Rechtzeitiges Kümmern ist wichtig:

Digitaler Nachlass muss geregelt sein

Jedem Unternehmer dürfte klar sein, dass frühzeitig Regelungen für den Fall getroffen werden müssen, wenn man selbst nicht mehr in der Lage ist, Entscheidungen zu treffen - sei es durch schwere Erkrankung oder den Tod. Ist es oft schon schwierig, den realen Nachlass zu regeln, so wird der digitale Nachlass oft vergessen. Wer denkt schon daran, eine Liste mit wichtigen Passwörtern anzulegen und diese einerseits gut zu *„verstekken"*, aber andererseits auch eine Vertrauensperson zu bestimmen, die Zugriff auf den digitalen Nachlass bekommen soll. Auch muss entschieden werden, was mit diesem Nachlass passieren soll, ob er gelöscht werden soll, ob die Daten weiterhin benötigt werden, was unbedingt gespeichert werden muss …

Digital = analog

Ein digitaler Nachlass ist wie ein analoger Nachlass zu betrachten. Erben haben Rechte und auch Pflichten, wenn sie das Erbe annehmen. Hier gilt das Alles-oder-Nichts-Prinzip, es geht nicht, nur das analoge Erbe oder nur das digitale Erbe anzunehmen. Es ist das Prinzip des Gesamtrechtsnachfolgers. Aktenordner und Schreibtisch werden zu Computer und Cloud.
In der analogen Welt ist es normalerweise kein schwieriges Unterfangen, sich Zugang zu den Informationen zu verschaffen. Ein Safe- oder Schließfachschlüssel lässt sich im Gegensatz zu Dutzenden von Passwörtern leicht irgendwo sicher deponieren. In der digitalen Welt sieht dies anders aus. Hier muss eine strukturierte Liste mit Anbietern und Passwörtern erstellt werden. Diese muss zwar sicher aufbewahrt werden, muss aber trotzdem schnell zugänglich sein, damit die Liste immer aktuell bleibt.

Vorgehensweise

Drei wesentliche Punkte müssen Sie beachten:
1.) Verschaffen Sie sich einen Überblick darüber, was sich alles an digitalen Daten angesammelt hat.
2.) Entscheiden Sie, wer Zugang zu welchen Daten bekommen soll.
3.) Legen Sie möglichst detailliert fest, was mit den Daten geschehen soll.

Wer Zugang bekommen soll, muss drei Dinge wissen:
1.) Den Namen des Anbieters, bei dem das Konto ist,
2.) den Nutzernamen,
3.) das Passwort und ggf. die Info, was bei einer Zwei-Faktor-Authentifizierung noch erforderlich ist (das Smartphone, eine Sicherheitsfrage…).

Wichtigste Information sind die Angaben zu den E-Mail-Providern, da die E-Mail-Adressen häufig zur Identifikation dienen.
Denken Sie beim Erstellen der Liste auch an Accounts, die seit längerem nicht mehr genutzt werden oder die nur zum Testen angelegt wurden. Löschen Sie diese selbst oder bestimmen Sie, was damit passieren soll.
Legen Sie die Liste - wenn möglich auf Papier und ohne digitale Kopie auf dem PC - an, die diese Angaben enthält und verwahren Sie diese an einem sicheren Ort: Einem PC ohne Internetanbindung, einem Stick, einer externen Festplatte, einem Ordner, den Sie in den Safe legen und die Datei auf dem Rechner löschen.
Ein Passwort-Manager ist eine Option für die digitale Aufbewahrung, allerdings muss das Master-Passwort überaus komplex sein, damit im Falle eines Cyberangriffs nicht alle Daten in die Hände von Kriminellen fallen.
Nachdem Sie einen Passwort-Manager installiert haben, müssen Sie für jedes Ihrer Benutzerkonten den verwendeten Benutzernamen, die zugehörigen Kennwörter, eine Bezeichnung für das Benutzerkonto (bzw. den Webdienst) sowie ggf. weitere Informationen wie z. B. die Webadresse in die Datenbank eintragen. Diese Kennwortdatenbank ist durch ein Hauptkennwort gesichert (verschlüsselt).

