



**erbio**



# Digitaler Nachlass: Hinweise

## Worum geht es beim Digitalen Nachlass und weshalb ist es wichtig?

Digitale Dienste, Apps, Software und Online-Services spielen inzwischen in vielen Lebensbereichen eine Rolle. Dies können harmlose Informationsdienste zu Reisen oder Ernährung sein. Es kann aber auch um sensible Daten gehen, wie private Korrespondenz per E-Mail und Chats in sozialen Medien, kostspielige Abos (auch: Bahn Card) und Zugang zu Bezahldiensten wie Paypal. All dies gehört zu Ihrem digitalen Nachlass.

Den digitalen Nachlass zu regeln ist wichtig, um sicherzustellen, dass Ihre persönlichen und oft sensiblen Informationen auch nach Ihrem Tod richtig behandelt werden. Hier sind einige Gründe, warum Sie dies tun sollten:

1. Daten, Fotos und **digitale Informationen gehören im Todesfall zur Erbmasse**. Diese Daten können für Ihre Erben von emotionalem und praktischen Wert sein und sollen nicht ungewollt verloren gehen.
2. Auch Rechte und Pflichten aus **online geschlossenen Verträgen gehen auf Ihre Erben über**. Die wenigsten Verträge enden automatisch mit dem Tod. Möglicherweise gibt es nicht stornierte Reisebuchungen, bestellte Gegenstände oder laufende Abos. Mit einem geregelten digitalen Nachlass ersparen Sie Ihren Erben viel Arbeit und möglicherweise auch unnötige Kosten.
3. Selbst nach Ihrem Tod können Ihre digitalen Informationen gestohlen und missbraucht werden und der Missbrauch wird womöglich spät oder nie bemerkt. So könnten falsche Nachrichten in Ihrem Namen verschickt und Verträge geschlossen werden. Weiterhin ist auch **die Privatsphäre Ihrer Hinterbliebenen** betroffen, falls zum Beispiel E-Mail-Konten oder private Chats an Fremde gelangen. Durch die Regelung des Digitalen Nachlasses können Sie gezielt bestimmte Dienste schließen lassen oder den Status von zB. einigen sozialen Netzwerken so ändern, dass Missbrauch nicht mehr möglich ist.
4. Der **Zugang zu digitalen Konten ist schwierig**. Ohne E-Mail-Adressen, Passwörter oder Zugang zum Smartphone können Ihre Erben nicht auf Ihre Benutzerkonten zugreifen und Abos kündigen, Daten sichern oder löschen. Zwar sind Anbieter digitaler Dienste verpflichtet, den Erben vollen Zugang

zum Nutzerkonto zu gewähren. Doch es ist zeitraubend, sämtliche Konten aufzuspüren, die von Bedeutung sind. Und selbst wenn die Anbieter bekannt sind, müssen Ihre Erben sich dort zunächst mit dem Erbschein legitimieren, sollten sie die Zugangsdaten nicht kennen. In dieser Zeit laufen die Kosten für nicht gekündigte Dienste weiter.

5. Ihre **Erben wissen womöglich nicht, was Sie sich für Ihre Profile in sozialen Medien gewünscht hätten**. Möchten Sie das Nutzerkonto kommentarlos schließen, eine Information oder gar ein Foto oder Video dort hinterlassen? Facebook bietet zum Beispiel die Möglichkeit, das Konto in einen Gedenkzustand zu versetzen, so dass Freunde und Angehörige in der Chronik Erinnerungen hinterlassen können und die Inhalte des Profils erhalten bleiben. Bei den beruflichen Netzwerken Xing und LinkedIn wird das Profil unsichtbar geschaltet, sobald die Betreiber über den Tod des Mitglieds informiert werden. Sie erleichtern Ihren Erben das zu tun, was Sie sich wünschen, wenn Sie Ihren Willen und die Zugangsdaten hinterlegen.

Im Folgenden erläutern wir, wie Sie bei der Regelung und vor allem der sicheren Hinterlegung Ihres Digitalen Nachlasses vorgehen können.

