# Checklistenartiger Leitfaden

## zur Förderung von IT-Sicherheit sowie ethischer und datenschutzkonformer Gestaltung von Webportalen

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
INF FAKULTÄT FÜR INFORMATIK
AMSL Advanced Multimedia and Security Lab
SACHSEN-ANHALT
#moderndenken

„Checklistenartiger Leitfaden“ im Rahmen des Digitalisierungsprojektes „Technische Querschnittsziele in Medizin, Gesundheit und Soziales"



**Veröffentlicht am: 22.12.2023**

**Impressum:**
Fakultät für Informatik
Advanced Multimedia and Security
Institut für Technische und Betriebliche Informationssysteme
Otto-von-Guericke-Universität Magdeburg

Universitätsplatz 2
39106 Magdeburg
Germany

Tel.: +49 391 67-58965
Fax.: +49 391 67-48110
E-Mail: sec-by-design@iti.cs.uni-magdeburg.de
Internet: https://omen.cs.uni-magdeburg.de/itiamsl/deutsch/home/index.html

Das Projekt wird aus Mittel des Landes unterstützt.

**Projektvergabe durch:**
Ministerium für Arbeit, Soziales, Gesundheit und Gleichstellung des Landes Sachsen-Anhalt
Turmschanzenstraße 25
39114 Magdeburg

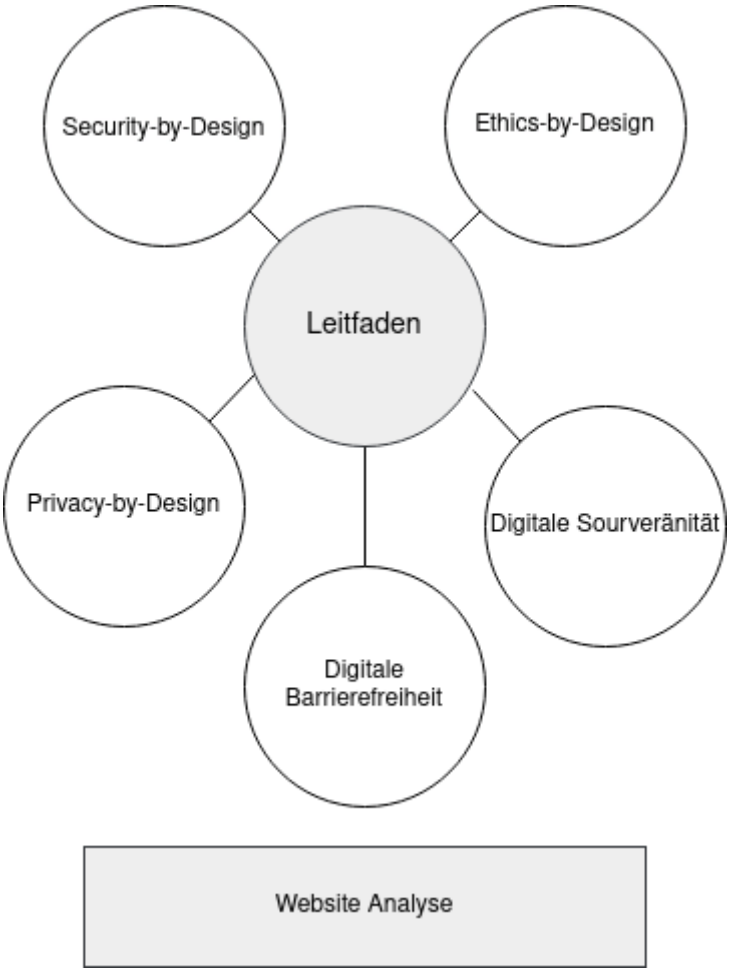
Telefon +49-(0)391-567-4612
E-Mail: ms-presse@ms.sachsen-anhalt.de
Internet: www.ms.sachsen-anhalt.de

Weitere Informationen zur Digitalisierung des Landes Sachsen-Anhalt unter www.mid.sachsen-anhalt/digitales/strategie-sachsen-anhalt-2030

# Inhaltsverzeichnis

# Vorwort

Die Digitalisierung bietet bspw. im Gesundheitswesen viele Chancen. Dazu gehören die medizinische Versorgung von Patientinnen und Patienten über große Distanzen hinweg oder die digitale Vernetzung von Akteuren.




Im Mittelpunkt stehen dabei stets die Bürgerinnen und Bürger. Sie treten oftmals über Webportale[1] mit Institutionen in den Dialog und teilen dabei viele – gerade in den Bereichen der Medizin, Gesundheit und Sozialem besonders sensible - Daten, die sorgfältig geschützt werden müssen. Der Schutz dieser Daten hat höchste Priorität und muss bereits in der Design-Phase bei der Erstellung eines Webportals bedacht werden. Hierfür ist es hilfreich sich an den Ansätzen Security by Design, Ethics by Design und Privacy by Design zu orientieren.

