermeiden: So beherrschen Sie die automatische Windows-Verschlüsselung

Liebe Kundin, lieber Kunde,

im Sinne unseres Service-Gedankens bei Euronics Jakob ist es unser Anspruch, Ihnen proaktiv zur Seite zu stehen. Wir möchten Sie über wichtige technische Themen aufklären noch bevor sie zu einem Problem werden können, anstatt erst zu reagieren, wenn es vielleicht schon zu spät ist. Ihre Datensicherheit liegt uns sehr am Herzen und eine aktuelle Änderung von Microsoft bei Windows 11 könnte direkten Einfluss darauf haben.

Microsoft hat damit begonnen eine leistungsstarke Sicherheitsfunktion – die Geräteverschlüsselung – automatisch zu aktivieren. Das ist einerseits ein großer Gewinn für den Schutz Ihrer Daten bei Diebstahl, birgt aber andererseits auch ein oft übersehenes Risiko: den unwiederbringlichen Verlust Ihrer Daten bei einem technischen Defekt, wenn die nötige Vorbereitung nicht stattgefunden hat.

Damit Sie sicher und informiert bleiben, erklären wir Ihnen in diesem Service-Artikel einfach und verständlich, was diese Funktion macht, wo die Gefahr liegt und wie Sie sich optimal schützen können.

Was die Geräteverschlüsselung genau macht:

Stellen Sie sich die Festplatte Ihres Computers als einen fest eingebauten Safe vor. In diesem Safe liegen alle Ihre Daten – Dokumente, Bilder, Programme. Die Windows 11 Geräteverschlüsselung ist ein automatischer Schließmechanismus für diesen Datensafe. Sie nimmt jede einzelne Datei und verschlüsselt sie mit einem einzigartigen Code, wodurch die Daten in ein unlesbares Format umgewandelt werden. Das passiert permanent im Hintergrund, ohne dass Sie etwas davon merken.

Wenn Sie Ihren Computer hochfahren, wird dieser Safe **automatisch** vom **TPM-Sicherheitschip** aufgeschlossen. Sie können Ihren PC also wie gewohnt nutzen, aber mit dem Wissen, dass Ihre Daten geschützt sind.

Was ist der große Vorteil:

Der entscheidende Vorteil zeigt sich bei **Diebstahl oder Verlust**. Ein Dieb könnte die Festplatte ausbauen und an einen anderen PC anschließen – er würde aber nur unlesbaren Datenmüll sehen. Ohne die originale Hardware-Kombination Ihres Geräts ist es praktisch unmöglich die Daten zu entschlüsseln. Ihr digitales Leben bleibt privat, auch wenn die Hardware weg ist.

Was ist die große Gefahr:

Die größte Gefahr ist nicht, dass ein Fremder die Verschlüsselung knackt, sondern dass **Sie sich selbst unwiederbringlich aussperren**. Es gibt keine Hintertür. Wenn Sie durch ein

technisches Problem auf den Wiederherstellungsschlüssel angewiesen sind und diesen nicht zur Hand haben, sind Ihre Daten **für immer verloren**. Nicht einmal ein IT-Profi kann Ihnen dann noch helfen. Die Technologie, die Ihre Daten vor Dieben schützt, wird in diesem Moment zu einer unüberwindbaren Mauer.

Die enge Kopplung an den TPM-Sicherheitschip ist ein zweischneidiges Schwert. Einerseits bietet sie maximalen Schutz, andererseits kann **ein Defekt am Mainboard, ein fehlerhaftes System-Update oder ein Hardwaretausch** dazu führen, dass das System den Zugriff sperrt. In all diesen Fällen gilt: Ohne den Wiederherstellungsschlüssel sind Ihre Daten unwiderruflich unzugänglich.

Was bedeutet das für mich?

Mit dem Update auf Windows 11 Version 24H2 / 25H2 hat Microsoft diese Geräteverschlüsselung bei vielen Geräten **standardmäßig aktiviert**. Ihr System ist also möglicherweise jetzt sicherer als zuvor, birgt aber auch das Risiko, sich auszusperren. Sie stehen daher vor einer wichtigen Entscheidung und haben zwei sinnvolle Möglichkeiten:

- **Option 1: Sie deaktivieren diese zusätzliche Sicherheitsmaßnahme.** Damit umgehen Sie die Gefahr, sich im Fehlerfall selbst auszusperren. Der Preis dafür ist jedoch ein geringerer Schutz bei Diebstahl. Dies ist der Weg des geringsten Risikos in Bezug auf Datenverlust durch einen Systemfehler.
- **Option 2: Sie stellen den sicheren Betrieb aktiv sicher.** Sie behalten den hohen Sicherheitsstandard bei und sorgen selbst für den Notfallzugang. Das bedeutet, Sie überprüfen, ob die Verschlüsselung eingeschaltet ist und – ganz entscheidend – stellen sicher, dass der Wiederherstellungsschlüssel in Ihrem Microsoft-Konto hinterlegt ist. Es ist wichtig, dass Sie auf dieses Konto zugreifen können **und idealerweise den Schlüssel zusätzlich ausdrucken oder an einem zweiten, sicheren Ort speichern.** Dies ist der Weg des maximalen Schutzes.

Wir lassen Sie nicht allein – so unterstützen wir Sie:

Die Sicherheit Ihrer Daten liegt uns am Herzen. Da diese automatische Aktivierung für viele neu ist, möchten wir Sie bestmöglich unterstützen.

Damit Sie einfach und schnell überprüfen können, ob Ihr Gerät verschlüsselt ist und Ihr Wiederherstellungsschlüssel sicher hinterlegt wurde, haben wir für Sie eine **bebilderte Schritt-für-Schritt-Anleitung** erstellt.

Sollten Sie sich dabei unsicher fühlen oder technische Unterstützung bevorzugen, sind wir selbstverständlich auch persönlich für Sie da. Vereinbaren Sie einfach unter der Telefonnummer **09101 / 8672** oder unter info@euronics-jakob.de einen Termin mit einem unserer Techniker, der alles für Sie überprüft und die für Sie passende Konfiguration sicherstellt.

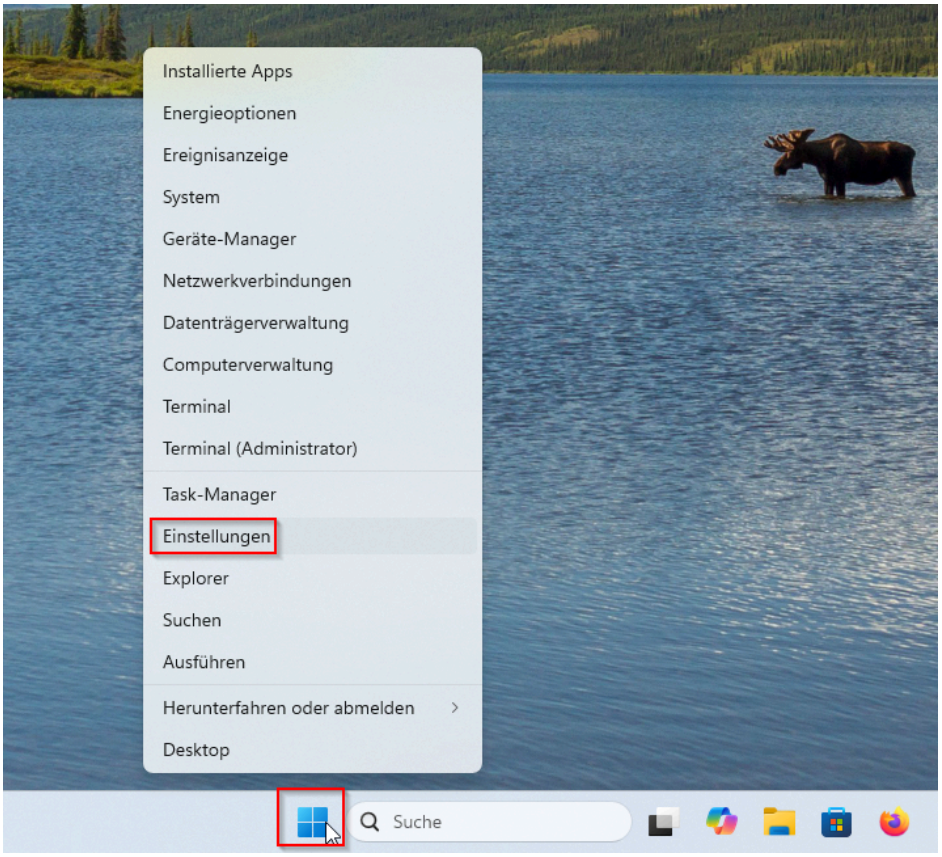
Schritt für Schritt zum Ziel:

Bitlocker prüfen, entscheiden und ggf. deaktivieren

Schritt 1.1: Die Einstellungen öffnen:

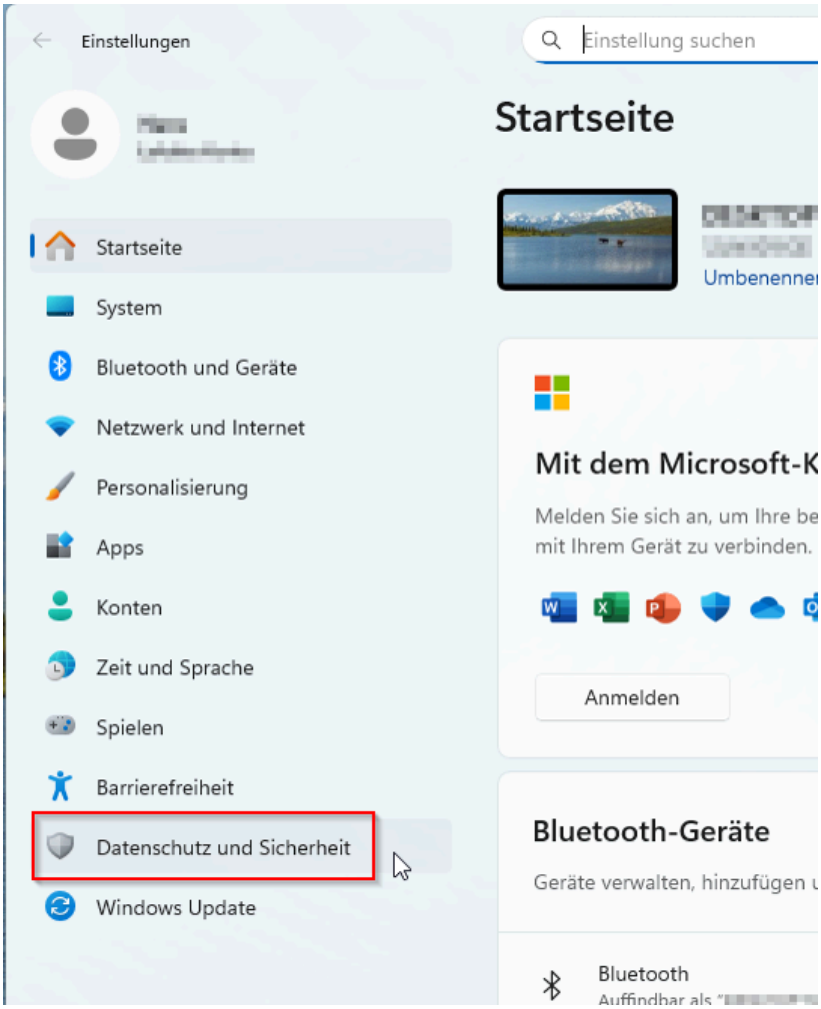
Klicken Sie bitte mit der **rechten Maustaste** auf das **blaue Windows-Symbol** (den Start-Knopf) in der Taskleiste, ganz unten auf Ihrem Bildschirm.

Es öffnet sich ein Menü. Wählen Sie dort bitte den Punkt **"Einstellungen"** aus, so wie im Bild rot markiert.



Schritt 2.2: Den Bereich "Datenschutz und Sicherheit" auswählen:
Nachdem sich das Einstellungsfenster geöffnet hat, sehen Sie auf der linken Seite eine Liste mit verschiedenen Bereichen.

Klicken Sie dort bitte auf **"Datenschutz und Sicherheit"**, erkennbar am Schild-Symbol, so wie im Bild rot markiert.

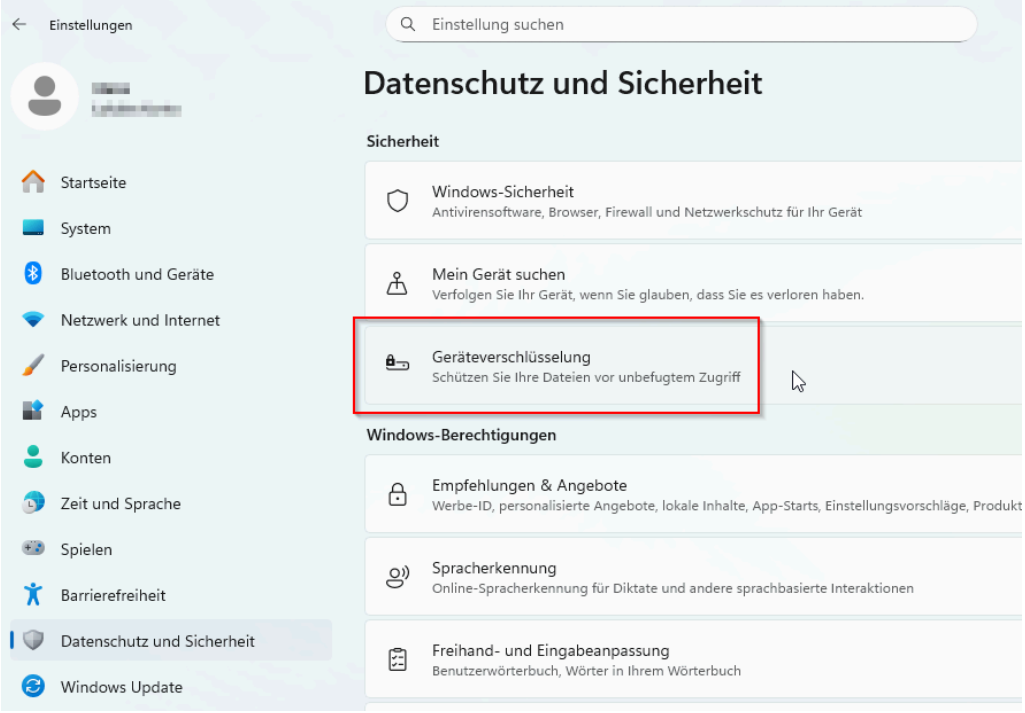


Schritt 1.3: Die Einstellungen zur Geräteverschlüsselung öffnen

Im Hauptfenster sehen Sie nun die Optionen für "Datenschutz und Sicherheit". Suchen Sie bitte unter der Zwischenüberschrift **Sicherheit** den Menüpunkt **"Geräteverschlüsselung"** , so wie im Bild rot markiert.