## Hinweise für die Hinterlegung:

Auch Ihre Daten, digitale Fotos, Mitgliedskonten bei sozialen Netzwerken und online geschlossene Verträge gehören zu Ihrer Erbmasse, sie sind Ihr Digitaler Nachlass. Daher können Sie in Ihrem Testament regeln, wer welchen Zugang erhalten, was gelöscht werden soll und was Sie sich für Ihre Konten und Profile wünschen.

erbio unterstützt Sie im Testaments-Modul dabei, Ihren Willen im Testament zu hinterlegen. Dennoch gibt es speziell zum Digitalen Nachlass wichtige Aspekte zu beachten, um die es hier gehen soll.

Beim digitalen Nachlass ist die **sichere Hinterlegung** besonders wichtig, da Ihre Zugangsdaten auf keinen Fall in falsche Hände geraten dürfen, weder zu Lebzeiten noch nach dem Tod.

Daher können wir ausdrücklich **nicht dazu raten, unser entsprechendes Formular "Verzeichnis der Zugangsdaten" ausgedruckt im Vorsorgeordner** zu hinterlegen.

Stattdessen stellen wir Ihnen einige Methoden vor, die deutlich sicherer sind.

### 1. Passwortgeschützter USB-Stick im Bankschließfach

Nach unseren derzeitigen Informationen ist eine sehr sichere Methode für Ihre Zugangsdaten, wenn Sie diese auf einem Datenträger (zB. USB-Stick/Memory Stick) speichern und den Zugang zu dem USB-Stick mit einem Passwort oder Nummerncode sichern (Tipps zur Beschaffung eines solchen USB-Sticks finden Sie weiter unten).

- Den USB-Stick verwahren Sie in einem Bankschließfach.
- Das Passwort dazu verwahren Sie in Ihrem Vorsorgeordner. Sobald der USB-Stick im Bankschließfach liegt, können Sie das Passwort auch vertrauten Personen mitteilen, so dass es nicht verloren gehen kann.

Regeln Sie den Zugang zum Schließfach mit der Bank so, dass nur Ihre Erben durch Vorlage eines Erbscheins, einer Sterbeurkunde sowie des Personalausweises an das Bankschließfach gelangen. Sie können mit der Bank auch vereinbaren, dass von Ihnen bevollmächtigte Personen oder vom Gericht bestätigte Betreuer Zugang zum Schließfach bekommen, sollten Sie dazu nicht mehr in der Lage sein. Die meisten Filialbanken bieten solche Services in größeren Niederlassungen an.

Hinterlegen Sie in Ihrem Vorsorgeordner und im Testament, wo sich Ihr Bankschließfach mit dem USB-Stick befindet.

Falls Sie später Änderungen an den Zugangsdaten vornehmen möchten, bereiten Sie zu Hause einen zweiten USB-Stick vor und tauschen Sie den neuen Stick zu den Öffnungszeiten der Filialbank gegen den alten aus. Löschen Sie alle Daten auf dem alten USB-Stick so schnell wie möglich. Den leeren USB-Stick können Sie bei der nächsten Änderung wieder zum Austausch verwenden.

Das Passwort können Sie auch erneuern und entsprechend im Vorsorgeordner aktualisieren, dies ist jedoch nicht unbedingt erforderlich, da der USB-Stick sicher im Bankschließfach liegt.

Natürlich können Sie auch anders herum vorgehen und das Passwort des USB-Sticks im Bankschließfach aufbewahren und den Stick im Vorsorgeordner zu Hause. Jedoch besteht hier das Risiko, dass der Stick zu Hause verloren geht oder zerstört wird. Sicherer ist der Weg, den wir hier beschrieben haben und da der regelmäßige Zugang zum Bankschließfach kein Geld kostet, bevorzugen wir die hier beschriebene Methode.

Ein entsprechendes Bankschließfach bei einer Filialbank in kleiner Größe kostet ca. 120€ pro Jahr.

