



Feri Cilurzo

dipl. Treuhandexperte, Fachmann Finanz- und Rechnungswesen mit eidg. Fachausweis
Mitglied des Instituts Treuhand 4.0 von TREUHAND|SUISSE, Bern
Partner und Mitglied der Geschäftsleitung, Aeberli Treuhand AG, Zürich
www.aeberli.ch / www.treuhand40.ch



Dieser Fachbeitrag steht Ihnen auch als Audiodatei zur Verfügung: auf www.trex.ch gehen, direkt hören oder herunterladen.

Erbrecht

Digitaler Nachlass: Vorsorge zu Lebzeiten und Abwicklung im Todesfall

Unser Leben ist bis in den Tod digital: E-Banking, Kryptos, Cloud-Daten und Social-Media-Profile verschwinden nicht einfach mit dem letzten Log-in. Der nachfolgende Beitrag zeigt, welche Elemente zum digitalen Nachlass gehören, welche rechtlichen und technischen Hürden bestehen und mit welchen konkreten Instrumenten – vom digitalen Inventar über Passwortmanagement und Vorsorgeauftrag bis zu Nachlassfunktionen der Plattformen – Treuhandprofis ihre Mandanten wirksam schützen und im Ernstfall handlungsfähig bleiben.

Die Bedeutung des digitalen Nachlasses für Treuhänder

Unser Alltag findet längst auch digital statt. Wir kommunizieren online, speichern Fotos und Dokumente in der Cloud, erledigen Bankgeschäfte via E-Banking, besitzen Kryptowährungen und haben Dutzende Online-Accounts. In der Schweiz gibt es 2,7 Millionen aktive Facebook- und 5 Millionen LinkedIn-Nutzer. Doch viele denken nicht daran, dass all diese digitalen Spuren und Vermögenswerte auch nach ihrem Tod bestehen bleiben. Anders als beim Verlust eines physischen Schlüssels, bei dem ein Schlüsseldienst helfen kann, gibt es im digitalen Bereich keinen einfachen Rettungsdienst: Ohne

die passenden Passwörter bleiben Zugänge oft für immer verschlossen und digitale Werte gehen verloren oder werden unbrauchbar.

Für Treuhänderinnen und Treuhänder gewinnt das Thema des digitalen Nachlasses daher kontinuierlich an Bedeutung. Eine aktuelle Studie der Stiftung für Technologiefolgen-Abschätzung (TA-SWISS) aus dem Jahr 2024 mit dem Titel «Der Tod im digitalen Zeitalter» belegt, dass viele Hinterbliebene weder wissen, welche Konten existieren, noch wie darauf zugegriffen werden kann. Dies macht den Todesfall noch schwerer.¹ Als Vertrauenspersonen, die ihre Kunden ganzheitlich betreuen, sind Treuhandexperten heute nicht nur für klassische Nachlassfragen, sondern auch für die digitalen Hinterlassen-

schaften zuständig. Andernfalls stehen die Erben im Todesfall des Kunden vor grossen Herausforderungen: Wichtige Online-Konten könnten für sie unzugänglich sein, Vermögenswerte in digitalen Wallets könnten verloren gehen oder persönliche Daten könnten in die falschen Hände geraten.

Dieser Beitrag zeigt auf, wie Treuhänder ihre Kunden vorausschauend beraten können, damit deren digitaler Nachlass im Todesfall geregelt ist. Anschliessend wird dargestellt, wie Treuhänder Erben und Nachlassverwalter bei der Abwicklung des digitalen Nachlasses unterstützen können.

1. Vorsorge und Beratung von Kunden

1.1 Was zum digitalen Nachlass gehört: Definition und Kategorien

Zum digitalen Nachlass zählen alle digitalen Daten, Konten, Zugangsrechte und Vermögenswerte einer Person, unabhängig davon, ob sie online im Internet oder offline auf lokalen Geräten gespeichert sind. Dazu zählen unter anderem:

- **Digitale Identitäten und Profile:** Alle Online-Profile in sozialen Netzwerken (Facebook,

Instagram, LinkedIn, X/Twitter usw.), Blogs, Foren sowie Benutzerkonten für E-Mail und Messenger-Dienste, wie z.B. WhatsApp. Diese bilden die digitale Identität einer Person und enthalten persönliche Inhalte wie Posts, Kommentare, Nachrichten und Fotos.

- **Online-Daten und Cloud-Speicher:** Dateien und Datensammlungen, die in Cloud-Diensten (z.B. Dropbox, Google Drive, Microsoft OneDrive, iCloud) oder auf anderen Online-Plattformen gespeichert sind, inklusive Online-Fotoalben und Back-ups.

- **Finanzielle Online-Konten:** Digitale Vermögenswerte und Zahlungszugänge wie Online-Banking-Zugänge, E-Wallets (PayPal u.Ä.), Kryptowährungs-Wallets auf Kryptobörsen oder in Hardware-Wallets, Online-Depots und Trading-Accounts, Shopping-Guthaben, Bonuspunktkonten und Ähnliches.

- **Digitale Inhalte und Lizenzen:** Gekaufte digitale Güter und Rechte, zum Beispiel E-Books, Musik- und Filmbibliotheken (iTunes, Kindle usw.), Softwarelizenzen, Domains und Websites, digitale Abonnemente sowie virtuelle

Güter in Online-Spielen. Oft sind diese Inhalte an Nutzerkonten gekoppelt und, rechtlich betrachtet, lizenziert, statt im klassischen Sinn «besessen».

- **Geräte und lokale Datenträger:** Hardware wie Smartphones, Computer, Laptops, Tablets, externe Festplatten, USB-Sticks oder auch Smart-Home-Geräte. Auf ihnen befinden sich persönliche Daten (Dokumente, E-Mails, Fotos, Videos) und oft auch gespeicherte Passwörter oder automatisch eingeloggte Accounts. Diese physischen Datenträger sind Schlüssel zum digitalen Nachlass, denn ihr Besitz ermöglicht in vielen Fällen erst den Zugriff auf Online-Konten (z.B. via gespeicherte Log-ins oder Authenticator-Apps).