Klicken Sie auf diesen Punkt, um zu den Details der Verschlüsselung zu gelangen.

Wichtiger Hinweis: Falls dieser Menüpunkt bei Ihnen nicht vorhanden ist, unterstützt Ihr Gerät diese spezielle Art der Verschlüsselung möglicherweise nicht oder es sind noch nicht alle erforderlichen Windows-Updates installiert.



Schritt 1.4: Status prüfen und die richtige Entscheidung treffen

Hier sind Sie nun im Menü "Geräteverschlüsselung". Ihr Bildschirm wird jetzt einer der folgenden drei Situationen ähneln. Finden Sie heraus, welcher Fall bei Ihnen zutrifft, und lesen Sie die entsprechende Handlungsempfehlung.

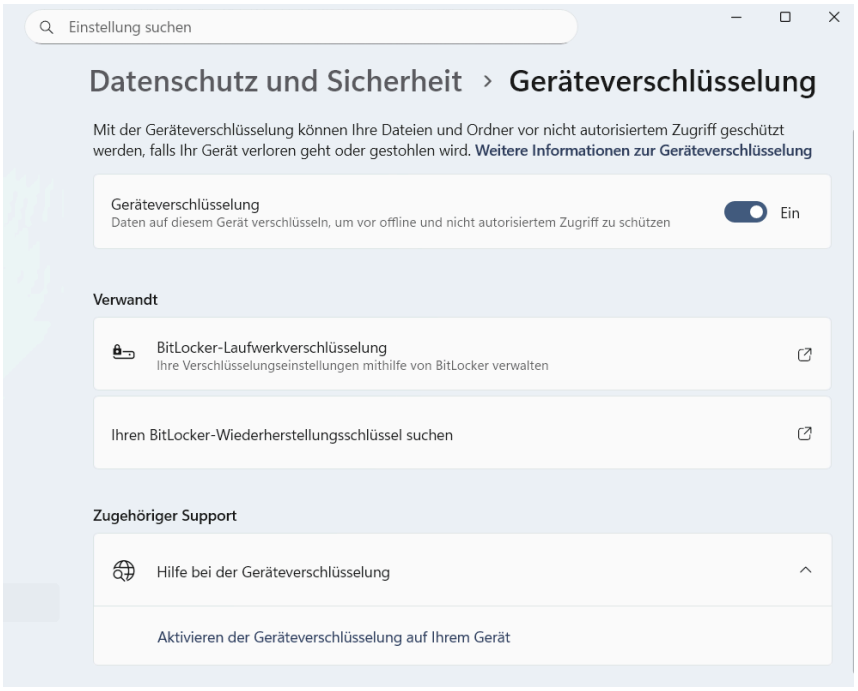
Fall 1: Der Schalter steht auf "Aus"



Das bedeutet: Ihre Geräteverschlüsselung ist **ausgeschaltet**. Ihre Daten sind nicht verschlüsselt. Sie sind damit zwar nicht vor Diebstahl geschützt, können sich aber auch nicht versehentlich aussperren.

- **Option 1 (So belassen):** Wenn Sie diese Funktion nicht nutzen möchten, sind Sie an diesem Punkt fertig und müssen nichts weiter tun.
- **Option 2 (Aktivieren):** Wenn Sie den Schutz nutzen möchten, legen Sie den Schalter auf "Ein". Ihr Computer wird Sie dann auffordern, sich mit einem Microsoft-Konto zu verbinden, um den Schlüssel zu sichern. **Folgen Sie dazu einfach der Anleitung weiter ab Option 2. BitLocker / Geräteverschlüsselung Aktivieren und Prüfen**

Fall 2: Der Schalter steht auf "Ein" (Alles in Ordnung)



Das bedeutet: Der Schalter steht auf **Ein** und es wird **keine** gelbe Warnmeldung angezeigt. Herzlichen Glückwunsch, Ihre Verschlüsselung ist **vollständig und fehlerfrei aktiviert**. Ihre Daten sind geschützt.

- **Option 1 (Deaktivieren):** Falls Sie die Funktion (trotz korrekter Einrichtung) nicht nutzen möchten, um jedes Risiko des Aussperrens zu umgehen, können Sie den Schalter einfach auf "Aus" stellen. **Folgen Sie dazu einfach der Anleitung weiter (Schritt 5).**
- **Option 2 (Absichern - Dringend empfohlen):** Sie sollten jetzt *unbedingt* prüfen, ob der Schlüssel korrekt in Ihrem Microsoft-Konto gespeichert ist und ihn zusätzlich ausdrucken oder an einem zweiten, sicheren Ort speichern. Springen Sie dazu bitte zum nächsten Abschnitt: **Schritt 2.7: Den Wiederherstellungsschlüssel online prüfen**

Fall 3: Der Schalter steht auf "Ein" (MIT Warnmeldung)



Das bedeutet: Der Schalter steht auf **Ein** (Markierung 1), aber darüber wird eine **gelbe Warnmeldung** angezeigt (Markierung 2).

Dies ist der **gefährlichste Zustand!** Ihre Daten sind zwar verschlüsselt, aber der Wiederherstellungsschlüssel wurde **noch nicht gesichert**. Er existiert aktuell *nur* auf dem TPM-Chip Ihres PCs. Bei einem Defekt oder einer Systemänderung wären Ihre Daten **unwiederbringlich verloren**, da Sie keine Notfall-Kopie des Schlüssels besitzen. **Sie müssen jetzt handeln!**

- **Option 1 (Sofort deaktivieren):** Wenn Sie kein Microsoft-Konto nutzen möchten oder unsicher sind, stellen Sie den Schalter (Markierung 1) auf **"Aus"**. Die Entschlüsselung kann einen Moment dauern, aber danach ist die Gefahr gebannt. **Folgen Sie dazu einfach der Anleitung weiter.**

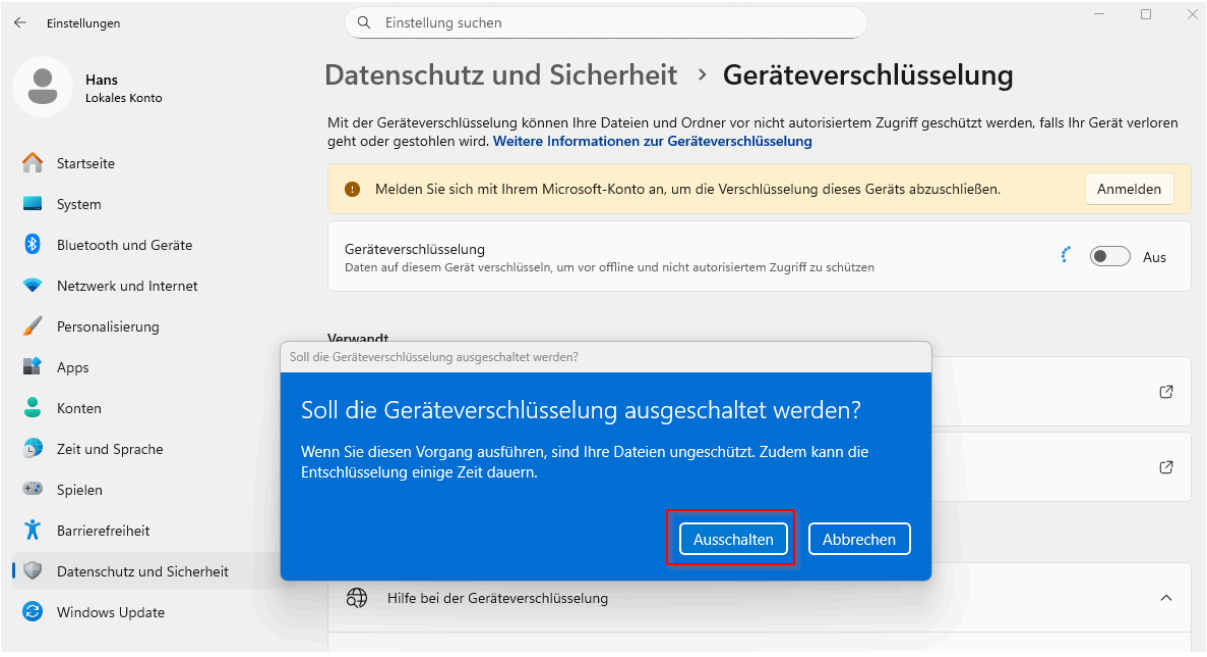
- **Option 2 (Sicherung neu generieren): Folgen Sie einfach der Anleitung weiter**, um die Verschlüsselung neu zu aktivieren und den Schlüssel zu sichern.

