Seinen «digitalen Nachlass» regeln

Wer das Internet nutzt, hinterlässt digitale Spuren: Bankverbindungen, Benutzerkonten und -profile, Dokumente, Fotos und Mails. Auch nach Ihrem Tod leben Ihre Daten im Internet munter weiter. Um das zu verhindern, sollten auch Sie Ihren digitalen Nachlass regeln. Konkret geht es um die gezielte Weitergabe von Zugangsdaten (Benutzernamen und Passwörter).

Dr. iur. Marc'Antonio Iten

Was passiert mit meinen Bildern, Daten, digitalen Profilen, Konten und Texten, wenn ich sterbe? Wem gehören eigentlich meine Daten? Und wer entscheidet, was mit meinen Online-Profilen geschieht, wenn ich sterbe? Diese uns zahlreiche weitere Frage betreffen den digitalen Nachlass. Zu Ihrem digitalen Nachlass gehört alles, was Sie in Clouds, auf E-Mail-Konten, Festplatten von PCs, Smartphones und Tablets, in sozialen Netzwerken, auf Websites und Online-Diensten gespeichert haben. Das sind zum Beispiel:

- Daten, die in Clouds, auf Harddisks, Laptops, PCs, Smartphones, Speicherkarten, Tablets, USB-Sticks etc. gespeichert sind
- Eigene Websites (inkl. Webhosting-Verträge)
- E-Mail-Konten (inkl. E-Mails)
- Digitale Foto-, Musik- und Video-Sammlungen
- Guthaben in Kryptowährungen (Bitcoins etc.)
- Verträge mit kostenpflichtigen Online-Diensten und Webshops (z.B. Banken, Reise-veranstalter, Alibaba, Amazon, Anbieter von Kryptowährungen, eBay, iTunes, PayPal, Ricardo, YouTube etc.)
- Social-Media-Profile (Facebook, Instagram, LinkedIn, Twitter, XING etc.)
- Software-Lizenzen
- Streaming-Dienste (Netflix, Spotify etc.)
- Digitale Texte und E-Books

Dr. iur. Marc'Antonio Iten

Der Verfasser ist Buchautor und Co-Geschäftsführer der Dr. Strebel, Dudli + Fröhlich Steuerberatung und Treuhand AG in Zürich.

Das Gesetz regelt nicht ausdrücklich, was nach Ihrem Tod mit den Daten geschehen soll, die Sie – bewusst oder unbewusst – auf PCs, Smartphones und im Internet gespeichert haben. Für Sie gelten die Allgemeinen Geschäftsbedingungen der verschiedenen Dienste, die Sie nutzen. Viele Anbieter solcher Dienste haben ihren Sitz im Ausland, sodass ausländisches Recht gelten kann. Bis heute haben sich noch keine einheitlichen Regeln für den Umgang mit dem digitalen Nachlass durchgesetzt. Angehörige und Willensvollstrecker, die sich Zugang zu den Daten einer verstorbenen Person verschaffen wollen, erleben darum oft einen regelrechten Spiessrutenlauf.

Erben und Willensvollstrecker haben in der Regel keine genaue Kenntnis über die Online-Aktivitäten der verstorbenen Person. Weder wissen sie, wo sie digitale Konten und Profile angelegt hat und wo ihre digitalen Daten gespeichert sind, noch kennen sie die Zugangsdaten für die einzelnen Datenträger und Online-Dienste. Wer verhindern möchte, dass Daten nach seinem Tod ungeregelt weiterexistieren, sollte seinen digitalen Nachlass frühzeitig regeln.

Stellen Sie sicher, dass die Personen, die Sie dafür vorgesehen haben, nach Ihrem Tod Zugang haben zu Ihren elektronischen Datenträgern (Cloud-Dienste, Harddisks, Laptops, PCs, Smartphones, USB-Sticks etc.), zu Ihren E-Mail-Konten und Ihren Profilen in sozialen Netzwerken (Facebook, Instagram, LinkedIn, Twitter etc.), zu kostenpflichtigen Online-Diensten und Webshops (Amazon, iTunes, Netflix, Portale für Kryptowährungen, YouTube etc.) sowie zu Cloud-Dienstleistungen (Dropbox, iCloud etc.).

