

Willkommen beim...

Digitaler Nachlass

Bettina Steffens | Referentin am Landesmedienzentrum im Bereich Medienbildung

18.09.2025

Zunehmende Digitalisierung begegnet uns z.B.



1. Gesundheitswesen

- › Elektronische Patientenakte (ePA), Telemedizin

2. Medienkonsum

- › eZeitung, eBooks, Streaming-Dienste

3. Finanzen

- › Digitale Rechnungen

4. Mobilität

- › Digitale Bahncard, E-Ticketing

5. Kommunikation

- › Messenger-Dienste, Videokonferenzen

6. Alltag

- › Smart Home, Online-Einkauf

Zunehmende Digitalisierung

Vor und Nachteile 2. Medienkonsum

Beispiel eZeitung

› Vorteile:

- › Zugang zu aktuellen Nachrichten jederzeit und überall.
- › Möglichkeit, Artikel zu speichern oder zu teilen.

› Herausforderungen:

- › Gewöhnung an digitale Lesegeräte (Tablets, E-Reader).
- › Anderes Lesen, mögliche Sehprobleme bei Bildschirmen.

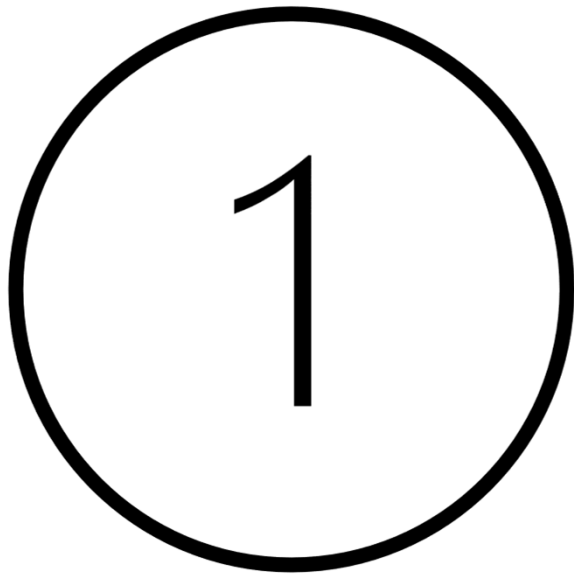


Ihre Gedanken, Fragen oder Wünsche zum
Thema?



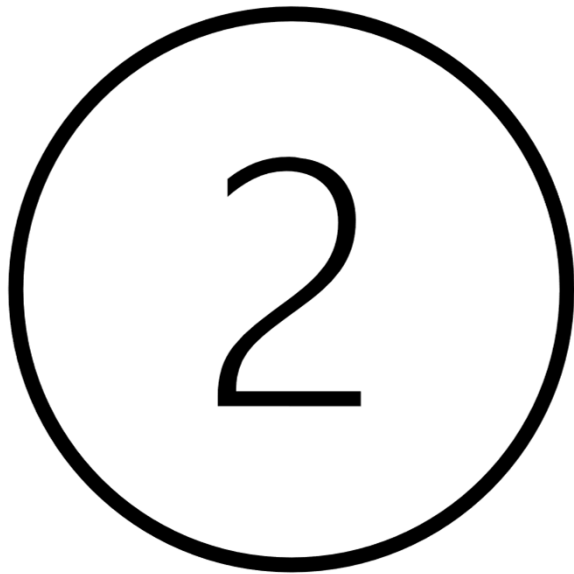
Das Digitale Erbe/Digitaler





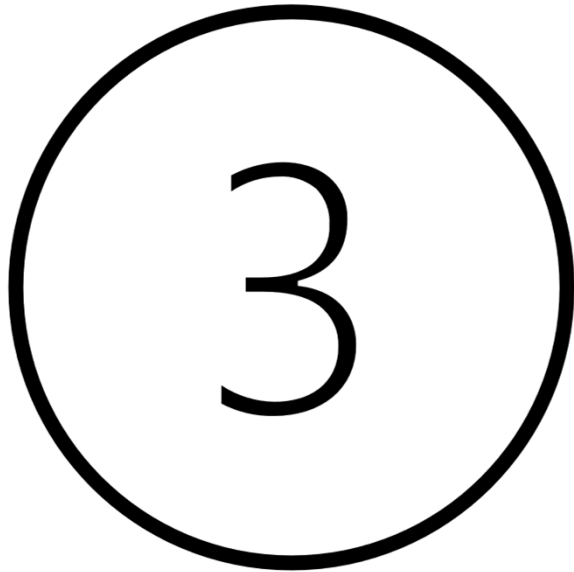
Digitaler Nachlass umfasst:

- › **alle digitalen Daten und Konten**, die eine Person während ihres Lebens angesammelt hat.
- › Dazu gehören E-Mail-Konten, Apps, soziale Medien, Cloud-Speicher, Online-Banking und andere digitale Dienste.