Schritt 1.5: Geräteverschlüsselung deaktivieren

Als nächstes wird die Geräteverschlüsselung ausgeschaltet, klicken Sie bitte auf den blauen Schalter, der aktuell noch auf **"Ein"** steht.



Direkt danach erscheint ein blaues Hinweisfenster mit der Frage "Soll die Geräteverschlüsselung ausgeschaltet werden?". Dieses Fenster weist Sie darauf hin, dass die Entschlüsselung einige Zeit dauern kann. Um den Vorgang zu starten, klicken Sie bitte auf **"Ausschalten"** (im Bild rot umrahmt).



Schritt 1.6: Die Entschlüsselung läuft

Nach Ihrer Bestätigung sehen Sie nun eine Meldung mit einem **blauen Ladebalken**. Das bedeutet, dass Ihr Computer jetzt arbeitet und den Schutz von Ihren Dateien entfernt.

Das Wichtigste für Sie: Sie müssen jetzt nicht warten und dem Balken zusehen. Wie die Meldung schon sagt: **Sie können Ihr Gerät ganz normal weiterverwenden.** Sie können arbeiten, im Internet surfen oder spielen, während die Entschlüsselung ungestört im Hintergrund weiterläuft. Bitte schalten Sie den Computer nicht aus. Bitte schließen Sie Ihr Netzteil an und sorgen Sie dafür, dass der Laptop während dieses Vorgangs Strom hat.



Schritt 1.7: Erfolgreich deaktiviert

Sobald der Ladebalken verschwunden ist, sollte Ihr Bildschirm so aussehen wie hier abgebildet. Der Schalter steht nun dauerhaft auf **"Aus"** (im Bild rot umrahmt).



Geschafft! Wenn Sie sich für die Option **"Verschlüsselung deaktivieren" (Option 1)** entschieden haben, ist der Vorgang hiermit erfolgreich abgeschlossen.

Das Risiko, sich selbst auszusperren, ist damit beseitigt. Sie müssen nichts weiter tun und können das Fenster der Einstellungen nun schließen.

Wenn Sie sich für die **Option 2** entschieden haben, die Bitlocker / Geräteverschlüsselung zu aktivieren, machen Sie nun weiter mit der Anleitung.

Option 2. Bitlocker / Geräteverschlüsselung Aktivieren und Prüfen

Wenn Sie sich für **Option 2** entschieden haben, stellen wir nun sicher, dass die Verschlüsselung korrekt eingerichtet ist und Sie im Notfall Zugriff auf Ihren Schlüssel haben.

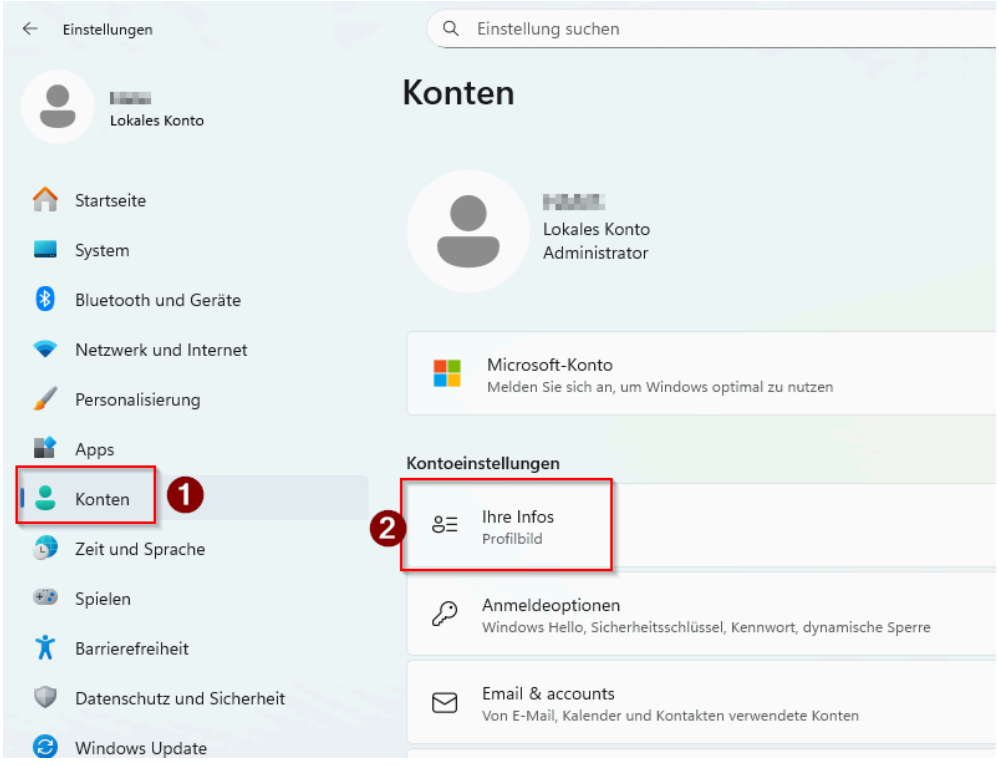
Hinweis: Ein Microsoft-Konto ist nicht zwingend erforderlich. Wir empfehlen diese Variante, da sie die Sicherung des Wiederherstellungsschlüssels deutlich vereinfacht und die weitere Anleitung darauf aufbaut. Bitte entscheiden Sie selbst, ob Sie diesen Weg – auch im Hinblick auf bekannte Datenschutzaspekte – nutzen möchten. Alternativ ist auch eine manuelle Sicherung des Schlüssels möglich.

Schritt 2.1: Den Kontotyp prüfen

Das System der Geräteverschlüsselung und die automatische Sicherung des Notfall-Schlüssels funktionieren am besten und einfachsten in Verbindung mit einem **Microsoft-Konto**. Deshalb prüfen wir zuerst, ob Sie ein solches Konto oder ein lokales Konto verwenden.

Gehen Sie dazu in den Einstellungen bitte wie folgt vor:

1. Klicken Sie auf der linken Seite auf den Menüpunkt **"Konten"** (Markierung 1).
2. Wählen Sie anschließend im rechten Bereich den Punkt **"Ihre Infos"** (Markierung 2).