Ganz ähnlich wie ein Telefonbuch genutzt wird, um Kontakte anzurufen, unterstützen die meisten Passwort-Manager einen automatisierten Login bei Online-Diensten und Web-Portalen. Dementsprechend sollte es sich beim Hauptkennwort um ein starkes Kennwort handeln. Gegebenenfalls lässt sich die Sicherheit durch eine zusätzliche Schlüsseldatei oder durch Zwei-Faktor-Authentifizierung (2FA) weiter erhöhen.
Gesichert werden sollte das Hauptkennwort nicht auf dem Rechner, auf dem sich die Datenbank des Passwort-Managers befindet. Nutzen Sie hierfür einen Stick, den Sie ebenfalls veschlüsseln können.
In Passwort-Manager integriert ist meist auch ein Kennwortgenerator, mit dem verschieden starke Kennwörter zufällig generiert werden können. Unter Umständen erstellt dieser auf Grundlage der zufälligen Eingabe des Benutzers mit Maus

Zum digitalen Nachlass gehören:

- Social Media (WhatsApp, Facebook, Instagram, TicToc …)
- Messenger-Dienste
- Online-Konten (bei Internet-Providern, Versicherungen, Banken, Bezahldiensten wie Paypal, Shops, dem Finanzamt, der Krankenkasse ….)
- Smart Home Anwendungen (Alarmanlage, Staubsauger, Küchengeräte, Rollladen, Rasenmäher, Klimaanlagen, Licht, Musik …)
- Cloud Dienste
- Smartphone, Tablett, PC, Laptop
- Internetdomains
- Blogs

Einen Überblick gibt es z.B. hier:

oder Tastatur Kennwörter mit beliebiger Länge und verschiedenen Zeichensätzen. Leicht lassen sich Kennwörter mit 100 und mehr Bit erstellen. Diese starken Kennwörter mit 15 und mehr Zeichen sind dann allerdings nur noch mit einer Kennwortverwaltung praktikabel verwendbar.

Eigene Maßnahmen

Sie sollten auch auf den Anbieterseiten prüfen, ob es dort Vorsorgeregelungen gibt. Der **Kontoinaktivität-Manager** bei **Google** bietet z.B. verschiedene Optionen: Vom Löschen bei einer bestimmten Zeit der Inaktivität bis zur Information an von Ihnen festgelegte Personen bei Inaktivität.

Bei **Facebook** können Sie einen Nachlasskontakt festlegen, der das Profil löschen oder in den Gedenkmodus setzen kann.

Urteil: Schon 2018 hat der Bundesgerichtshof entschieden, dass Erben ein Zugriffsrecht auf das Facebook-Konto des Verstorbenen haben, aber sie keine Inhalte verändern dürfen. Auch dürfe nichts hinzugefügt werden; lediglich das Lesen sei erlaubt. (AZ. III ZR 183/17)

Apple bietet einen beschränkten Zugriff, wenn Nachlasskontakte angegeben wurden, die einen Zugangsschlüssel besitzen und eine Kopie der Sterbeurkunde vorlegen können.

Testament

In einem allgemeinen Testament können natürlich auch Verfügungen über den digitalen Nachlass getroffen werden. Diese Festlegungen können von den Erben nicht ohne Weiteres ignoriert werden.

Sie können auch zusätzlich Vorsorgevollmachten ausstellen, die für unterschiedliche Bereiche und auch verschiedene Personen gültig sind. Diese Vollmachten sind sehr flexibel und können auch weiter eingeschränkt werden: *zu Lebzeiten, wenn keine eigene Entscheidung mehr möglich ist, über den Tod hinaus.*

Was z.B. kann vererbt werden?