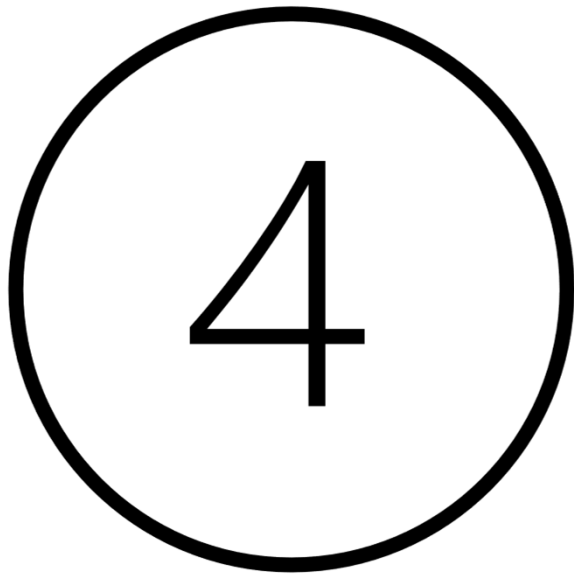
Inventarisierung

- › Erstellen Sie eine **Liste** aller **digitalen Konten und Dienste**, die Sie nutzen.
- › Notieren Sie die Zugangsdaten (Benutzername, Passwort) und speichern Sie diese sicher.



Vollmacht

- › Erteilen Sie einer **vertrauenswürdigen Person eine Vollmacht**, um auf Ihre digitalen Konten zugreifen zu können.
- › Stellen Sie sicher, dass die Vollmacht klar und präzise formuliert ist und alle notwendigen Informationen enthält.



Rechtliche Aspekte

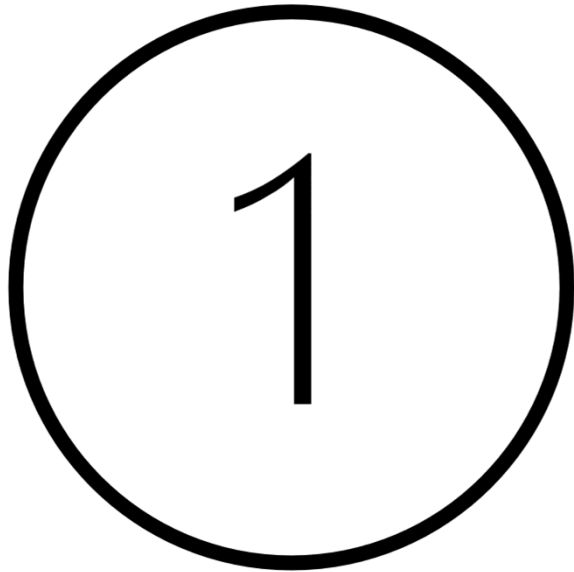
- › **Informieren Sie sich über die rechtlichen Bestimmungen** in Ihrem Land bezüglich des digitalen Nachlasses.
- › Stellen Sie sicher, dass die Vollmacht rechtlich bindend ist und auch nach Ihrem Tod gültig bleibt.



Austausch mit der bevollmächtigten Person

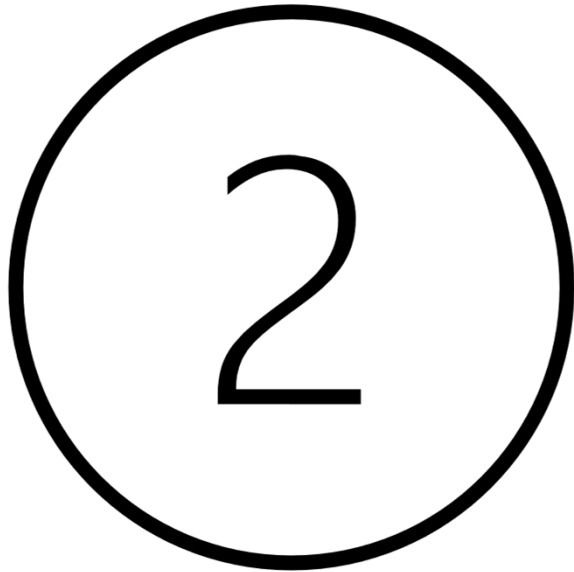
- › **Besprechen Sie mit der bevollmächtigten Person**, wie sie mit Ihrem digitalen Nachlass umgehen soll.
- › Geben Sie klare Anweisungen, welche Konten geschlossen, welche Daten gelöscht und welche Konten weitergeführt werden sollen.