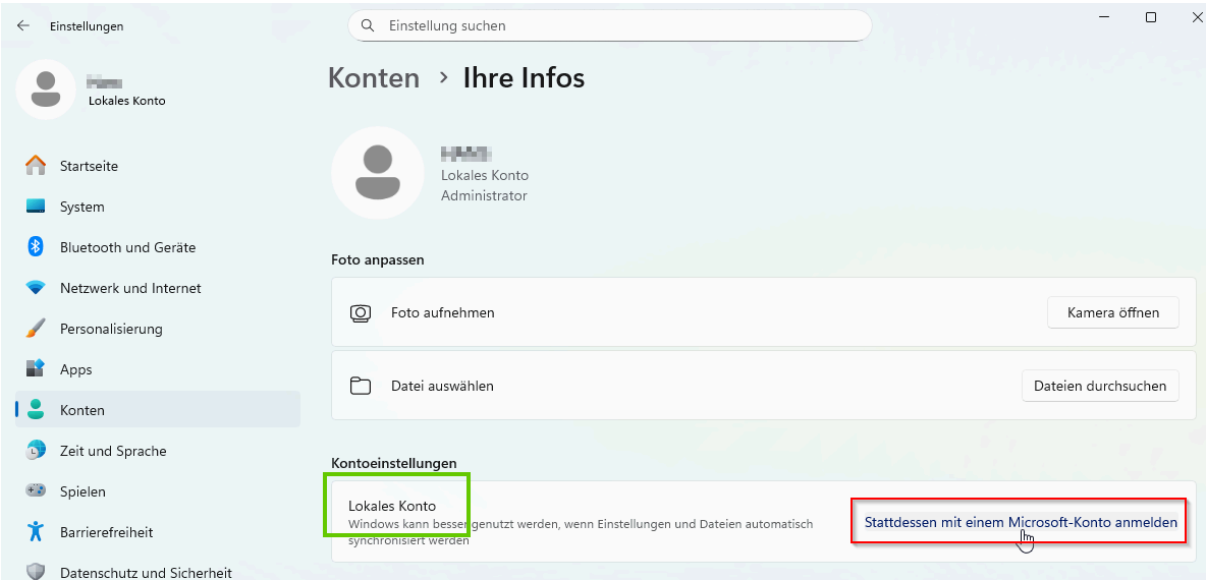


Schritt 2.2: Kontotyp prüfen und gegebenenfalls umstellen

Werfen Sie nun einen Blick auf den Bereich unter "Kontoeinstellungen", den wir im Bild **grün** markiert haben. Hier sehen Sie, wie Ihr Benutzerkonto aktuell eingerichtet ist.

Fall A: Dort steht bereits eine E-Mail-Adresse oder "Microsoft-Konto" Perfekt! Ihr Konto ist bereits optimal eingerichtet. Sie müssen hier nichts ändern. Bitte springen Sie direkt weiter zu **Schritt 4**.

Fall B: Dort steht "Lokales Konto" (wie im Bild zu sehen) Hier besteht Handlungsbedarf. Ein "Lokales Konto" speichert Daten nur auf dem Gerät selbst. Damit Ihr Wiederherstellungsschlüssel im Notfall sicher in der Microsoft-Cloud abgerufen werden kann, müssen wir das Konto verknüpfen. Klicken Sie dazu bitte auf den Link **"Stattdessen mit einem Microsoft-Konto anmelden"** (im Bild rot markiert) und folgen Sie den Anweisungen am Bildschirm.



Was bedeutet diese Umstellung für Sie?

- **Keine Sorge:** Ihre Dateien, Programme und Einstellungen bleiben alle erhalten. Nichts geht verloren.
- **Neue Anmeldung:** Anstatt Ihres alten, lokalen Passworts nutzen Sie künftig die Zugangsdaten Ihres Microsoft-Kontos. Meistens werden Sie dabei aufgefordert, eine **PIN** (einen kurzen Zahlencode) einzurichten. Das macht die tägliche Anmeldung an Ihrem PC für Sie sogar schneller und komfortabler als vorher.
- **Der entscheidende Vorteil:** Nur durch diese Verknüpfung wird der "Generalschlüssel" für Ihre Verschlüsselung automatisch online gesichert, sodass Sie ihn nie verlieren können.

Hinweis: Nach dieser Umstellung melden Sie sich am PC nicht mehr mit Ihrem alten lokalen Passwort an, sondern mit dem Passwort Ihres Microsoft-Kontos oder der neu vergebenen PIN. Schreiben Sie sich diese unbedingt auf!

Schritt 2.3: Anmelden oder neues Konto erstellen

Es hat sich nun ein neues Fenster geöffnet (siehe Bild). Hier haben Sie zwei Möglichkeiten, je nachdem, ob Sie bereits Microsoft-Dienste nutzen oder nicht:

Möglichkeit A: Sie haben bereits ein Konto von Microsoft (z. B. endend auf **@outlook.de**, **@hotmail.com** oder **@live.de**)? Oder nutzen Sie bereits Dienste wie Xbox oder Skype?

- Geben Sie einfach diese E-Mail-Adresse in das Feld ein und klicken Sie auf den blauen Button **"Weiter"**.

Möglichkeit B: Sie haben noch kein Konto Wenn Sie noch keine solche Adresse besitzen, ist das kein Problem. Sie können hier kostenlos eine erstellen.

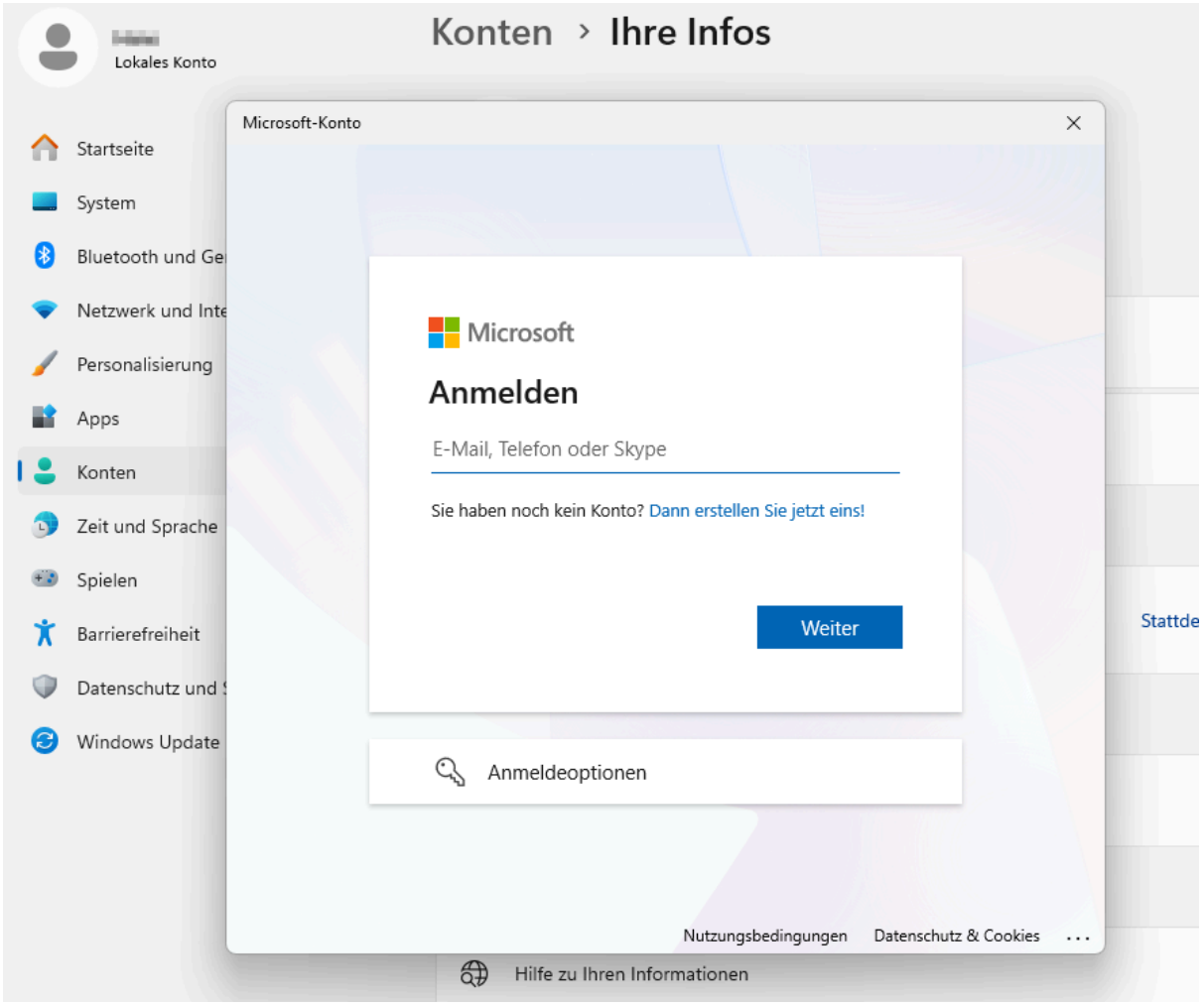
- Klicken Sie dazu auf den blauen Link **"Dann erstellen Sie jetzt eins!"** und folgen Sie den Anweisungen, um sich eine neue Adresse auszusuchen.