Software, die käuflich erworben wurde, darf weiterverkauft werden, solange die Zahl der erworbenen Lizenzen nicht überschritten wird. In den meisten Fällen muss sie - nach dem Speichern der Programmdatei - deinstalliert werden und kann dann verkauft werden.

Kryptowährungen (z.B. Bitcoins) können vererbt werden. Benötigt werden von den Erben das Wallet (die verschlüsselten Daten) und der Private Key, der den Zugriff ermöglicht.

Ebooks können in der Regel nicht vererbt werden, da die Käufer/Leser mit dem Kauf nur ein einfaches, persönliches Nutzungsrecht erwerben. Wenn Ihre Erben die Bibliothek weiterhin nutzen möchten, dann können sie dies nur unter Ihrem Namen und mit Ihren Zugangsdaten.

Wer ist berechtigt?

Berechtigt, sich um den digitalen Nachlass zu kümmern, sind alle, die von Ihnen bevollmächtigt werden - und die Erben.

Wenn Sie nichts festlegen, dann wird der digitale Nachlass wie ein analoger Nachlass behandelt. Für die Erben dürfte es dann aber kompliziert werden, wenn sie keine Zugangsdaten haben und vielleicht gar nicht wissen, wo überall Konten geführt werden. Die Dienstanbieter sind verpflichtet, Auskunft zu geben, aber dies dauert, und es müssen Nachweise beigebracht werden.

Die Bevollmächtigten können entscheiden, was sie mit den Daten machen, wenn Sie keine Vorgaben gemacht haben:

- Nicht mehr genutzte Konten sollten gelöscht werden.
- Abonnements, die nicht mehr benötigt werden, sollten gekündigt werden, damit nicht weiterhin Geld abgebucht wird. Auch kommt es zu Problemen, wenn die Bankkonten aufgelöst werden, da dann kein Geld mehr abgebucht werden kann.

Vor einer Löschung der Konten sollte eine Datensicherung erfolgen, denn gelöschte Konten lassen sich in der Regel nicht wieder herstellen. Im Falle von Geldanlagen in Kryptowährungen kann dies beispielsweise fatal sein.

Erben müssen das gesamte Erbe annehmen oder ausschlagen. Bevollmächtigte können es ablehnen, sich um den digitalen Nachlass zu kümmern. Hier sind im Vorfeld klare Absprachen erforderlich.