Beispiele für eine Vollmacht für ein digitales Erbe



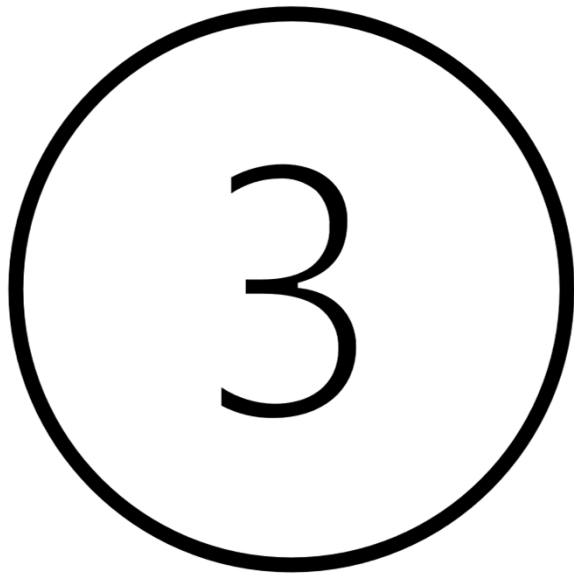
Persönliche Daten

- › Name, Vorname **des Vollmachtgebers**
- › Geburtsdatum und Geburtsort
- › Adresse
- › Telefon- und Mobilnummer
- › E-Mail-Adresse



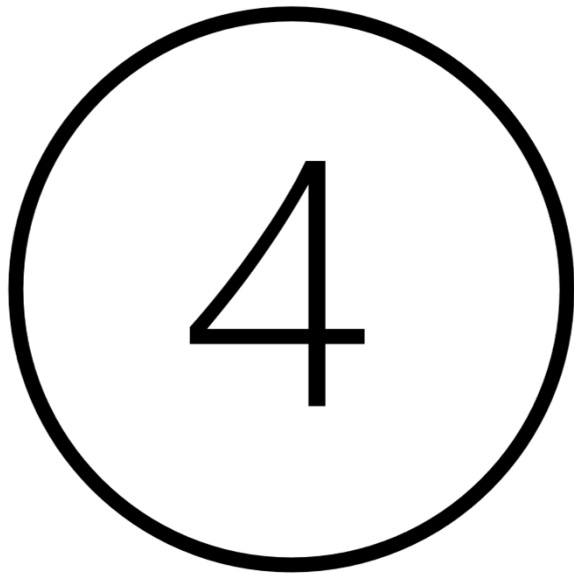
Persönliche Daten

- › Name, Vorname der **bevollmächtigten Person**
- › Geburtsdatum und Geburtsort
- › Adresse
- › Telefon- und Mobilnummer
- › E-Mail-Adresse



Bevollmächtigung

- › **Klare Formulierung**, dass die bevollmächtigte Person berechtigt ist, auf alle digitalen Konten und Daten des Vollmachtgebers zuzugreifen
- › **Hinweis auf die hinterlegte Übersicht** der Accounts und den Aufbewahrungsort dieser Übersicht.



Gültigkeit der Vollmacht

- › Festlegung, dass die **Vollmacht nur wirksam** ist, solange die bevollmächtigte Person das Dokument im Original besitzt und vorlegen kann.
- › Festlegung, dass die **Vollmacht über den Tod des Vollmachtgebers hinaus gültig** bleibt.

Ort, Datum, Unterschrift

Beispiel:



Die benannte Person wird hiermit bevollmächtigt, mit meinem digitalen Erbe zu verfahren, wie ich es in der hinterlegten Übersicht meiner Accounts detailliert aufgeführt habe.

Die bevollmächtigte Person kennt den Aufbewahrungsort der Übersicht.

Diese Vollmacht ist nur wirksam, solange die bevollmächtigte Person dieses Dokument im Original besitzt und vorlegen kann.

Diese Vollmacht gilt über meinen Tod hinaus.

Ort, Datum

Unterschrift
des Vollmachtgebers

Vollmacht für mein Digitales Erbe

Ich _____ Vollmachtgeber/Vollmachtgeberin
(NAME, VORNAME)

Geburtsdatum Geburtsort

Adresse

Telefon

Mobil-Nummer E-Mail-Adresse

erteile hiermit die Vollmacht an

Name, Vorname (bevollmächtigte Person)

Geburtsdatum Geburtsort

Adresse

Telefon

Mobil-Nummer E-Mail-Adresse

Die benannte Person wird hiermit bevollmächtigt, mit meinem digitalen Erbe zu verfahren, wie ich es in der hinterlegten Übersicht meiner Accounts detailliert aufgeführt habe.
Die bevollmächtigte Person kennt den Aufbewahrungsort der Übersicht.
Diese Vollmacht ist nur wirksam, solange die bevollmächtigte Person dieses Dokument im Original besitzt und vorlegen kann.
Diese Vollmacht gilt über meinen Tod hinaus



Ort, Datum Unterschrift

Zum Beispiel:
https://www.patientenverfuegung.de/wp-content/uploads/2024/03/HVD_Vollmacht_DigitaleErbe_2019.pdf



Wofür braucht man ein Digitales Erbe?

1. E-Mail-Konten und Clouds
2. Sozialen Netzwerken und Messengern
3. Freundschafts- und Partnerbörsen
4. Online-Kaufhäusern, Tauschbörsen und Auktionen
5. Online-Banken, Online-Bezahlssystemen und Aktiendepots
6. Kommunikations- und Mobilitätsanbietern
7. Foto-, Video- und Streaming-Diensten
8. Prämiensystemen (PayBack)
9. Online-Spielen
10. bei Apps für Fitnessarmbänder, Smart-Home-Systemen
11. weiteren Plattformen z.B. Verein, Freizeit, Handwerker...