Viele dieser Elemente haben einen immateriellen, emotionalen Wert, etwa Familienfotos oder letzte E-Mails, oder sogar einen erheblichen finanziellen Wert, wie Kryptoguthaben oder Online-Guthaben. Entsprechend müssen sie ebenso sorgfältig in die Nachlassplanung einbezogen werden wie materielle Werte.

1.2 Rechtliche Ausgangslage in der Schweiz: Anspruch vs. Zugriff

Auf den ersten Blick ist die gesetzliche Lage klar: In der Schweiz gilt die Universalsukzession (Gesamtrechtsnachfolge nach Art. 560 ZGB). Das heisst, mit dem Tod tritt die Erbengemeinschaft in sämtliche Rechtspositionen der verstorbenen Person ein, und zwar grundsätzlich auch in digitale Verträge, Konten und Lizenzrechte. Mit anderen Worten stehen den Erben rein rechtlich dieselben Ansprüche auf die digitalen Güter und Daten des Erblassers zu, wie es bei physischen Gegenständen der Fall ist.² Die Praxis sieht jedoch anders aus: Obwohl der rechtliche Anspruch besteht, scheitert der tatsächliche Zugriff auf digitale Konten und Inhalte oft an technischen und rechtlichen Hürden. Wichtige Problempunkte sind dabei:

- **Fehlende Zugangsdaten:** Ohne Passwörter oder Entsperrcodes bleiben Smartphones, Computer und Online-Accounts verschlossen. Zudem setzen viele Dienste eine Zwei-Faktor-Authentifizierung ein, wodurch sich der Zugang ohne das registrierte Mobilgerät zusätzlich erschwert. Wenn keine entsprechenden Vorkehrungen getroffen wurden, müssen Erben unter Umständen aufwendig versuchen, Passwörter zu rekonstruieren, was nicht immer möglich ist.
- **Nutzungsbedingungen der Anbieter:** Die allgemeinen Geschäftsbedingungen (AGB) vieler Online-Dienste – meist von ausländischen Unternehmen angeboten – schränken den Übergang von Konten auf Erben ein. Oft sind persönliche Accounts laut AGB nicht übertragbar. Einige Dienste behalten

sich vor, das Konto im Todesfall zu löschen oder den Zugriff nur sehr eingeschränkt zu erlauben. Diese vertraglichen Regelungen stehen teilweise im Widerspruch zum Schweizer Erbrecht, führen in der Praxis jedoch dazu, dass Erben ohne die Zustimmung des Anbieters nicht weiterkommen.³

- **Datenschutz und Persönlichkeitsrechte:** In digitalen Konten sind oft auch Daten Dritter enthalten, die weiterhin geschützt sind. Dazu zählen beispielsweise E-Mails von Geschäftspartnern, Chatverläufe oder gespeicherte personenbezogene Daten. Die TA-SWISS-Studie stellt klar, dass Persönlichkeitsrechte mit dem Tod enden, während Erben Informations- und Zugriffsrechte auf digitale Vermögenswerte haben. Nach Schweizer Recht enden die höchstpersönlichen Rechte der verstorbenen Person zwar mit dem Tod, doch der Schutz der Privatsphäre von Kommunikationspartnern bleibt bestehen. Anbieter berufen sich deshalb teils auf den Datenschutz, um Inhalte nicht herauszugeben, insbesondere wenn keine ausdrückliche Einwilligung oder Verfügung des Verstorbenen vorliegt. Erben dürfen also nicht automatisch alle Daten einsehen, selbst wenn sie rechtlich nachfolgen. Es muss also abgewogen werden, welche Einsicht zur Regelung des Nachlasses nötig und zulässig ist.
- **Uneinheitliche Regelungen der Plattformen:** Jeder Online-Dienst handhabt einen Todesfall anders. Einige E-Mail-Provider oder Social-Media-Plattformen löschen ein inaktives Konto automatisch nach einer gewissen Zeit oder sobald ihnen ein Todesfall gemeldet wird. Besonders kritisch ist die Änderung der Inaktivitätsrichtlinie von Google im Mai 2023. Seit Dezember 2023 werden Konten, die über zwei Jahre nicht genutzt wurden, mitsamt aller Inhalte in Gmail, Google Drive und Google Fotos gelöscht.⁴ Andere Dienste ermöglichen es Angehörigen, einen Account in einen Gedenkzustand zu versetzen (wie bei Facebook), sodass das Profil bestehen bleibt, ein Log-in jedoch nicht mehr möglich ist. Wieder andere Dienste gewähren nur nach einem aufwendigen Verfahren oder einem Gerichtsbeschluss Zugriff auf Kontoinhalte, sofern überhaupt. Kurz: Es gibt keinen Standard. Google etwa bietet mit dem Inaktivitätsmanager die Möglichkeit, schon zu Lebzeiten festzulegen, was mit dem Account passieren soll (Datenweitergabe an ausgewählte Personen oder Kontoautomatik bei Inaktivität). Facebook erlaubt es, einen Nachlasskontakt zu bestimmen oder das Konto löschen zu lassen. Apple hingegen hielt sich lange bedeckt: Gemäss den traditionellen Apple-Richtlinien endete ein Apple-ID-Account mit dem Tod des Nutzers, sodass iCloud-Daten ohne vor-

herige spezielle Vorkehrungen für Erben unzugänglich blieben. Neuere Apple-Funktionen wie Digital Legacy (seit iOS 15 eingeführt) müssen vom Nutzer zu Lebzeiten aktiv eingerichtet werden. Geschieht dies nicht, bleibt es beim Grundsatz, dass kein Zugang gewährt wird. Aufgrund dieser Unterschiede müssen Erben im digitalen Nachlass oft Einzelfalllösungen suchen und mit jedem Anbieter separat verhandeln.

→ Fazit Rechtslage

Der digitale Nachlass bewegt sich derzeit in einer Grauzone zwischen Erbrecht, Vertragsrecht, Datenschutz und den AGB der Konzerne. In der Schweiz fehlt eine spezifische gesetzliche Regelung. Das hat für die Praxis folgende Bedeutung: Ohne Vorbereitung und ohne die nötigen Zugänge nützen den Erben ihre erbrechtlichen Ansprüche wenig. Sie stehen vor gesperrten Bildschirmen und verschlossenen Datentresoren. Genau hier setzt eine vorausschauende Beratung an, damit der «Schlüssel» zum digitalen Erbe nicht verloren geht.