IT-Sicherheits- und Gewährleistungsziele von Anfang an mitzudenken, ist als Security by Design bekannt. Diese Ziele sind eng mit den technischen Querschnittszielen[2], bestehend aus Datenschutz, Digitale Souveränität, Informationelle Selbstbestimmung und Informationssicherheit, verbunden.

Diese wichtigen Aspekte werden auch durch die Strategie „Sachsen-Anhalt Digital 2030“[3] betont:

> *"Querschnittsziele, welche für die Digitalisierung des Landes und unser Handeln zentral sind, wie die Digitale Souveränität, „Risiken als Chancen zu verstehen“, IT-Sicherheit, Datenschutz, Barrierefreiheit, Ethik, Open Data sowie Open Source finden sich explizit in den strategischen Zielstellungen wieder. Ebenso streben wir danach die Verwaltungsdigitalisierung nachhaltig zu gestalten."*

Dies zeigt schon die große Bandbreite der miteinander verzahnten Aspekte und Herausforderungen für eine nachhaltige Digitalstrategie auf. Entsprechend greift auch dieses Dokument weitere Aspekte auf.

1 Bundesamt für Sicherheit in der Informationstechnik (2023): Abschlussbericht Projekt MaSiGov – Markt- und Schwachstellenanalyse zur Sicherheit von E-Government-Apps und Webportalen, Seite 6

2 Ministerium für Wirtschaft, Wissenschaft und Digitalisierung des Landes Sachsen-Anhalt (2021): Digitale Agenda für das Land Sachsen-Anhalt, Seite 53ff.

3 Ministerium für Infrastruktur und Digitales (Land Sachsen-Anhalt): Strategie „Sachsen-Anhalt Digital 2030“, https://mid.sachsen-anhalt.de/fileadmin/Bibliothek/Politik_und_Verwaltung/MLV/MID/Ministerium/Publikationen/Sachsen-Anhalt-Digital-2030.pdf

So ist Ethics by Design ein weiterer wichtiger Aspekt bei der Gestaltung eines Webportals. Ersteres bezieht sich auf die IT-Sicherheits- und Gewährleistungsziele vor und während eines Entstehungsprozesses. Als untergeordneter Punkt bezieht sich Ethics by Design auf die Berücksichtigung ethischer Überlegungen. Dazu gehören z.B. Aspekte wie Gender Mainstreaming, digitale Nachhaltigkeit, der verantwortungsbewusste Umgang mit Ressourcenverbrauch von und durch Technik und digitale Barrierefreiheit.

In den dritten Bereich Privacy by Design im Rahmen von Security by Design fallen nicht nur Drittanbieterfreiheit, welche u.a. die Datensparsamkeit und -souveränität unterstützen, sondern auch angestrebte Vorgaben, mit denen eine sichere Umgebung für Nutzende des Webportals umgesetzt werden soll. Dazu zählen z.B. Mindestanforderungen für Passwörter und eine verschlüsselte Kommunikation.

Auf den folgenden Seiten wird eine Auswahl an Aspekten gezeigt, die die oben genannten Ziele berücksichtigen soll, um sicherzustellen, dass bereits während der ersten Schritte eines Digitalisierungsprojektes die Bereiche IT-Sicherheit, Datenschutz als auch digitale Inklusion im Sinne der Nutzer:innen umgesetzt werden.

Dieser checklistenartige Leitfaden richtet sich vor allem an diejenigen, die an einem Projekt zur Gestaltung eines Webportals beteiligt sind und eine erste Orientierung zum Thema Security by Design, Ethics by Design und Privacy by Design suchen. Es unterstützt damit das in der Strategie „Sachsen-Anhalt Digital 2030“[4] unter Themenfeld 16: Digitale Gesundheitsversorgung, Pflege und Beratungsangebote beschriebene Vorhaben:

> *„Wir schaffen Instrumente, um die technischen Querschnittziele im Sinne von Security-by-Default und Privacy in Medizin, Gesundheit und Sozialem zu identifizieren und eine leichtere Umsetzung zu erreichen."*

Darüber hinaus kann der Leitfaden auch für Institutionen hilfreich sein, die bereits ein Webportal betreiben und dieses in Hinsicht auf IT-Sicherheit, Datenschutz und digitaler Inklusion verbessern möchten. Des Weiteren sind neben wichtigen Informationen über Best Practices auch exemplarisch ausgewählte praktische Tipps zu finden. Zusätzlich enthält das Dokument Vorlagen für eine Webportalanalyse, welche mit öffentlich zugänglichen Werkzeugen umgesetzt werden kann und zum Selbsttest an der eigenen Internetpräsenz anregen soll.