Digitales Erbe, was ist zu tun?

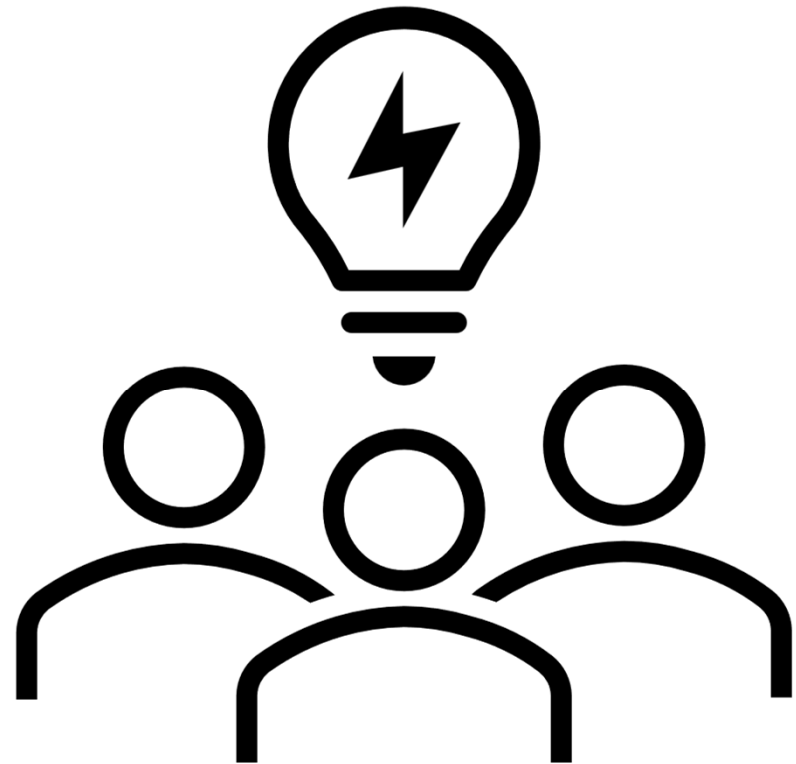
- › Beauftragen Sie eine vertraute Person mit der Verwaltung Ihrer Konten nach Ihrem Tod.
- › Erstellen Sie eine handschriftliche und unterzeichnete Vollmacht, welche über den Tod hinaus gilt.
- › Darauf sind alle notwendigen Zugänge (Passwörter, Benutzernamen, usw.).
- › Liste erstellen mit allen Daten und Forderungen, was mit den Konten passieren soll.
- › Überreichen Sie diese der Person.
- › Speichern Sie auf einem USB-Stick alle Informationen im PDF-Format, legen Sie diesen an einen sicheren Ort.

Beispiele digitales Erbe

Portal	URL	Benutzer-name	Passwort	Die bevollmächtigte Person soll wie folgt mit meinen Daten verfahren:
GMX	www.gmx.de	Meine.Mail	Entenhausen_99	Profil löschen.
Facebook	www.Facebook.de	Mein.Name	Kassen_bon!1!9! 9	www.gmx.de
WhatsApp	Auf dem Smartphone			Kontakte informieren, dann Profil löschen inklusive aller Daten
Eigene Webseite	www.MeineSeite123.de	Meine.Seite	35234tgwtg//&ha ha	Ansprechpartner informieren und Webseite löschen lassen Kontakt: Webseiten Horst, E-Mail: Horst@Webseite.de ; Tel. 049-123456789

Datenschutz und Datensicherheit

Datenschutz und
Datensicherheit
was ist der
Unterschied?



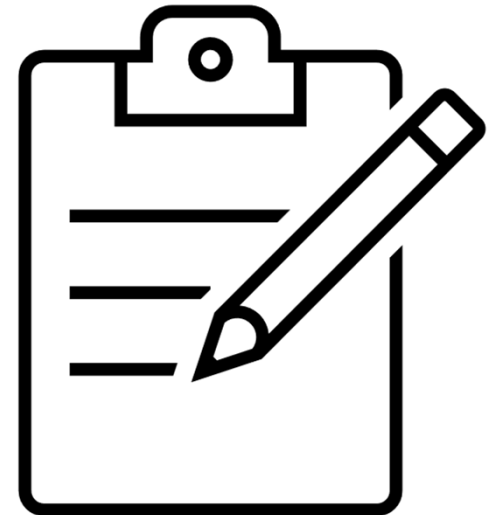
In der gesamten EU gilt die Datenschutzgrundverordnung (kurz: DSGVO).

Diese Gesetze bilden die Rahmung für den Datenschutz, die Erhebung von Daten und die Weitergabe von Daten.