Wie geht es nach diesem Fenster weiter? Der Computer führt Sie nun durch ein paar kurze Schritte:

1. Sie müssen das **Passwort** für Ihr Microsoft-Konto eingeben (oder beim Neuerstellen eines festlegen).
2. Aus Sicherheitsgründen müssen Sie meist noch einmal Ihr **altes Computer-Passwort** eingeben, um die Umstellung zu bestätigen.
3. Zum Schluss werden Sie oft gebeten, eine **PIN** (einen kurzen Zahlencode) für Windows Hello zu erstellen. Folgen Sie diesen Anweisungen einfach, bis sich das Fenster schließt.

Ihr altes Passwort wird durch das Microsoft-Passwort oder die neue PIN ersetzt. Bitte merken Sie sich diese neuen Zugangsdaten gut!

Sobald Ihr Konto erfolgreich umgestellt ist und Sie wieder die normalen Einstellungen sehen, finden Sie dort ein "Microsoft-Konto" und kein “Lokales Konto” mehr. Bitte notieren Sie sich die Zugangsdaten (E-Mail / Passwort), sowie den neu vergebenen Computer-Pin. Danach machen wir mit **Schritt 4** weiter.



Schritt 2.4: Die Verschlüsselung wieder aktivieren

Da Ihr Konto nun korrekt eingerichtet ist, können wir die Sicherheitsfunktion wieder einschalten.

1. Klicken Sie im linken Menüband wieder auf **"Datenschutz und Sicherheit"**.
2. Wählen Sie rechts wieder den Punkt **"Geräteverschlüsselung"**.

Sie sehen nun, dass der Schalter aktuell auf **"Aus"** steht (siehe Bild). Klicken Sie diesen Schalter an, um ihn auf **"Ein"** zu stellen.

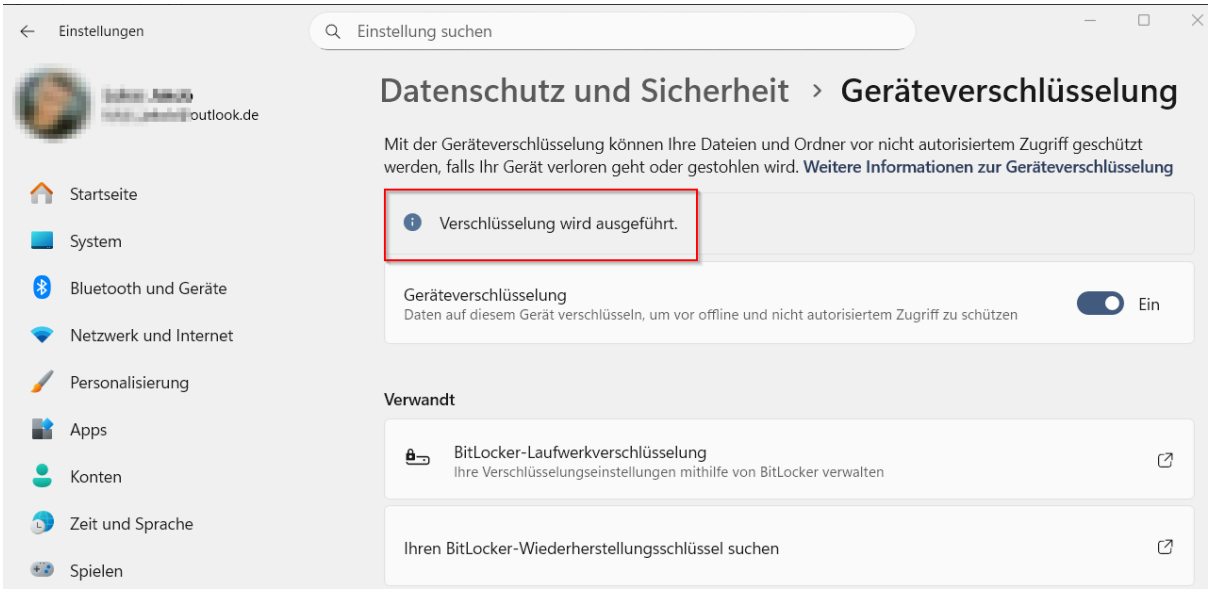
Was jetzt passiert: Ihr Computer beginnt sofort damit, Ihre Festplatte wieder sicher zu verschlüsseln. Das Geniale dabei ist: Da Sie jetzt mit einem Microsoft-Konto angemeldet sind, wird der wichtige Wiederherstellungsschlüssel in diesem Moment **automatisch und sicher** in Ihrem Online-Konto hinterlegt. Sie müssen ihn nicht manuell abtippen.



Schritt 2.5: Die Verschlüsselung läuft

Nach dem Einschalten sehen Sie nun die Meldung **"Verschlüsselung wird ausgeführt"** (im Bild rot markiert).

Das ist ein sehr gutes Zeichen! Es bedeutet, dass Ihr System gerade dabei ist, den "Tresor" zu verschließen und Ihre Daten zu sichern. Wie auch schon beim Ausschalten gilt hier: Dieser Vorgang läuft komplett im Hintergrund. **Sie können Ihren Computer ganz normal weiter benutzen**, arbeiten oder surfen, ohne warten zu müssen. Bitte schalten Sie den Computer nicht aus. Bitte schließen Sie Ihr Netzteil an und sorgen Sie dafür, dass der Laptop während dieses Vorgangs Strom hat.