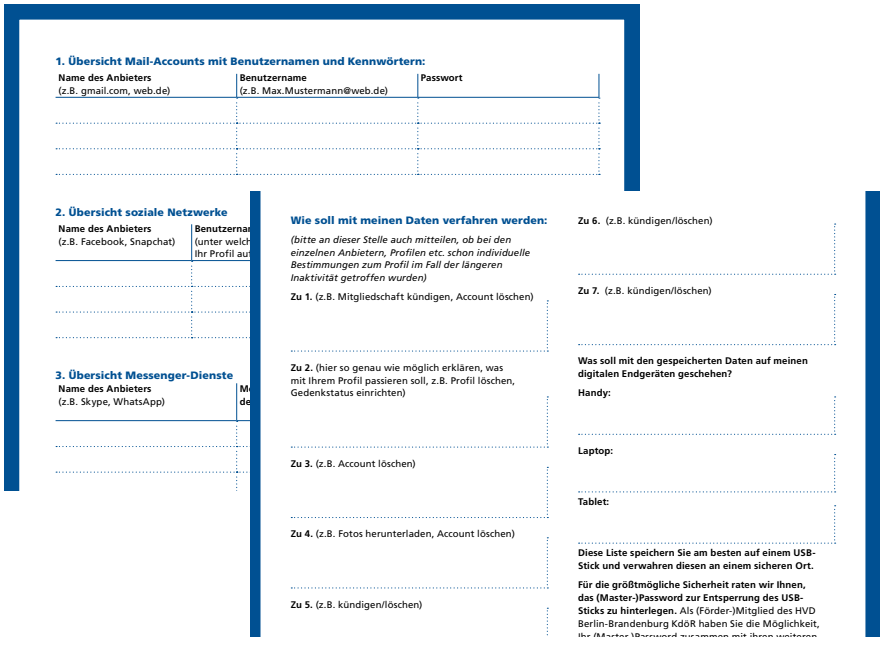
Zusammenfassung

1.) Eine Vertrauensperson als Nachlassverwalter auswählen.
2.) Dem Verwalter eine Vollmacht *„über den Tod hinaus“* ausstellen und festlegen, ob er auch schon zu Lebzeiten handeln darf, wenn man selbst nicht mehr dazu in der Lage sein sollte.
3.) Legen Sie eine geordnete Liste aller Accounts an (vom Streaming, über Banking, bis zu Social Media und Abonnements). Achten Sie darauf, dass die Liste regelmäßig aktualisiert wird. Die Liste kann analog auf Pa_ pier angelegt werden oder mit Hilfe eines Passwortmanagers.
4.) Bewahren Sie diese Liste - ob auf Papier oder als Stick - an einem sicheren, aber leicht zugänglichen (wegen der Aktualisierungen) Ort auf und teilen Sie dem Nachlassverwalter den Ort mit.

Vergessen Sie Ihre privaten Daten nicht, auch hier sollten Sie festlegen, was mit ihnen passieren soll.

Sie können weitere Informationen in der Geschäftsstelle abrufen: Listen, die Ihnen das Zusammenstellen der Zugangsdaten für die Accounts erleichtern, und ausführlichere Informationen zum Thema als pdf. Melden Sie sich bei Natasa Röhle, natasa.roehle@zhh.de.

Quellen (u.a.):
- Zentrum für europäischen Verbraucherschutz, 2023
- HVD_ Vollmacht_Digitales Erbe, 2019
- Erben und Vererben, 2024
- https://www.ecommerce-verbindungsstelle.de/internet-auftritt/digitaler-nachlass.html



1. Übersicht Mail-Accounts mit Benutzernamen und Kennwörtern:

Name des Anbieters (z.B. gmail.com, web.de)	Benutzername (z.B. Max.Mustermann@web.de)	Passwort

2. Übersicht soziale Netzwerke

Name des Anbieters (z.B. Facebook, Snapchat)	Benutzernam (unter welch Ihr Profil au

3. Übersicht Messenger-Dienste

Name des Anbieters (z.B. Skype, WhatsApp)	M de

Wie soll mit meinen Daten verfahren werden:

(bitte an dieser Stelle auch mitteilen, ob bei den einzelnen Anbietern, Profilen etc. schon individuelle Bestimmungen zum Profil im Fall der längeren Inaktivität getroffen wurden)

Zu 1. (z.B. Mitgliedschaft kündigen, Account löschen)

Zu 2. (hier so genau wie möglich erklären, was mit Ihrem Profil passieren soll, z.B. Profil löschen, Gedenkstatus einrichten)

Zu 3. (z.B. Account löschen)

Zu 4. (z.B. Fotos herunterladen, Account löschen)

Zu 5. (z.B. kündigen/löschen)

Zu 6. (z.B. kündigen/löschen)

Zu 7. (z.B. kündigen/löschen)

Was soll mit den gespeicherten Daten auf meinen digitalen Endgeräten geschehen?

Handy:

Laptop:

Tablet:

Diese Liste speichern Sie am besten auf einem USB-Stick und verwahren diesen an einem sicheren Ort.

Für die größtmögliche Sicherheit raten wir Ihnen, das (Master-)Password zur Entsperrung des USB-Sticks zu hinterlegen. Als (Förder-)Mitglied des HVD Berlin-Brandenburg KdöR haben Sie die Möglichkeit,