1.3 Vorausschauende Beratung: Den digitalen Nachlass zu Lebzeiten regeln

Angesichts der genannten Unsicherheiten ist es von entscheidender Bedeutung, dass Treuhänder ihre Kunden bereits zu Lebzeiten für das Thema «digitaler Nachlass» sensibilisieren und bei Bedarf konkrete Vorkehrungen treffen. Internationale Umfragen zeigen: Zwei Drittel der Internetnutzer haben ihren digitalen Nachlass nicht geregelt. Zwar wächst das Bewusstsein, doch die Umsetzung bleibt gering. Viele Menschen sind sich nicht darüber im Klaren, welche Last ungeklärte Online-Konten und Daten für Hinterbliebene darstellen können. Treuhänder können hier helfen, Klarheit zu schaffen. In der Praxis haben sich folgende Massnahmen bewährt, um den digitalen Nachlass rechtzeitig zu regeln:

1. **Digitales Inventar erstellen:** Als ersten Schritt sollte der Kunde – gegebenenfalls mit Unterstützung des Treuhänders – eine vollständige Bestandsaufnahme aller digitalen Konten, Profile, Geräte und Vermögenswerte vornehmen. In dieses digitale Inventar gehören sämtliche Zugangspunkte, wie beispielsweise E-Mail-Accounts, Social-Media-Profile, Cloud-Speicher, Online-Abos, Shopping-Accounts, Banking-Zugänge, Kryptokonten sowie Handy und Laptop. Auch «versteckte» Digitalkonten, wie beispielsweise Kundenkonten bei Online-Shops, Streaming-Diensten oder Bonusprogrammen, sollten erfasst werden. Wichtig ist, diese Übersicht regelmässig zu aktualisieren, da immer wieder

neue Dienste hinzukommen oder alte wegfallen. Das Inventar bildet die Grundlage dafür, dass im Ernstfall nichts übersehen wird. Es kann in Form eines schriftlichen Verzeichnisses oder mithilfe spezieller Software geführt werden.

→ Eine Übersicht für ein solches Inventar können Sie auf www.trex.ch beim Artikel herunterladen.

2. Passwörter und Zugangsdaten managen:

Eine der grössten Hürden im Todesfall sind fehlende Passwörter. Treuhänder sollten ihren Kunden daher ein strukturiertes Passwortmanagement nahelegen. Bewährt hat sich die Nutzung eines Passwortmanagers (wie z.B. 1 Password oder der Schweizer Anbieter SecureSafe u.a.), in dem alle Zugangsdaten zentral und verschlüsselt gespeichert sind. SecureSafe ist ISO-27001-zertifiziert, speichert Daten in der Schweiz nach FINMA-Standards und bietet eine spezielle Nachlassfunktion:

- Vorbereitung: Der Nutzer weist Begünstigten gezielt Dateien und Passwörter zu.
- Auslösung: Eine Vertrauensperson erhält einen Aktivierungscode, mit dem sie im Ernstfall den Nachlassprozess startet.
- Sicherheitsfrist: Nach der Aktivierung gibt es eine Sperrfrist, während der der Kontoinhaber informiert wird und den Prozess bei Missbrauch stoppen kann.
- Übergabe: Erst nach Fristablauf erhalten Begünstigte einen geschützten Zugriff auf die für sie bestimmten Daten.⁵

Der Vorteil von Passwortmanagern ist, dass es anstelle von Dutzenden Einzelpasswörtern, die irgendwo niedergeschrieben werden müssen, einen Masterzugang gibt. Dieser sollte im Notfall vererbbar bzw. zugänglich sein. Das heisst, es muss geregelt sein, wer im Todesfall Zugriff auf den Master-Key erhält. Alternativ kann man auch eine Passwortliste führen, doch dann muss geklärt sein, wo diese sicher hinterlegt wird (z.B. im Tresor, im Bankschliessfach oder bei einer Vertrauensperson) und wie sichergestellt wird, dass sie aktuell bleibt. In jedem Fall sollte der Kunde eine Lösung haben, damit seine Erben nicht vor einem digitalen Rätsel stehen.

3. Testamentarische Verfügungen für digitale

Werte: Es empfiehlt sich, letztwillige Anordnungen zum Umgang mit dem digitalen Nachlass zu treffen. Im Testament oder in einem Ergänzungsbrief zum Testament kann der Kunde festhalten, was mit seinen wichtigsten digitalen Konten und Inhalten geschehen soll.

Zum Beispiel: Sollen Social-Media-Profile gelöscht oder in Gedenkzustand versetzt werden? Wer soll Zugriff auf die persönlichen Fotos und E-Mails erhalten? Gibt es digitale Vermögenswerte (z.B. Kryptoguthaben), die an bestimmte Erben vererbt werden sollen? Ebenso kann eine Person ausdrücklich beauftragt werden, den digitalen Nachlass abzuwickeln. Dies kann rechtlich durch die Ernennung eines Willensvollstreckers geschehen. Fehlt eine solche Ernennung, muss die Erbengemeinschaft die digitale Nachlassabwicklung gemeinschaftlich vornehmen, was potenziell Konflikte birgt. Eine aktuelle Schweizer Nachlassstudie zeigt: 89 Prozent setzen einen Willensvollstrecker ein, zunächst oft den Ehepartner, später eine juristische Person.⁶ Daher ist es sinnvoll, im Testament entweder einen Willensvollstrecker einzusetzen oder zumindest innerhalb der Familie eine klare Absprache zu treffen, wer sich um die digitalen Angelegenheiten kümmert. Diese Person sollte idealerweise technisch versiert sein und das Vertrauen aller Beteiligten geniessen. Treuhänder können bei der Formulierung solcher Verfügungen helfen und darauf achten, dass sie eindeutig und im Rahmen des rechtlich Zulässigen sind. Beispielsweise kann verfügt werden, dass bestimmte Daten nach dem Tod gelöscht werden sollen. Die Erben sollten dann diese Wünsche respektieren, soweit sie nicht gegen Gesetze verstossen.