1. Recht auf Auskunft: Sie können jederzeit nachfragen, welche Daten über Sie gesammelt wurden und warum.
2. Recht auf Löschung: Sie können verlangen, dass Ihre Daten gelöscht werden, wenn sie nicht mehr benötigt werden.
3. Datensicherheit: Ihre persönlichen Informationen müssen sicher aufbewahrt werden, damit niemand Unbefugtes darauf zugreifen kann.

Kurz zusammengefasst Unterschied zw. Datenschutz u. Datensicherheit

- › **Datenschutz:** Persönliche Daten werden geschützt und nicht ungefragt von Unternehmen weitergegeben
- › **Datensicherheit:** Persönliche Daten werden technisch (bspw. durch Passwörter) durch Sie gesichert – oder von Unternehmen, die Ihre Daten verarbeiten.



Sicherheitsmaßnahmen Tipps

1

- › Nutzen Sie sichere Passwörter und aktivieren Sie die Zwei-Faktor-Authentifizierung, um den Zugang zu Ihren Konten zu schützen.
- › Bewahren Sie die Liste der Zugangsdaten an einem sicheren Ort auf, der nur von der bevollmächtigten Person zugänglich ist.

Passwort Generator: Schnell & einfach ein sicheres Passwort generieren

Von [Jan Frederik Strasmann, LL. M.](#)

Letzte Aktualisierung am: 3. Juli 2025

Geschätzte Lesedauer: 8 Minuten



Kommentare



Sicherheitsmaßnahmen Tipps

2

In wenigen Schritten zum sicheren Passwort

Sie haben zwei Strategien zur Wahl

Langes und weniger komplexes Passwort

Nutzen Sie ein langes Passwort (mindestens 25 Zeichen), brauchen Sie nur zwei Zeichenarten, z.B. Groß- und Kleinbuchstaben.

Umsetzungsbeispiel: tisch_himmel_kenia_blau_pfanckuchenteig_lachen

Kürzeres und komplexes Passwort

Nutzen Sie ein kurzes Passwort (mindestens acht Zeichen), sollten Sie vier Zeichenarten kombinieren (Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen).

Umsetzungsbeispiel: q7yPv8!x\$B



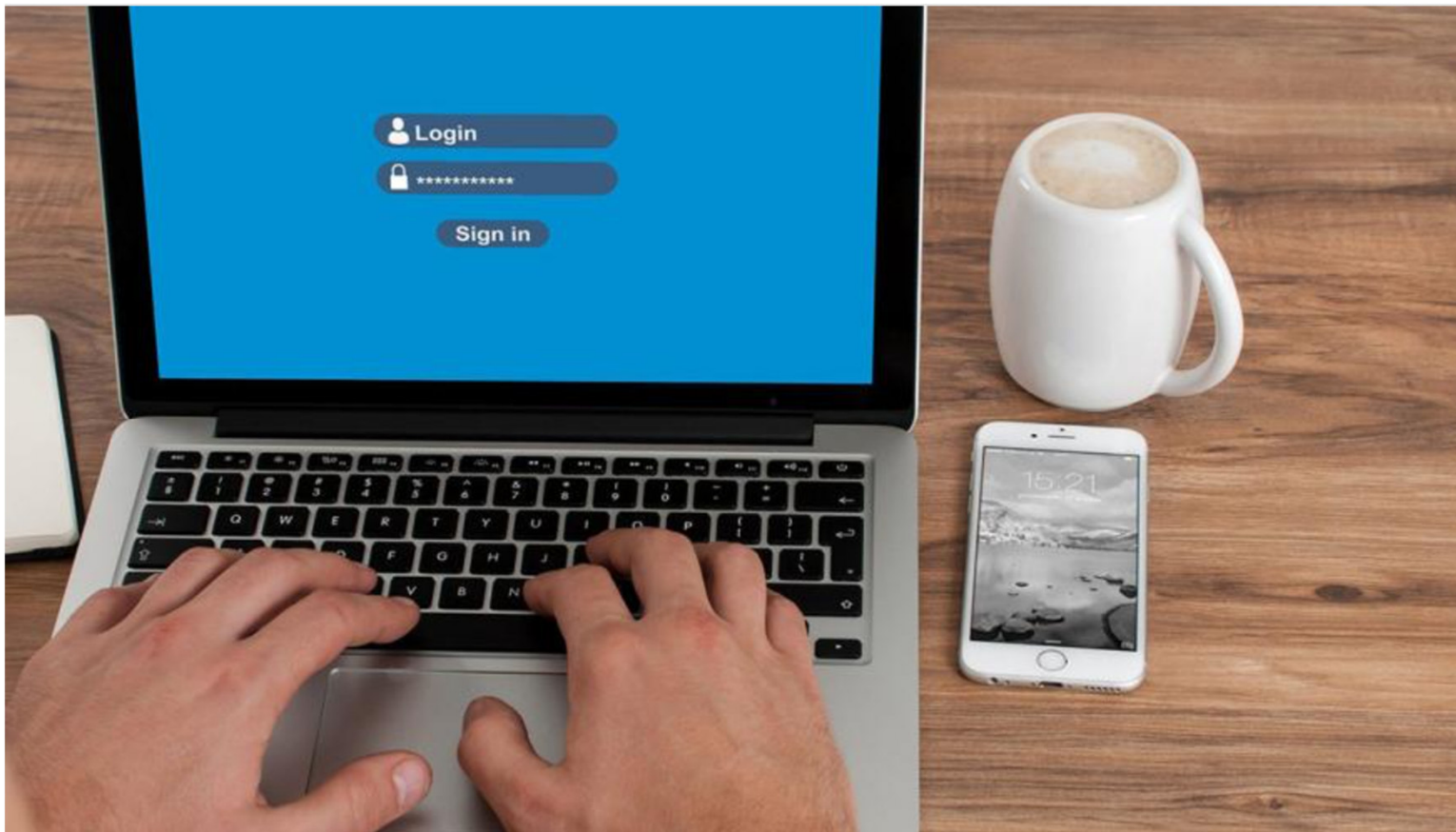
© Bundesamt für Sicherheit in der Informationstechnik