**Achtung:** wählen Sie kein anonymes Schließfach, das durch Schlüssel oder Code für jedermann erreichbar wäre, sondern ein Bankschließfach, für das Sie (oder Ihre Erben oder bevollmächtigte Personen) sich in der Bankfiliale ausweisen müssen.

## 2. Verzeichnis der Zugangsdaten beim Notar hinterlegen

Eine weitere, sichere Möglichkeit besteht darin, das Verzeichnis der Zugangsdaten bei einem Notar zu hinterlegen. Ihre Erben bzw. bevollmächtigte Personen oder gerichtlich bestellte Betreuer erhalten das Verzeichnis der Zugangsdaten dann vom Notar, sollten Sie es nicht mehr können.

Falls Sie Ihr Testament ohnehin bei einem Notar hinterlegen, ergibt es viel Sinn, dort auch das Verzeichnis Ihrer Zugangsdaten zu hinterlassen. Falls Sie Änderungen an den Zugangsdaten vornehmen möchten, bereiten Sie zu Hause ein neues Verzeichnis vor und tauschen es beim Notar aus. Behalten Sie keine Kopien des Verzeichnisses auf Ihrem Rechner (auch nicht im Papierkorb) oder in ausgedruckter Form. Die Hinterlegung beim Notar ist mit Kosten verbunden, ebenso jede Aktualisierung von dort hinterlegten Dokumenten.

Falls Sie Ihre Zugangsdaten nicht in offen lesbarer Form beim Notar hinterlegen möchten, lesen Sie bitte weiter.

### **3. Passwortgeschützter USB-Stick beim Notar, Passwort des USB-Sticks im Vorsorgeordner**

Analog zum Bankschließfach können Sie auch beim Notar verfahren. Speichern Sie Ihre Zugangsdaten bzw. das Verzeichnis der Zugangsdaten auf einem mit Passwort oder Nummerncode geschützten USB-Stick ab.

- Den USB-Stick verwahren Sie beim Notar
- Das Passwort dazu verwahren Sie in Ihrem Vorsorgeordner. Sobald der USB-Stick sich beim Notar befindet, können Sie das Passwort auch vertrauten Personen mitteilen, so dass es nicht verloren gehen kann.

Außerdem hinterlegen Sie im Vorsorgeordner sowie auch im Testament, welcher Notar den USB-Stick verwahrt. Ihre Erben erhalten den USB-Stick im Todesfall vom Notar und können mit dem Passwort aus dem Vorsorgeordner auf die Zugangsdaten zugreifen.

Falls Sie später Änderungen an den Zugangsdaten vornehmen möchten, bereiten Sie zu Hause einen zweiten USB-Stick vor und tauschen Sie den neuen Stick beim Notar gegen den alten aus. Löschen Sie alle Daten auf dem alten USB-Stick so schnell wie möglich. Den leeren USB-Stick können Sie bei der nächsten Änderung wieder zum Austausch verwenden.

Das Passwort können Sie auch erneuern und entsprechend im Vorsorgeordner aktualisieren, dies ist jedoch nicht unbedingt erforderlich, da der USB-Stick sicher beim Notar liegt.

Auch die Hinterlegung eines USB-Sticks beim Notar ist mit Kosten verbunden, ebenso jeder Termin, bei dem Sie den Datenträger austauschen.

### **4. Passwortgeschützter USB-Stick im Vorsorgeordner, Passwort des USB-Sticks beim Notar**

Etwas preiswerter ist es, wenn Sie das Verfahren umdrehen. Auch hierbei kopieren Sie das Verzeichnis der Zugangsdaten auf einen USB-Stick und sichern diesen mit einem komplexen Passwort bzw. Nummerncode.

- Den gesicherten USB-Stick verwahren Sie in Ihrem Vorsorgeordner.
- Das Passwort bzw. den Nummerncode hinterlegen Sie beim Notar.