4. Vorsorgeauftrag mit digitalen Kompetenzen:

Während das Testament für die Zeit nach dem Tod gilt, deckt der Vorsorgeauftrag die Situation ab, in der jemand noch lebt, aber urteilsunfähig wird (z.B. durch Unfall oder Krankheit). Auch in diesem Dokument sollten digitale Belange ausdrücklich geregelt sein. Der Kunde kann im Vorsorgeauftrag eine Person bestimmen, die im Fall der Handlungsunfähigkeit berechtigt ist, sämtliche digitalen Angelegenheiten zu erledigen, etwa Online-Bankzahlungen fortzuführen, Verträge zu kündigen oder E-Mails im Namen des Auftraggebers zu verwalten.

→ Eine mögliche Formulierung: «Dieser Vorsorgeauftrag ermächtigt die Vorsorgebeauftragte ausdrücklich dazu, sämtliche Handlungen in meinen digitalen Angelegenheiten vorzunehmen und dabei Rechte und Pflichten für mich zu begründen. Sie ist befugt, meine gesamten digitalen Vermögenswerte sowie mein digitales Leben umfassend zu verwalten, zu regeln und abzuwickeln. Dies gilt für alle geschäftlichen, finanziellen, privaten oder höchstpersönlichen Inhalte gleichermaßen. Die Vorsorgebeauftragte erhält insbesondere Zugriff auf meine gesamte Hard- und Software, auf

E-Mail-Konten sowie alle weiteren Benutzerkonten und darf diese im Rahmen ihrer Aufgaben nutzen. Ich bemühe mich, laufend sämtliche Zugangsdaten sicher in einem Passwortsafe oder ähnlich zu speichern und der Vorsorgebeauftragten den Speicherort sowie auch das Masterpasswort zugänglich zu machen bzw. bekannt zu geben. Sie ist zudem ausdrücklich berechtigt, notwendige Zugangsdaten zu verwenden oder bei Bedarf wiederherzustellen. Um dies zu ermöglichen, befreie ich alle relevanten Geheimnisträger so weit wie möglich von ihren Schweigepflichten gegenüber der Vorsorgebeauftragten.»^{7, 8}

Damit Banken oder Diensteanbieter im Vorsorgefall der beauftragten Person auch tatsächlich Zugriff gewähren dürfen, ist es wichtig, die Befugnisse klar zu definieren. Treuhänder sollten ihre Kunden auf diese Möglichkeit hinweisen und bei Bedarf juristisch fundierte Formulierungen bereitstellen. Gegebenenfalls ist es ratsam, bestehende Vorsorgeaufträge entsprechend zu ergänzen, da ältere Dokumente digitale Aspekte oft nicht berücksichtigen.

5. Nachlassfunktionen der Anbieter nutzen:

Viele grosse Online-Anbieter haben inzwischen spezielle Einstellungen oder Verfahren für den Todesfall eingeführt. Treuhänder sollten ihre Kunden darauf aufmerksam machen und bei der Einrichtung helfen. Beispiele: Bei Google kann man über den Kontoinaktivitätsmanager festlegen, ab wann ein Konto als inaktiv gilt (3, 6, 12 oder 18 Monate) und welche Person benachrichtigt wird bzw. Zugriff auf Inhalte erhält.⁹ Besonders wichtig: Wer dies nicht einrichtet, riskiert die automatische Löschung seines Kontos nach zwei Jahren Inaktivität, inklusive aller E-Mails, Fotos und Dokumente. Facebook und Instagram erlauben es, einen Nachlasskontakt zu definieren, der im Todesfall gewisse Aktionen durchführen darf (Beitrag verfassen, Profilbild ändern usw.), oder man kann verfügen, dass das Konto komplett gelöscht wird.¹⁰ Apple bietet seit iOS 15 die Möglichkeit, sogenannte digitale Legacy-Kontakte einzurichten, die mit einem speziellen Zugangsschlüssel nach dem Tod auf iCloud-Daten zugreifen können, aber nur, wenn diese Kontakte zu Lebzeiten definiert wurden. Ähnliche Mechanismen gibt es bei Microsoft (für Outlook-/Hotmail-Konten), LinkedIn (Profile können von Angehörigen gemeldet und entfernt werden) und anderen. Wichtig: Die Kunden sollten verstehen, dass diese Funktionen kein Ersatz für ein eigenes Inventar und Passwörter sind, aber eine zusätz-

liche Absicherung darstellen. Gerade weil nicht alle Anbieter solche Services haben, bleibt die primäre Verantwortung beim Nutzer selbst. Dennoch: Wer die Nachlassoptionen seiner wichtigsten Online-Dienste aktiviert, erhöht die Chance, dass im Ernstfall alles nach Wunsch abläuft.

6. Zugangsdaten sicher hinterlegen und Vertrauensperson informieren: Die beste Planung nützt wenig, wenn niemand davon weiss. Treuhänder sollten ihren Kunden deshalb raten, zumindest einer Vertrauensperson mitzuteilen, welche Vorkehrungen getroffen wurden und wo sich die entsprechenden Zugangsinformationen befinden. Konkret sollte beispielsweise bekannt sein, wo das Passwortinventar aufbewahrt wird (und wie es zugänglich ist, etwa durch einen Schliessfachschlüssel), wer als digitaler Nachlassverwalter vorgesehen ist und ob es besondere Anweisungen gibt. Es bietet sich an, ein verschlüsseltes digitales Schliessfach oder einen Datentresor zu nutzen. Dies erfordert Feingefühl: Einerseits soll sichergestellt werden, dass die Informationen im Ernstfall verfügbar sind, andererseits soll Missbrauch zu Lebzeiten verhindert werden. Schweizer Lösungen wie LegacyNotes (empfohlen von Pro Senectute) bieten hierfür spezielle Plattformen, die Daten erst nach validierter Sterbeurkunde freigeben.¹¹ Hier ist oft eine gute Lösung, die Daten bei einer neutralen Stelle (Notar, Bank, Anwalt oder eben Treuhänder) zu hinterlegen, die sie nur gegen Vorweisen eines Todesnachweises aushändigt. Bei internationalen Anbietern ist Vorsicht geboten: Diese gilt es sorgfältig auszuwählen, insbesondere bezüglich der Einhaltung des Datenschutzes. Es ist darauf zu achten, dass für den Vertrag europäisches Recht gilt.¹²