Da für den Bereich Gesundheitsversorgung, Pflege und Beratungsangebote die Querschnittziele besonders wichtig sind und Kommunikation sowie Daten als besonders schutzwürdig betrachtet werden, können auch andere Aspekte dieser Bereiche von dem Leitfaden profitieren und selektiv entsprechend des Schutzbedarfs geeignete Handlungsanleitungen finden, woraus sich eine allgemeine Nutzbarkeit ergibt.

Des Weiteren sind neben wichtigen Informationen über Best Practices auch exemplarisch ausgewählte praktische Tipps zu finden, die in unterschiedlichen Bereichen relevant sein können. Zusätzlich enthält das Dokument Vorlagen für eine Webportalanalyse, welche mit öffentlich zu-

4 Ministerium für Infrastruktur und Digitales (Land Sachsen-Anhalt): Strategie Sachsen-Anhalt Digital 2030, https://mid.sachsen-anhalt.de/fileadmin/Bibliothek/Politik_und_Verwaltung/MLV/MID/Ministerium/Publikationen/Sachsen-Anhalt-Digital-2030.pdf

gänglichen Werkzeugen umgesetzt werden kann und zum Selbsttest an der eigenen Internetpräsenz anregen soll.

Der checklistenartige Leitfaden betrachtet lediglich eine Auswahl wichtiger Schritte hin zu einem sicheren Webportal und erörtert beispielhaft, wie IT-Sicherheit ermittelt oder gefördert werden kann. Er ersetzt das aktuelle und umfangreiche Wissen eines IT-Sicherheitsexperten nicht.

Es ist weiter zu beachten, dass diese Zusammenfassung eine allgemeine unverbindliche Information darstellt. Die Inhalte sind exemplarisch ausgewählt, um allgemein den Handlungsbedarf sowie Gestaltungsmöglichkeiten zu motivieren.
Die angegebenen Werkzeuge sind Beispiele zur Illustration und bedürfen ebenfalls einer geeigneten Konfiguration. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf Vollständigkeit und/oder Aktualität, insbesondere kann diese Zusammenfassung nicht den besonderen Umständen des Einzelfalles Rechnung tragen und stellt keine Rechtsberatung im Einzelfall dar. Zur Lösung von konkreten Rechtsfällen konsultieren Sie bitte unbedingt vorher einen Rechtsanwalt. Eine Verwendung liegt daher in der eigenen Verantwortung der Lesenden/Hörenden.
Die Inhalte des Leitfadens sind auf Basis von wissenschaftlichen Veröffentlichungen zusammengetragen worden. Hierbei handelt es sich um Zitierungen und Auslegungen derer. Jegliche Haftung wird ausgeschlossen.

Für die angegebenen Werkzeuge/Tools/Tests erfolgt ebenfalls keine Haftung bei Schäden. Die Nutzung erfolgt auf eigenes Risiko. Achtung: Eine Konfiguration ist oftmals erforderlich. Lesen Sie deshalb vorher die Hinweise und Informationen dazu entsprechend.

# Motivation

Dem sicheren Design von Informationssystemen und insbesondere von Webportalen aus dem Bereich der Beratungsangebote sollte in einer zunehmend vernetzteren Gesellschaft, die beginnt wichtige Verwaltungsprozesse und Dienstleistungen zu digitalisieren, eine hohe Bedeutung beigemessen werden. Der Schutz der Daten aus dem Bereich Gesundheitsversorgung, Pflege und Beratungsangebote ist für Bürger:innen in vielerlei Hinsicht von höchster Bedeutung. Wird er verletzt, sind Bürger:innen betroffen und die verantwortlichen Institutionen ebenso. Die Folgen können z.B. Reputationsschäden oder rechtliche Konsequenzen sein und mit einem nachhaltig verletzten Vertrauensverhältnis zu Nutzer:innen einhergehen.

Im Bereich Gesundheitsversorgung, Pflege und Beratungsangebote sind die Querschnittziele besonders wichtig und sowohl Kommunikation als auch Daten als besonders schutzwürdig zu betrachten. Dennoch können die in diesem Leitfaden vorgestellten Punkte auch in anderen Bereichen angewendet werden um selektiv entsprechend des Schutzbedarfs geeignete Handlungsanleitungen zu finden, wodurch sich eine allgemeine Nutzbarkeit ergibt.