www.bsi.bund.de



Sicherheitsmaßnahmen Tipps

3



<https://tinyurl.com/2rjnx4pm>

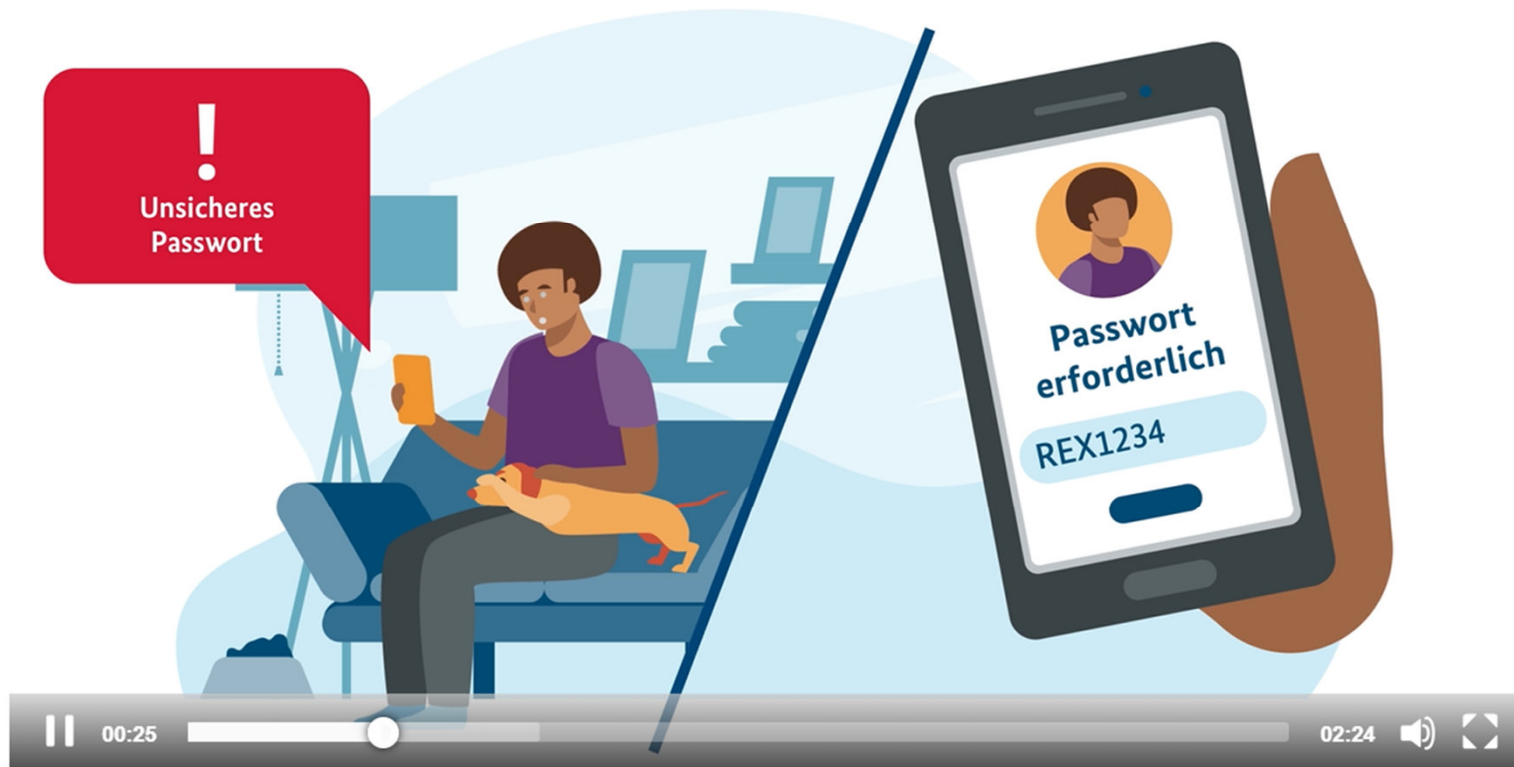
www.lmz-bw.de

Wie sieht ein sicheres Passwort aus?