1.4 Besonderer Hinweis: Kryptowährungen

Bei der Vorsorge für Kryptowährungen ist höchste Sorgfalt geboten. Kryptowährungen wie Bitcoin existieren ausschliesslich virtuell und sind durch kryptografische Schlüssel gesichert. Ohne den privaten Schlüssel oder die Wiederherstellungsphrase ist ein Kryptoguthaben unwiederbringlich verloren. Es gibt keine Bank, die in diesem Fall Zugriff gewähren könnte. Treuhänder müssen ihre Kunden daher unbedingt dafür sensibilisieren, ihre Wallet-Zugangsdaten zu dokumentieren und sicher zu verwahren. Dies kann beispielsweise bedeuten, den Seed auf Papier in einem versiegelten Umschlag im Tresor zu hinterlegen oder eine Hardware-Wallet zusammen mit der PIN zu deponieren. Experten warnen eindringlich davor, Private Keys direkt ins Testament zu schreiben, da dieses nach der Eröffnung öffentlich einsehbar werden kann. Zudem sollte geregelt sein, wer technisch in der

Lage ist, die Coins zu transferieren. Gleichzeitig ist Diskretion wichtig, da offen herumliegende Informationen ein Sicherheitsrisiko darstellen. Hier den richtigen Mittelweg zu finden – Zugriff für Berechtigte zu ermöglichen, aber Unbefugten den Zugang zu verwehren – ist eine anspruchsvolle Aufgabe. Treuhänder können bei dieser Aufgabe beratend unterstützen. Durch diese vorausschauenden Massnahmen lässt sich der digitale Nachlass deutlich besser bewältigen. Der Kunde hat die Gewissheit, dass seine digitalen Werte und Erinnerungen nicht im digitalen Nirwana verschwinden. Zudem werden die Erben im Trauerfall enorm entlastet. Das Thema sollte idealerweise in jede umfassende Nachlassberatung von Treuhändern einfließen. Oft genügt schon ein gezielter Fragenkatalog, um den Mandanten die Bedeutung vor Augen zu führen. Erfahrungsgemäss sind viele Kunden dankbar, wenn dieses heikle Thema angesprochen wird, denn die meisten schieben es vor sich her. Hier kann der Treuhänder proaktiv handeln und seine Fachkompetenz unter Beweis stellen.

2. Abwicklung des digitalen Nachlasses im Todesfall

Wenn ein Kunde verstirbt, stellt sich die Frage, wie mit seinem digitalen Nachlass umgegangen werden soll. Idealerweise hat die verstorbene Person Vorkehrungen getroffen (wie in Punkt 1 beschrieben). Doch selbst dann stehen Erben und Nachlassverwalter vor praktischen Aufgaben, um die digitale Hinterlassenschaft abzuwickeln. In dieser Phase können Treuhänder eine unterstützende Rolle spielen, sei es als Berater der Erben oder als Willensvollstrecker. Zunächst ist es hilfreich, die grössten Hürden und Ziele bei der Nachlassabwicklung zu klären:

- **Zugangsprobleme überwinden:** Gibt es funktionierende Passwörter oder andere Zugangsmöglichkeiten zu den Geräten und Konten des Verstorbenen? Falls nein, wie kann man dennoch an die Daten gelangen (z.B. über Kundendienst der Anbieter)?
- **Daten sichern, bevor sie verloren gehen:** Viele Online-Dienste könnten das Konto des Verstorbenen sperren oder Daten nach einer gewissen Inaktivitätszeit löschen. Es gilt also, schnell, aber sorgfältig zu handeln, um nichts Wertvolles zu verlieren.
- **Entscheidungen über Inhalte treffen:** Welche Daten sollen erhalten bleiben (z.B. Familienfotos), welche sollen aus Pietäts- oder Datenschutzgründen gelöscht werden (z.B. persönliche Chatverläufe)? Wer trifft diese Entscheidungen und auf welcher Grundlage?
- **Wirtschaftliche Werte retten:** Gibt es digitale Guthaben oder Vermögenswerte, die für

die Erbmasse gesichert werden müssen (z.B. Geld auf Online-Konten, Kryptowährungen, laufende Online-Verträge)? Diese müssen identifiziert und möglichst rasch in den Besitz der Erben gebracht werden, bevor Gebühren oder Sperrungen eintreten.

- **Formalitäten und Anbieterkommunikation:** Nahezu jeder digitale Dienst hat eigene Prozesse für den Todesfall. Oft müssen Erben Sterbeurkunden oder Erbnachweise einreichen, um Konten aufzulösen oder Daten herausverlangt zu bekommen. Dies erfordert Koordination und Geduld im Kontakt mit dem Kundensupport der Anbieter.

Angesichts all dieser Punkte empfehlen sich beim Vorgehen nach einem Todesfall einige Grundsätze und Schritte, an denen Treuhänder sich orientieren können:

- **Zugriff sicherstellen und Daten schnell sichern:** Zeit ist ein kritischer Faktor. Erfahrungsgemäss sperren manche Anbieter die Accounts kurze Zeit nach Kenntnis des Todesfalls oder es gehen Daten verloren, wenn Abonnemente enden und der Speicher gelöscht wird. Daher sollten alle greifbaren Geräte des Verstorbenen (Smartphone, Laptop, Tablet usw.) so früh wie möglich eingesammelt, aufgeladen und eingeschaltet werden, solange sie noch entsperrt sind oder sich entsperren lassen. Sind die Passwörter bekannt (z.B. aus Unterlagen oder dem Passwortmanager), sollten die wichtigsten Accounts umgehend geöffnet und ein Back-up der Daten erstellt werden. Insbesondere E-Mails, Cloud-Speicher und Fotos/Videos sollten zeitnah gesichert werden. Wenn möglich, sollte man die Sicherheitsmechanismen temporär entschärfen. Beispielsweise sollte man den PC nicht ausschalten, solange man noch Zugriff hat, oder das Handy am Strom lassen, um ein automatisches Sperren zu vermeiden. Bevor ein Anbieter vom Todesfall erfährt, kann unter Umständen noch ein Log-in mit bekannten Zugangsdaten funktionieren. Hier ist rechtlich Vorsicht geboten: Streng genommen, sind viele Accounts laut AGB persönlich, sodass ein Log-in durch Dritte gegen die Nutzungsbedingungen verstösst. In der Praxis ist es allerdings meist der einzige Weg, an die Daten zu gelangen. Ein im Auftrag handelnder Willensvollstrecker oder Erbe bewegt sich hierbei in einer Grauzone. Viele tun es, um wichtige Informationen zu retten. Treuhänder sollten zumindest darauf hinweisen, dass die Verwendung von Zugangsdaten durch Unbefugte rechtliche Konsequenzen haben kann. Faktisch wird dies jedoch oft toleriert, wenn Erben oder Bevollmächtigte so handeln. In jedem Fall gilt: Zuerst die Daten sichern, dann über eine Löschung nachden-