Änderungen Ihrer Zugangsdaten können Sie nun auf dem passwortgeschützten Stick machen, das Passwort bleibt jedoch immer unverändert. Daher sollte das Passwort bei diesem Verfahren besonders komplex sein.

Hinterlegen Sie in Ihrem Vorsorgeordner und im Testament, welcher Notar über das Passwort verfügt.

Auf diese Weise entstehen bei Änderungen der Zugangsdaten keine zusätzlichen Notarkosten. Allerdings kann der USB-Stick auf diese Art verloren gehen oder zerstört werden, was bei der Hinterlegung beim Notar oder im Bankschließfach deutlich unwahrscheinlicher ist.

## 5. Browserbasierte Passwort-Manager

Ein weiterer sicherer Weg sind Passwort-Management-Systeme, die online über einen Browser erreichbar sind oder sogar in den Browser installiert werden können. Hier legen Sie zunächst ein Master-Passwort fest, das Zugriff auf alle anderen Passwörter ermöglicht. Innerhalb des Passwort-Management-Systems können Sie dann alle erdenklichen Zugangsdaten ablegen und erreichbar machen. Das Master-Passwort können Sie wie oben beschrieben in einem Bankschließfach oder bei einem Notar aufbewahren und so Ihren Erben oder bevollmächtigten Personen zugänglich machen.

Mit dieser Methode ist die Passwordeingabe für Sie selbst im Alltag deutlich einfacher. Die Systeme unterstützen auch bei der sicheren Passwortwahl und bei der Aktualisierung. Sie ersparen sich damit auch, ein Formular oder Verzeichnis zu pflegen und aktuell zu halten.

Allerdings darf das Master-Passwort nie verloren gehen, da ansonsten der Zugriff auf die dahinter liegenden Zugangsdaten kaum mehr möglich ist.

Solche Systeme kosten ca. 20€/Jahr.

Falls Sie ein browserbasiertes Passwort-Management-System ausprobieren möchten, schauen Sie sich zum Beispiel die folgenden Anbieter an. Sie können dort direkt Zugangsdaten hinterlegen, aber auch das ausgefüllte erbio Verzeichnis der Zugangsdaten als PDF-Dokument.

<https://nordpass.com/>

<https://start.1password.com/>

<https://de.norton.com/>

<https://www.dashlane.com/>

<https://bitwarden.com/>

<https://www.roboform.com/>

**Wichtig:** Die Verwahrung ausgedruckter Zugangsdaten, Master-Passwörter oder ungesicherter Datenträger zu Hause bzw. im Vorsorgeordner ist nicht zu empfehlen. Zwar können Sie den Vorsorgeordner oder USB-Stick in einem Tresor oder abgeschlossenen Raum verwahren, jedoch ist dort üblicherweise das Risiko höher, dass Ihre Zugangsdaten in falsche Hände geraten oder zerstört werden, als im Bankschließfach oder bei einem Notar.

## **Tipps zu passwortgeschützten USB-Sticks bzw. passwortgeschützten Datenträgern**

Verlässliche USB-Sticks (auch als Memory Sticks, Speicher-Sticks oder Flash-Laufwerke bezeichnet) mit Sicherungsmöglichkeit sind schon ab 10€ zu haben. Für die Ablage weniger Dokumente (zB. Ihre Zugangsdaten zu digitalen Nutzungskonten) genügt ein USB-Stick mit zB. 1GB Speichervolumen vollkommen. Nur falls Sie darauf viele Dateien mit hohem Speicherbedarf (zB. Videodateien, viele hochauflösende Fotos) hinterlegen möchten, benötigen Sie vielleicht mehr Speicherkapazität.

Empfehlenswert sind zB. USB-Sticks, die ein eigenes Ziffernfeld haben, in das ein Zahlen-Code eingegeben werden muss (ab ca. 50€). Üblicherweise sind das 7 bis 15-stellige Ziffernfolgen, die Sie selbst wählen können.