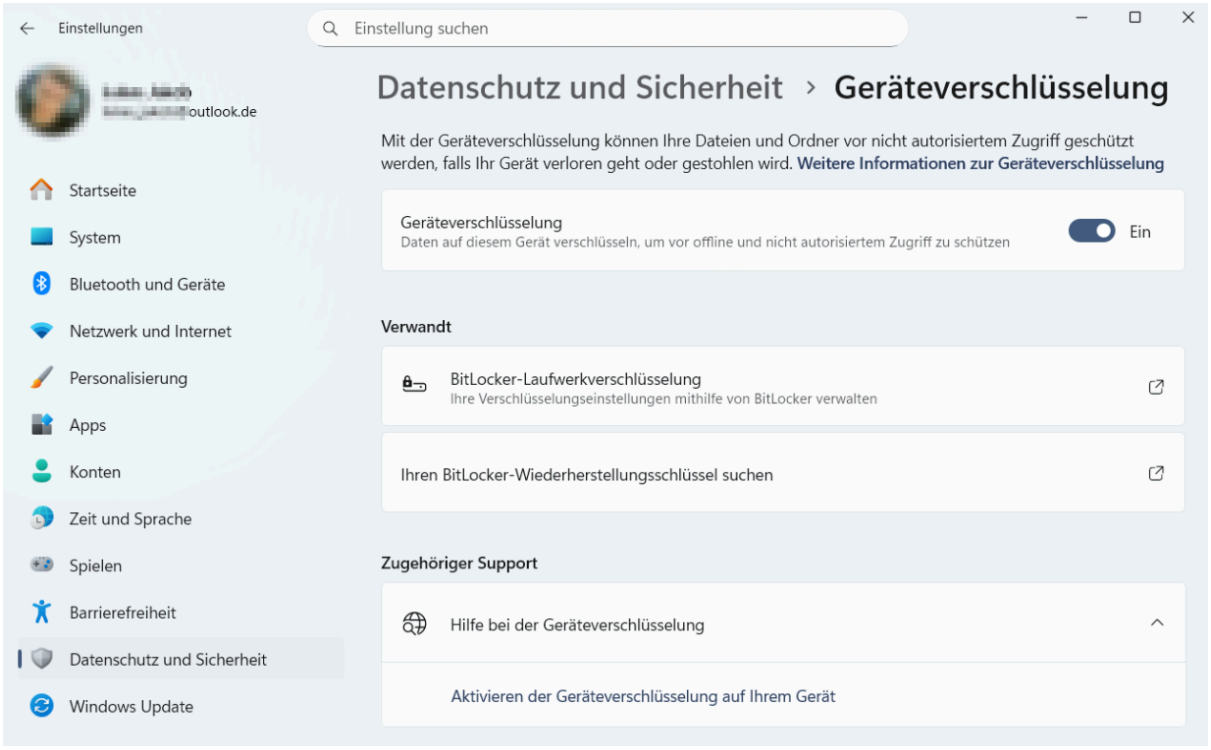


Schritt 2.6: Verschlüsselung aktiv – aber wir müssen noch etwas prüfen

Wenn Ihr Bildschirm nun so aussieht wie auf diesem Bild, ist der eigentliche Vorgang abgeschlossen. Der Schalter steht auf **"Ein"** und es sind keine gelben Warnmeldungen oder Ladebalken mehr zu sehen.

Das bedeutet: Ihr Gerät ist nun vollständig verschlüsselt und bestmöglich gegen Datendiebstahl geschützt.

Wichtig: Lehnen Sie sich bitte noch nicht zurück! Dass die Verschlüsselung "an" ist, reicht nicht aus. Wir müssen jetzt unbedingt sicherstellen, dass Sie im Notfall auch wieder an Ihre Daten kommen. Deshalb prüfen wir im nächsten Abschnitt gemeinsam, ob der passende **Wiederherstellungsschlüssel** auch tatsächlich korrekt in Ihrem Microsoft-Konto angekommen ist.



Schritt 2.7: Den Wiederherstellungsschlüssel online prüfen

Nun verlassen wir kurz die Einstellungen Ihres PCs und gehen ins Internet. Das können Sie direkt am gleichen Computer machen oder – noch besser – **nehmen Sie dafür Ihr Smartphone oder Tablet**. So sehen Sie gleich, dass Sie auch ohne Ihren PC auf den Schlüssel zugreifen können.

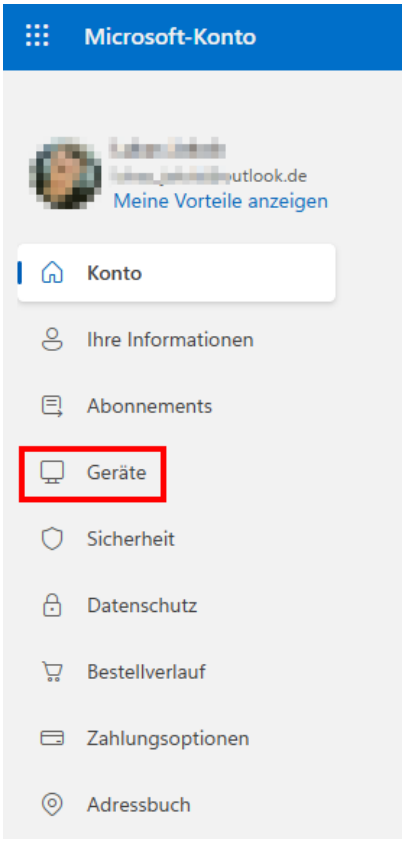
1. Öffnen Sie einen Internet-Browser (z. B. Google Chrome, Microsoft Edge oder Safari auf dem Handy).
2. Geben Sie oben in die Adresszeile folgende Internetadresse ein: https://account.microsoft.com/
3. Klicken Sie auf der Webseite auf **"Anmelden"** und geben Sie dort die E-Mail-Adresse und das Passwort Ihres Microsoft-Kontos ein.

Schritt 2.8: Den Bereich "Geräte" öffnen

Sobald Sie sich erfolgreich angemeldet haben, sehen Sie die Startseite Ihres Microsoft-Kontos.

Suchen Sie im Menü auf der linken Seite (am Handy finden Sie das Menü oft oben links) nach dem Punkt **"Geräte"**. Er ist mit einem kleinen Computer-Symbol gekennzeichnet (im Bild rot umrahmt).

Klicken Sie darauf, um eine Übersicht aller Computer und Laptops anzuzeigen, die mit diesem Konto verknüpft sind.

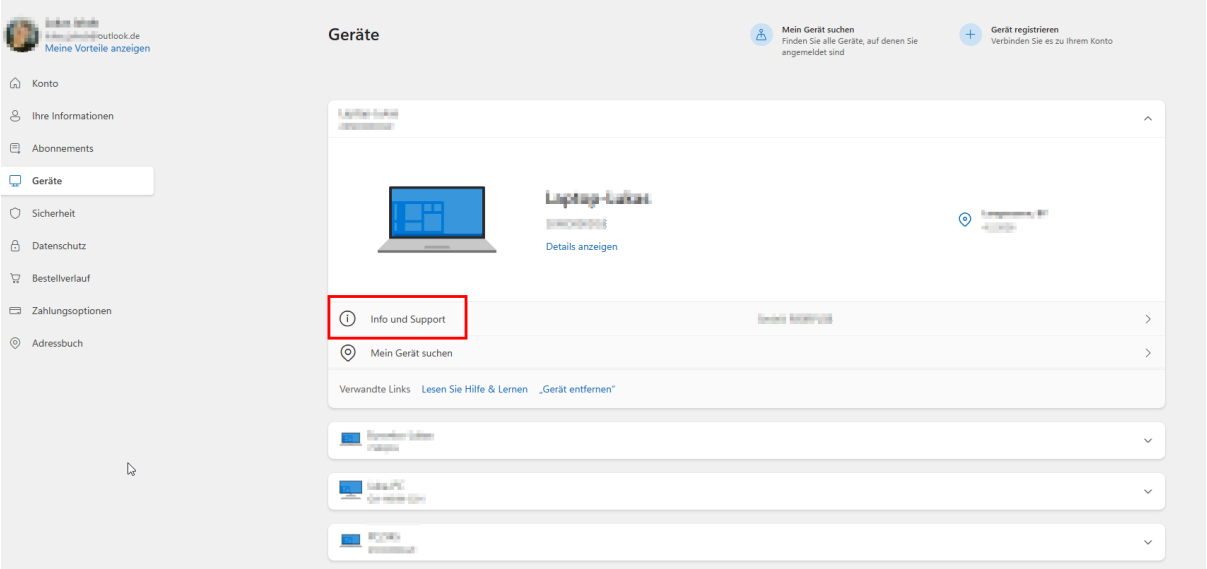


Schritt 2.9: Die Details zum Gerät öffnen

In der Übersicht sehen Sie nun alle Computer, die mit Ihrem Microsoft-Konto bekannt sind.