Dazu bieten sich grundsätzlich drei Möglichkeiten an: Sie regeln Ihren digitalen Nachlass in einem klassischen Testament, Sie nutzen die verschiedenen Werkzeuge Ihrer Service-Anbieter, oder Sie schliessen einen kostenpflichtigen Vertrag mit einem digitalen Vererbungsdienst ab.

1. **Klassisch: Digitalen Nachlass im Testament regeln**
   Sie können Ihren digitalen Nachlass in einem klassischen Testament regeln. Darin legen Sie fest, wer auf Ihre Daten zugreifen darf, mit welchem Benutzernamen und Passwort diese zugänglich sind und was mit Ihren Daten geschehen soll.
   Am besten erstellen Sie eine Übersicht über Ihre Accounts mit den dazugehörigen Benutzernamen (ID) und Passwörtern, die Sie Ihrem Willensvollstrecker in einem verschlossenen Couvert übergeben. Diese Informationen sollten mindestens einmal pro Jahr aktualisiert werden. Essenziell sind in jedem Fall die Zugangsdaten (ID und Passwort) zu Ihren Datenträgern (PCs, USB Sticks, Festplatten und Smartphones). Allenfalls kann es sinnvoll sein, für die Abwicklung Ihres digitalen Nachlasses einen separaten Willensvollstrecker zu ernennen («digitaler Willensvollstrecker»).

2. **Unübersichtlich: Individuelle Lösungen der einzelnen Anbieter**
   Bisher haben sich bei den Anbietern von digitalen Diensten noch keine einheitlichen Abläufe durchgesetzt. Es gibt so viele Lösungen beim Tod von Nutzern, wie es Internet-Plattformen gibt. Einige Anbieter gewähren den Hinterbliebenen Zugang, andere nicht. Die meisten Anbieter haben ihren Sitz im Ausland, darum gilt in der Regel ausländisches Recht, das an einem meist weit entfernten Ort durchgesetzt werden müsste. Als Nutzer sollten Sie unbedingt prüfen, welche Lösungen Ihre Anbieter vorsehen, damit Sie anschliessend entscheiden können, wie Sie Ihren digitalen Nachlass bestmöglich regeln.

3. **Kostenpflichtig: Digitale Vererbungsdienste**
   Es gibt diverse digitale Vererbungsdienste (bspw. deinadieu.ch, SecureSafe), bei denen Sie Ihre Zugangsdaten und auch wichtige Dokumente für den Todesfall speichern können. Diese Dienste weisen Sie an, an wen diese Informationen im Todesfall weitergegeben werden sollen. Solche Dienste haben sich in der Praxis noch nicht fest etabliert, darum sind sie erst mit Vorbehalt zu empfehlen. In der Regel ist auch unklar, wo die Daten gelagert werden und wer sie einsehen kann.

4. **Bitcoins sicher vererben**
   Drei bis vier Millionen Bitcoins sind nach aktuellen Studien verloren, weil ihre Besitzer oder deren Erben die Zugangsschlüssel nicht mehr finden. Ein Bitcoin ist eine digitale Information aus Nullen und Einsen. Deshalb gelten Bitcoins im juristischen Sinn als immaterielle Vermögenswerte. Anders als bei Wertpapieren ist der Zugriff nur mit einem persönlichen Schlüssel möglich (Private Key).
   Für die sichere Vererbung genügt es nicht, wenn Sie Ihren Private Key aufschreiben und weitergegeben. Speichern Sie den Private Key zunächst in einer «digitalen Brieftasche» (Wallet), und richten Sie in einem zweiten Schritt einen persönlichen Nachlassplan dafür ein. Abschliessend sollten Sie sicherstellen, dass Ihr Nachlassplan nach Ihrem Tod den berechtigten Erben (und nur ihnen) zugänglich gemacht wird.