ken. Was einmal weg ist, kann nicht zurückgeholt werden. Es ist also besser, alle verfügbaren E-Mails, Dateien, Kontaktlisten usw. auf ein separates Medium zu kopieren, bevor man irgendwelche Konten schliesst oder Veränderungen vornimmt.

- **Digitale Vermögenswerte sichern und übertragen:** Hat der Verstorbene Online-Guthaben oder andere werthaltige digitale Assets hinterlassen, geniessen diese oberste Priorität. Dazu zählen Guthaben auf rein digitalen Bankplattformen, Kryptowährungen, Guthaben bei Online-Bezahldiensten, Verkäuferguthaben bei Ebay/Amazon oder Wallets in Apps. Solche Werte können im schlimmsten Fall verfallen, wenn niemand rechtzeitig darauf zugreift. Daher sollte sofort überprüft werden, ob entsprechende Informationen im digitalen Inventar oder in den Unterlagen zu finden sind. Kryptowährungen sollten umgehend in die sichere Verwaltung der Erben überführt werden, allerdings nur, wenn die Zugangs-Keys vorhanden sind. Gibt es ein Hardware-Wallet, muss es sorgfältig aufbewahrt werden. Liegen Passwörter zu Kryptobörsen vor, sollte ein Sachkundiger die Coins möglichst auf ein Erbenkonto transferieren oder in eine gemeinsame Wallet überführen. Achtung: Hier spielt die technische Kompetenz eine grosse Rolle. Falls niemand im Erbenkreis mit Kryptotransaktionen vertraut ist, sollte unbedingt fachkundiger Rat eingeholt werden, um keine Fehler zu machen (eine falsche Überweisung ist unwiderruflich). Bei Online-Bankkonten oder -Bezahldiensten empfiehlt es sich, die Anbieter zügig zu kontaktieren, den Tod zu melden und um Auszahlung des Guthabens auf ein Nachlasskonto zu bitten. In vielen Fällen verlangen Banken dazu einen Erbschein. Treuhänder können bei der Zusammenstellung solcher Dokumente helfen.
- **Konten verwalten, übertragen oder löschen:** Nachdem die wichtigsten Daten gesichert und Vermögenswerte geborgen sind, geht es darum, den digitalen Nachlass abzuwickeln, d.h. die digitalen Identitäten angemessen zu verwalten oder aufzulösen. Nicht alles sollte kopflos gelöscht werden. Man sollte in jedem Fall prüfen, ob ein Konto eventuell noch benötigt wird, z.B. um Informationen zu erhalten. Gleichzeitig möchte man aber nicht dauerhaft «Geisterkonten» bestehen lassen, die später zur Sicherheitslücke werden könnten. Verwaiste Accounts («Datenleichen») stellen ein erhebliches Sicherheitsrisiko dar: Sie sind anfällig für Hacking, Identitätsdiebstahl und Missbrauch. Folgende Vorgehensweisen haben sich etabliert:
 - **E-Mail-Konten:** E-Mails sind oft der Schlüssel zu anderen Konten (Passwörterücksetzungen laufen darüber). Deshalb sollte

mindestens ein zentrales E-Mail-Konto (z.B. die Hauptadresse) offen gehalten werden, bis sichergestellt ist, dass alle relevanten Dienste erfasst und umgestellt sind. Treuhänder können das Postfach nach wichtigen Mitteilungen (z.B. von Versicherungen, Verträgen, Kunden usw.) durchsuchen. Sobald dies erledigt ist, sollte man das Konto aus Datenschutzgründen jedoch schliessen. Viele E-Mail-Provider (GMX, Bluewin usw.) löschen Konten nach Benachrichtigung über den Tod oder nach längerer Inaktivität ohnehin. Bei geschäftlichen E-Mail-Accounts ist zu prüfen, ob Kollegen oder Nachfolger Zugriff erhalten müssen, um den Geschäftsbetrieb aufrechterhalten zu können.

- **Soziale Netzwerke:** In diesem Zusammenhang stellen sich vor allem Fragen zu Privatsphäre und Pietät. Hätte der Verstorbene gewollt, dass seine Profile online bleiben? Oder ziehen es die Angehörigen vor, diese zu löschen, um Missbrauch (z.B. durch Hacking) vorzubeugen? Facebook etwa ermöglicht im Gedenkzustand, dass Freunde weiterhin Beiträge auf der Pinnwand des Verstorbenen hinterlassen können. Für manche Trauernde ist das ein Ort des Gedenkens, der Trost spendet, für andere ist es eher ein unerwünschtes Weiterleben des Profils. Treuhänder sollten die Erben fragen, welche Präferenz besteht. Falls der Erblasser nichts verfügt hat, kann man eine Weile abwarten, um Erinnerungen zu sichern (Fotos und Beiträge herunterladen) und dann die Löschung veranlassen. Jeder grössere Dienst hat Formulare für Todesfallmeldungen. Oft genügt eine Kopie der Sterbeurkunde durch einen Angehörigen ersten Grades, um eine Löschung oder Memorialisierung zu beantragen.
- **Cloud-Dienste und Online-Speicher:** Hier sollten nach Möglichkeit alle für die Familie oder den Nachlass wichtigen Dateien heruntergeladen und gesichert werden. Dazu gehören Fotos, Videos, wichtige Dokumente, eventuell digitale Scans von Urkunden usw. Anschliessend kann man den Account kündigen. Wenn der Speicher kostenpflichtig war, spart man so weitere Gebühren. Zudem stellt man sicher, dass keine neuen Inhalte (z.B. automatische Back-ups vom inzwischen abgeschalteten Handy) mehr anfallen.
- **Smartphone und Computer:** Diese Geräte enthalten oft lokal gespeicherte Daten, zum Beispiel Fotos, persönliche Tagebücher oder Chat-Back-ups. Treuhänder sollten empfehlen, auch hiervon ein vollständiges Abbild (Image) zu erstellen, bevor entschieden wird,