Suchen Sie in dieser Liste nach dem Gerät, das wir gerade verschlüsselt haben.

- Klicken Sie unter dem Namen des Computers auf die Zeile **"Info und Support"** (im Bild rot umrahmt).

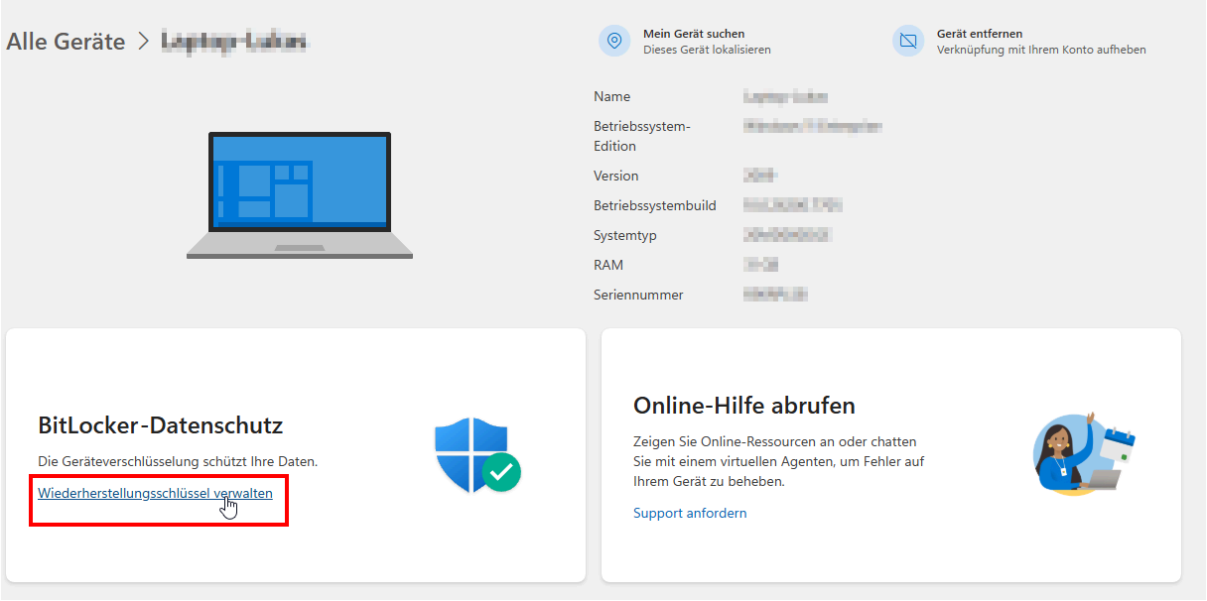


Schritt 2.10: Die Schlüsselverwaltung öffnen

In der Detailansicht Ihres Gerätes finden Sie nun verschiedene Informationen. Scrollen Sie gegebenenfalls ein wenig nach unten, bis Sie den Kasten mit der Überschrift **"BitLocker-Datenschutz"** sehen.

Klicken Sie dort auf den blauen Link **"Wiederherstellungsschlüssel verwalten"** (im Bild rot umrahmt).

Damit öffnen Sie sozusagen den digitalen Tresor, in dem Microsoft Ihren Notfall-Schlüssel für Sie aufbewahrt.



Schritt 11: Den Schlüssel prüfen und sicher aufbewahren

Jetzt sehen Sie das Ziel unserer Reise: Ihren **BitLocker-Wiederherstellungsschlüssel**. Das ist eine sehr lange Zahlenkombination, die wir im Bild rot markiert haben.

Bitte prüfen Sie kurz:

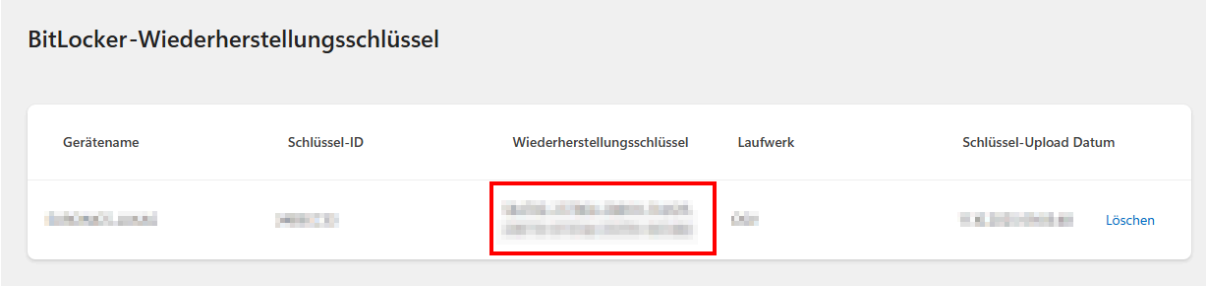
- **Datum:** In der Spalte ganz rechts steht das "Schlüssel-Upload Datum". Wenn wir die Verschlüsselung gerade erst aktiviert haben, sollte hier das heutige Datum stehen.
- **Gerätename:** Stellen Sie sicher, dass links der Name Ihres PCs steht.

Das Wichtigste zum Schluss: Dass der Schlüssel hier steht, ist sehr gut – aber verlassen Sie sich nicht allein darauf. Sollten Sie jemals keinen Zugriff mehr auf Ihr Microsoft-Konto haben, wäre auch der Schlüssel weg.

Unsere dringende Empfehlung: Sichern Sie diesen Schlüssel **außerhalb** Ihres Computers!

1. **Ausdrucken:** Drucken Sie diese Seite aus und heften Sie sie zu Ihren wichtigen Unterlagen.
2. **USB-Stick:** Speichern Sie die Nummer als Textdatei auf einem USB-Stick.

Nur wenn Sie diesen Schlüssel physisch griffbereit haben, sind Sie für jeden technischen Notfall abgesichert.



Hinweis: Der Wiederherstellungsschlüssel ist die lange Zahlenreihe aus 48 Ziffern. Die kurze 'Schlüssel-ID' reicht nicht aus.

Herzlichen Glückwunsch! Sie haben nun erfolgreich überprüft und sichergestellt, dass Ihre Daten nicht nur vor Dieben sicher sind, sondern auch für Sie selbst immer zugänglich bleiben.

Sollten Sie sich dabei unsicher fühlen oder technische Unterstützung bevorzugen, sind wir selbstverständlich auch persönlich für Sie da. Vereinbaren Sie einfach unter der Telefonnummer **09101 / 8672** oder unter info@euronics-jakob.de einen Termin mit einem unserer Techniker, der alles für Sie überprüft und die für Sie passende Konfiguration sicherstellt.