Ihre Meinung ist gefragt!

Sicherheitsmaßnahmen Tipps

4



<https://tinyurl.com/3czfvcn8>

Tipps für ein sicheres Passwort

Das Passwort sollte **mindestens acht Zeichen** lang sein.

Kombination von **großen und kleinen Buchstaben, Zahlen und Sonderzeichen**.

Kreativer und komplexer das Passwort desto besser.

Es sollte so sein, dass Sie es sich **gut merken können**, es aber für andere schwer zu knacken ist.

Eselsbrücken oder Hilfestellungen basteln, um sich die Passwörter leichter zu merken.

Einen Satz überlegen und dann nur die Anfangsbuchstaben jedes Wortes zu einem langen Passwort zusammenzufügen.

Beispiel: „Heute gehe ich mit einer Freundin zu einem Spieleabend für Senioren = „Hgim1Fz1SfS!“

Satz als ein Wort: Beispiel: Heutegeheichmit1Freundinzu1SpieleabendfürSenioren!

Für verschiedene Konten, verschiedene Passwörter nutzen.

Das erschwert es Zugriff auf alle Ihre Konten zu bekommen.

Sicherheitsmaßnahmen Tipps

5

Ein sicheres Passwort baut man am leichtesten mit
Eselsbrücken:

Überlegen Sie sich einen Satz, der Ihnen immer einfallen wird,
und nutzen Sie nur den ersten Buchstaben der einzelnen
Wörter sowie die Satzzeichen.

Das kann zum Beispiel so aussehen: **E**ine **k**leine **M**aus **n**agt
sich **d**urch **z**wei, **n**ein **d**rei, **g**roße **S**tücke **K**äse.

-> EkMnsd2,n3,gSK.



Passwort

WIE SICHER IST MEIN PASSWORT?

Probiere verschiedene Passwörter aus!

⚠ Aus Sicherheitsgründen solltest du nicht deine echten Passwörter eingeben.



„CheckDeinPasswort.de speichert keinerlei Daten und ist für Benutzer unbedenklich.“
RA Kai Schützle, Fachanwalt für IT-Recht

Du interessierst dich für Hacker und ihre Methoden?
Wir erklären dir: [Wie werden Passwörter geknackt?](#)



Sicherheitsregeln

Sicherheitsregeln im digitalen Alltag

› 1. **Nur das Nötigste preisgeben:**

- Geben Sie nur notwendige persönliche Informationen preis
- Veröffentlichen Sie keine sensiblen Daten (Adresse, Telefonnummer, etc.)

› 2. **Sichere Passwörter nutzen:**

- Verwenden Sie lange und komplexe Passwörter
- Ändern Sie Passwörter regelmäßig

› 3. **Zusätzliche Sicherheit:**

- Aktivieren Sie, wo möglich, die Zwei-Faktor-Authentifizierung

Sicherheitsregeln im digitalen Alltag

› **4. Regelmäßige Updates:**

- Aktualisieren Sie Ihr Betriebssystem und alle Programme
- Schließen Sie so Sicherheitslücken und vermeiden Sie Angriffe

› **5. Automatische Updates einrichten:**

- Nutzen Sie automatische Updates, wenn möglich

Sicherheitsregeln im digitalen Alltag

› **6. Regelmäßige Datensicherungen:**

- Erstellen Sie automatische Backups Ihrer Daten
- Nutzen Sie externe Festplatten oder vertrauenswürdige Cloud-Dienste