was mit den Geräten geschieht. Eventuell möchten die Angehörigen das Gerät weiternutzen oder einem Nachfolger übergeben (bei Geschäftslaptops beispielsweise an den Arbeitgeber). Vor der Weitergabe sollte das Gerät jedoch zurückgesetzt werden, nachdem alle wichtigen Daten extrahiert wurden. Wenn auf dem Gerät eine Passwortmanager-App installiert war, kann über diese eventuell noch vieles andere entschlüsselt werden. Es sollte also unbedingt geprüft werden, ob auf dem entsperrten Gerät ein Passwortsafe geöffnet ist.

- **Digitale Abos und Verträge:** Streaming-Abonnemente, Software-Abos oder z.B. Mitgliedschaften bei Online-Spielen sollte man kündigen, sobald sie nicht mehr gebraucht werden. Hier schützt man die Erbmasse vor weiterlaufenden Kosten. Bei einigen Diensten könnte eine anteilige Erstattung möglich sein. In jedem Fall verhindert man so, dass z.B. nach einem Jahr plötzlich Mahnungen an den Verstorbenen geschickt werden, weil ein Abo mangels Zahlung in Verzug geriet.

Die Devise lautet: geordnet und dokumentiert vorgehen. Treuhänder, die den Prozess begleiten, sollten jede Aktion notieren (z.B. «Account X am Datum Y gelöscht, Daten-Back-up liegt vor.»). So behält man den Überblick und kann den Erben oder Behörden gegenüber nötigenfalls Auskunft geben.

- **Professionelle Hilfe prüfen:** Niemand muss alles allein können. Ein digitaler Nachlass kann sehr komplex sein, insbesondere wenn es um technische Entsperrungen oder juristische Auseinandersetzungen mit Dienstleistern geht. Treuhänder sollten die Erben darauf hinweisen, dass es vollkommen legitim ist, in bestimmten Fällen Spezialisten beizuziehen. Beispiele: Lässt sich ein Smartphone trotz aller Versuche nicht entsperren, kann ein darauf spezialisiertes IT-Forensikunternehmen eventuell helfen (natürlich unter Einhaltung der Gesetze). Treuhänder haben hier die Aufgabe, die Grenzen der eigenen Kompetenz zu erkennen und im richtigen Moment externe Hilfe vorzuschlagen, anstatt risikobehaftete Experimente zu wagen. Gleichzeitig behalten sie die Rolle des Koordinators: Sie bündeln die Fäden zwischen Erben, Technikern, Juristen und den Anbietern, sodass die Erben sich nicht selbst mit jeder Facette befassen müssen.
- **Rechtliche und ethische Schranken respektieren:** Bei aller Zielorientierung dürfen Treuhänder und Erben die gesetzlichen und moralischen Grenzen nicht überschreiten. Vorsicht vor übereiltem Löschen! Auch wenn es aus Gründen der Privatsphäre gut gemeint ist, schnell etwas zu entfernen, gehören sämt-

liche Daten zunächst allen Erben gemeinsam. Kein einzelner Erbe darf Teile des Nachlasses eigenmächtig vernichten, bevor eine einvernehmliche Regelung getroffen wurde. Es wäre beispielsweise problematisch, wenn eine Person ohne Absprache den gesamten E-Mail-Account löscht, weil sie kompromittierende Inhalte vermutet. Damit könnten auch Informationen verloren gehen, die für die Erbteilung relevant gewesen wären. Zudem macht sie sich gegebenenfalls gegenüber den Miterben schadensersatzpflichtig. Ebenso heikel ist es, wenn der Verstorbene illegale Inhalte besessen hat (z.B. unerlaubte Kopien oder in Extremfällen strafbare Inhalte). Werden im Zuge der Nachlassdurchsicht solche Inhalte gefunden, ist ein umsichtiger Umgang nötig. Treuhänder sollten wissen, dass Erben nicht für die Taten des Verstorbenen bestraft werden, durch unsachgemässe Aktionen (etwa das Weiterverbreiten oder Vertuschen solcher Inhalte) aber selbst in Schwierigkeiten geraten könnten. In Zweifelsfällen ist rechtlicher Rat einzuholen.

- **Datenschutz:** Persönliche Daten unbeteiligter Dritter, die in digitalen Konten gefunden werden, dürfen nicht einfach öffentlich gemacht werden. Hier ist Diskretion Pflicht. Das ist ein Grund, warum es oft sinnvoll ist, wenn ein neutraler Treuhänder oder Willensvollstrecker die Sichtung übernimmt, statt dass alle Familienmitglieder ungefilterten Zugang zu möglicherweise sensiblen Informationen erhalten. Und zuletzt: Authentifizierung und Identitätsschutz sind wichtig. Es wäre unethisch und teilweise illegal, sich etwa über das Social-Media-Profil des Verstorbenen als diese Person auszugeben. Wenn sich ein Treuhänder einloggt, dann nur, um etwas Administratives zu erledigen (z.B. Daten herunterladen oder den Account deaktivieren), aber nicht, um unter falscher Identität zu agieren.

→ Zusammenfassend lässt sich sagen:

Die Abwicklung eines digitalen Nachlasses erfordert systematisches Vorgehen, technisches Wissen und soziale Kompetenz. Wenn dies gelingt, können digitale Nachlassangelegenheiten in geordnete Bahnen gelenkt werden, selbst in schwierigen Fällen.