Machen Sie sich ein wenig mit der Handhabung vertraut. Üben Sie mit dem Ziffernfeld und dem Stick, bevor Sie Ihre Daten wirklich dort hinterlegen. Stellen Sie sicher, dass Sie mit Ihrem Code tatsächlich auch wieder an Ihre Daten herankommen.

Falls Sie einen USB-Stick beim Notar oder in einem Bankschließfach verwahren, schaffen Sie sich am besten gleich zwei gleiche Sticks an. So können Sie immer einen zu Hause behalten. Falls sich dann Passwörter ändern oder neue hinzukommen, können Sie eine neue Version Ihres Verzeichnisses zu Hause auf den USB-Stick laden und diesen mit dem Stick beim Notar oder aus dem Bankschließfach austauschen.



**Wichtig:** Nach dem Tausch löschen Sie bitte sofort alle Daten auf dem USB-Stick mit dem veralteten Verzeichnis.



## Weitere Hinweise zum Ausdrucken und zur Ablage:

- Falls noch nicht geschehen, legen Sie sich einen **Vorsorgeordner** (einen großen Aktenordner) mit mehreren Trennblättern für verschiedene Bereiche (Bestattungsverfügung, Vermögensverzeichnis, Vorsorgevollmacht, Patientenverfügung, Testament, etc.) an.
- Legen Sie das ausgefüllte erbio-Formular Verzeichnis der Zugangsdaten **auf keinen Fall in den Vorsorgeordner**. Beschreiben Sie hier nur auf der entsprechenden erbio-Vorlage, wie Ihre Erben oder bevollmächtigte Personen auf Ihre digitalen Konten zugreifen können.
- Falls Sie das Formular oder die Vorlage am Bildschirm lesen oder ausfüllen möchten, nutzen Sie bitte ausschließlich das kostenlose Programm **Adobe**

**Acrobat Reader.** Mit anderen Programmen kann das Formular in der Darstellung abweichen.

- Falls Sie in einem Bereich über mehr Konten verfügen, als das Formular Ihnen anbietet, drucken Sie entsprechend mehr Seiten dieses Bereichs aus.
- Falls Sie bestimmte Zugangsdaten nur einer bestimmten Person zugänglich machen möchten, legen Sie dafür ein separates Verzeichnis an und entfernen Sie diese Zugangsdaten aus dem Verzeichnis aller anderen Daten.
- **Datenhygiene:** Löschen Sie regelmäßig Daten und Zugänge, die Sie nicht verwenden. Melden Sie sich von ungelesenen Newslettern ab. Löschen Sie Konten bei Shops, in denen Sie nicht mehr einkaufen.

## Ausfüllhinweise:

Unser Formular "Verzeichnis der Zugangsdaten" enthält wesentliche Bereiche, die nach aktuellem Stand der Technik die meisten Menschen in der ein oder anderen Weise nutzen.

Sie können aktuell Zugangsdaten eintragen zu:

- Smartphone / Mobiltelefon
- E-Mail-Konten
- Bezahldiensten
- sozialen Netzwerken
- eigener Homepage / Hosting
- Streaming-Diensten
- Digital-Abos
- Shops und Marktplätzen
- Software-Abos / App-Abos
- sonstigen Digital-Diensten

In jedem Bereich gibt es die Möglichkeit, mehrere Zugangsdaten dieser Art zu hinterlegen. Falls Sie mehr Felder benötigen, drucken Sie die entsprechenden Seiten gerne mehrfach aus.

Achten Sie sorgsam darauf, dass das ausgefüllte Formular "**Verzeichnis meiner Zugangsdaten**" **nie für Unbefugte erreichbar ist**. Schützen Sie es gut und nutzen Sie die Hinweise weiter oben.

Das Formular "**Ablage meiner Zugangsdaten**" können Sie hingegen im Vorsorgeordner zu Hause aufbewahren. Falls Sie ein Passwort-Management-System für die Zugänge Ihres Digitalen Nachlasses nutzen, tragen Sie **das Master-Passwort auf keinen Fall** in das Formular ein.