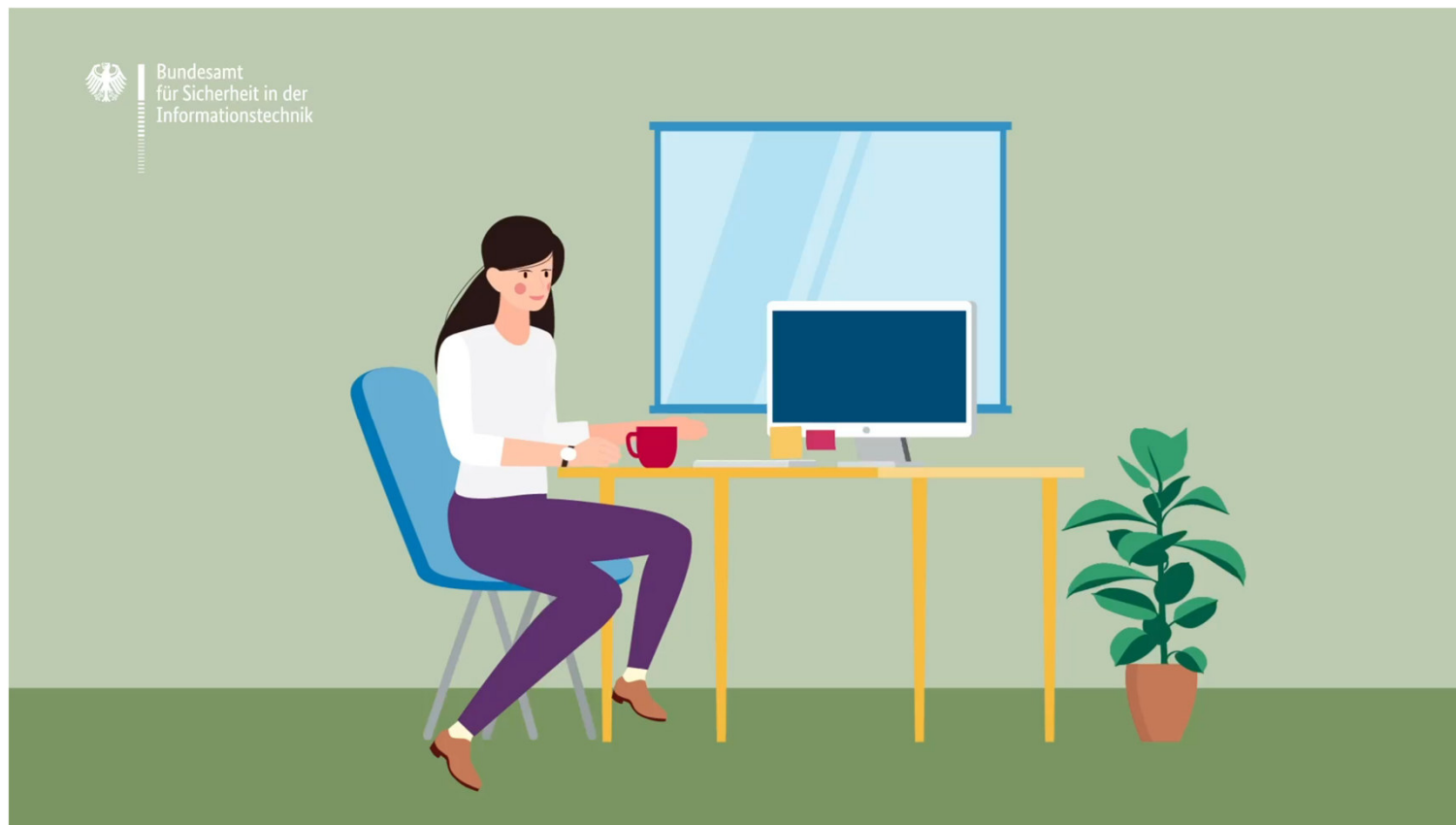
› **Vorteile von Backups:**

- Schnelle Wiederherstellung im Fall von Datenverlust oder Beschädigung

› **7. Umgang mit Links und E-Mails:**

- Öffnen Sie nur Links von vertrauenswürdigen Quellen
- Prüfen Sie Absenderadresse und URL **Schutz vor Betrug:**
- Seien Sie skeptisch gegenüber unbekannten oder verdächtigen Nachrichten

Zwei-Faktor-Authentisierung (2FA)



Zwei-Faktor-Authentifizierung (2FA)

- › Beispielweise bei PayPal oder Google Mail.
- › Bei erfolgreicher Eingabe des Passwortes wird ein Code an eine vom Besitzer des Kontos angegebene Handynummer versendet.
- › Nur mit dem Code kann man sich dann einloggen.
- › (Auch andere Zwei-Faktor-Authentifizierungsmethoden sind möglich, am gebräuchlichsten ist die Verifikation über eine SMS oder E-Mail)

Zwei-Faktor-Authentifizierung (2FA)

- › **Wo kommen diese Sicherheitsverfahren zum Einsatz?**
- › Online-Banking
- › Online-Ausweisfunktion des Personalausweises
- › Cloud-Anbieter
- › Mail-Anbieter
- › Soziale-Netzwerke
- › Steuererklärung (ELSTER)

Tipps & Kontaktdaten

Tipps

Ausführliche Informationen finden Sie unter:

- › <https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/digitale-vorsorge-digitaler-nachlass-was-passiert-mit-meinen-daten-12002>
- › Angebote für Seniorinnen und Senioren: <https://www.lmz-bw.de/seniorenangebote>
- › Seniorenbüros: https://www.rastatt.de/site/Rastatt-Stadt/get/params_E-600474546_Dattachment/3065226/Angebote%20des%20Senioren%C3%BCros%202025.pdf

Haben Sie noch Fragen? Oder
benötigen Sie weitere
Informationen?

Landesmedienzentrum Baden-
Württemberg

Rotenbergstraße 111

70190 Stuttgart

Senioren@lmz-bw.de

www.lmz-bw.de

Vielen Dank für's Mitmachen!

Bettina Steffens

Medienpädagogische Referentin

Landesmedienzentrum
Moltkestraße 64
76133 Karlsruhe

Telefon: [+49 711 2070-9893](tel:+4971120709893)

E-Mail: bsteffens@lmz-bw.de