3. Empfehlungen, Chancen und Fazit

Die vorangehenden Abschnitte haben gezeigt, dass der digitale Nachlass kein Nischenthema mehr ist, sondern zu einem zentralen Bestandteil moderner Nachlassplanung und -abwicklung geworden ist. Für Treuhänderinnen und Treu-

händer ergeben sich daraus mehrere Schlussfolgerungen und Chancen:

1. Digitalen Nachlass fest in die Beratung integrieren: Jeder Treuhänder, der Mandanten in Vermögens- und Nachlassfragen berät, sollte das Thema digitaler Nachlass aktiv mit auf die Agenda nehmen. Konkret heisst das: Bei der Erstellung von Testamenten, Vorsorgeaufträgen oder Nachlassregelungen sollte immer auch nach digitalen Vermögenswerten und Online-Konten gefragt werden. Ein einfaches Frageset kann hier Wunder wirken (Haben Sie Social-Media-Profile? Nutzen Sie E-Banking oder PayPal? Besitzen Sie Kryptowährungen? usw.). Dadurch signalisiert der Treuhänder Kompetenz und verhindert, dass sich im Nachhinein Lücken auftun.

2. Eigene Kompetenz aufbauen und aktuell halten: Das Gebiet des digitalen Nachlasses ist einem stetigen Wandel unterworfen. Treuhänder sollten sich deshalb weiterbilden und Know-how aufbauen, um in diesem Bereich sattelfest zu sein. Dazu gehören rechtliche Aspekte (Kenntnisse der neusten Gesetzesentwicklungen und Gerichtsentscheide zum Thema), technische Aspekte (Verständnis der gängigen Plattformen, Funktionen wie Inaktivitätsmanager, neue Trends wie NFT-Nachlässe usw.) sowie praktische Tools (Einsatz von Passwortmanagern, sichere Datenspeicherung, Checklisten für die Nachlassabwicklung). Ein Treuhänder muss nicht selbst programmieren können, aber er sollte beispielsweise wissen, was eine Zwei-Faktor-Authentifizierung ist, wie man bei Facebook einen Todesfall meldet oder welche Risiken mit einer Bitcoin-Wallet verbunden sind.

3. Zusammenarbeit fördern – interdisziplinär denken: Der digitale Nachlass betrifft verschiedene Disziplinen: Erbrecht, IT-Sicherheit, Datenschutz und manchmal auch Strafrecht. Treuhänder tun daher gut daran, ein Netzwerk aufzubauen, auf das sie im Bedarfsfall zurückgreifen können – etwa auf spezialisierte Anwälte, IT-Forenstiker oder Datensicherheitsexperten. So können sie ihren Mandanten eine umfassende Betreuung bieten, ohne alles allein abdecken zu müssen.

4. Neue Dienstleistung und Mehrwert für Mandanten: Die Begleitung beim digitalen Nachlass bietet Treuhändern auch eine Chance, ihr Serviceangebot zu erweitern. Von der Planung bis zur Abwicklung kann man hier Dienstleistungen anbieten, sei es in Form von einem Beratungsprodukt wie dem «Digitalen Nachlass-Check» für lebende Kunden oder als Teil des Mandats bei Nachlassabwicklungen.

5. Sensibilisierung und Aufklärung betreiben: Zu den treuhänderischen Sorgfaltspflichten gehört auch die Aufklärungsarbeit. So können Treuhänder beispielsweise Merkblätter

oder Checklisten zum digitalen Nachlass erstellen und ihren Kunden zur Verfügung stellen. Aufgeklärte Kunden treffen eine bessere Vorsorge. Ausserdem schützt sich der Treuhänder so selbst vor späteren Vorwürfen, er habe auf dieses oder jenes Versäumnis nicht hingewiesen.

6. Neue rechtliche Entwicklungen beachten:

In der TA-SWISS-Studie «Tod im digitalen Zeitalter» werden sechs zentrale Empfehlungen formuliert, darunter die Einführung einer digitalen Hinterlegung letztwilliger Verfügungen sowie spezifische Regelungen für den Zugriff auf personenbezogene Daten Verstorbener. Diese Entwicklungen zeigen, dass das Thema auch auf politischer Ebene an Bedeutung gewinnt. Treuhänder sollten diese Diskussionen daher verfolgen, um auf künftige Gesetzesänderungen vorbereitet zu sein und ihre Kunden entsprechend beraten zu können. ■

→ Abschliessend ist festzuhalten:

Vorsorge ist der beste Schutz. Der digitale Nachlass muss ebenso geplant werden wie das übrige Erbe. Durch eine strukturierte Dokumentation der digitalen Präsenz, die Sicherung der Zugänge und das Hinterlassen klarer Anweisungen schützen Treuhänder nicht nur die digitale Identität des Kunden, sondern entlasten auch die Angehörigen enorm. Im Todesfall zahlt sich jede vorher getroffene Vorkehrung aus. Sollten dennoch Probleme auftreten, stehen Treuhänder als kompetente Begleiter bereit, um gemeinsam Lösungen zu finden.

- ¹ <https://www.ta-swiss.ch/news/tod-und-digitalisierung>.
- ² R. Fornito und M. Näf, Der digitale Nachlass, bratschi wiederkehr & buob, Newsletter Mai 2015.
- ³ R. Fornito und M. Näf, Der digitale Nachlass, bratschi wiederkehr & buob, Newsletter Mai 2015.
- ⁴ https://www.itmagazine.ch/artikel/79672/Google_loescht_inaktive_Konten_und_Inhalte_kuenftig_nach_zwei_Jahren.html.
- ⁵ <https://www.securesafe.com/>.
- ⁶ VZ VermögensZentrum, So vererben Schweizerinnen und Schweizer ihr Vermögen, VZ-Studie, Oktober 2025.
- ⁷ Cordula Lötscher, Der digitale Nachlass, Schulthess Juristische Medien AG, Zürich, 2021, S. 159.
- ⁸ Reto Ineichen, Der digitale Nachlass in der Praxis (Teil II), Management and Law Blog, Hochschule Luzern, abrufbar unter: <https://hub.hslu.ch/management-and-law/2023/06/01/der-digitale-nachlass-in-der-praxis-teil-ii/>.
- ⁹ <https://support.google.com/accounts/answer/3036546?hl=de>.
- ¹⁰ https://www.facebook.com/help/legacycontact?locale=de_DE.
- ¹¹ <https://www.prosenectute.ch/de/dienstleistungen/docupass/online-hinterlegung/legacynotes.html>.
- ¹² Regula Heinzlmann, Digitaler Nachlass – rechtzeitig Verfügungen treffen, TREX, Ausgabe 3/2016, S. 170/171.