Die Situation um die allgemeine IT-Sicherheit für Behörden und kritische Infrastruktur zeigt sich nicht nur zum Beispiel durch Cyber-Angriffe wie im Landkreis Anhalt-Bitterfeld in Sachsen-Anhalt[5] oder auf Industrieunternehmen, sondern auch bei jenen auf Verkehr, Kommunikation und andere Dienstleister (beispielsweise Krankenkassen[6]), sodass die Konsequenzen jeden treffen können. Die Angriffe erfolgen dabei systematisch und sind professionell organisiert[7]. Daher sind auch andere Institutionen wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) bestrebt, Apps und Webportale für eine bessere IT-Sicherheit auf Schwachstellen zu prüfen[8].

Neben Datenschutz und -sicherheit soll möglichst eine hohe Datensouveränität erreicht werden. Durch die Integration von Drittanbieteranwendungen in die eigene Website, können erhebliche Risiken für die Privatsphäre der Nutzenden entstehen. Jede Verarbeitung von Daten bei Dritten birgt das Risiko, dass die Datenhoheit und die Kontrolle über die Daten eingeschränkt und/oder verletzt wird. Das Ausmaß einer Kategorisierung von Daten, die beispielsweise für digitale Werbung weiterverwendet werden sollen, ist alarmierend und sollte zur Vorsicht bei der Auswahl und Integration von Drittanbietern aufrufen[9].

Neben den genannten technischen Querschnittszielen, bezieht der Leitfaden auch ethische Ansätze wie z.B. Nachhaltigkeit und digitale Inklusion ein, die im Bereich Gesundheitsversorgung, Pflege und Beratungsangebote ebenfalls sehr bedeutsam sind. So unterstützt digitale Barrierefreiheit, als Teil der Inklusion, dass Menschen mit unterschiedlichen Fähigkeiten, unab-

5 DW (2021): Cyberattacke legt Landkreis lahm, https://www.dw.com/de/katastrophenfall-cyberattacke-legt-landkreis-lahm/a-58227033, letzter Aufruf 23.05.2023

6 Tagesschau (2023): Cyberangriff auf Krankenkassen-Dienstleister, https://www.tagesschau.de/wirtschaft/unternehmen/bitmarck-cyberattacke-krankenkasse-100.html, letzer Aufruf 23.05.2023

7 Europäische Kommission (2022): Crime as a service, https://cordis.europa.eu/programme/id/HORIZON_HORIZON-CL3-2023-FCT-01-05, letzter Aufruf 22.08.23

8 Bundesamt für Sicherheit in der Informationstechnik (2023): Abschlussbericht Projekt MaSiGov – Markt- und Schwachstellenanalyse zur Sicherheit von E-Government-Apps und Webportalen, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Oeffentliche_Verwaltung/Abschlussbericht_MaSiGov.pdf?__blob=publicationFile&v=5, letzter Aufruf 22.09.23

9 Dachwitz, Ingo (2023): Microsofts Datenmarktplatz Xandr - Das sind 650.000 Kategorien, in die uns die Online-Werbeindustrie einsortiert, https://netzpolitik.org/2023/microsofts-datenmarktplatz-xandr-das-sind-650-000-kategorien-in-die-uns-die-online-werbeindustrie-einsortiert/, letzter Aufruf 15.06.2023

hängig von physischen oder kognitiven Einschränkungen, gleichberechtigt an der digitalen Welt teilhaben können. Die Gestaltung von Technologien sollte nicht ausschließlich darauf abzielen Innovationen voranzutreiben, sondern sollte auch immer von Anfang an dafür Sorge tragen, dass keine Barrieren in der Bedienung zwischen Technik und Nutzer:innen bestehen. Es ist wichtig zu betonen, dass die digitale Barrierefreiheit nicht nur eine ethische Verpflichtung ist, sondern auch gesetzlich verankert. Normen wie die Europäische Norm 301 549[10] und die Web Content Accessibillity Guidlines (WCAG)[11] legen hierfür klare Standards fest, die sicherstellen, damit Technologien für alle zugänglich sind.

Zusätzlich zur Barrierefreiheit ist auch Gender Mainstreaming ein wesentlicher Aspekt der digitalen Inklusion. Gender Mainstreaming bedeutet, Geschlechterperspektiven von Anfang an in die Gestaltung einzubeziehen, um Gleichberechtigung und -stellung sicherzustellen, wodurch die vielfältigen Bedürfnisse erkannt werden und adäquate Lösungen gefunden werden können.

Zuletzt sei empfohlen, den folgenden checklistenartigen Leitfaden nicht zu einer einmaligen Verwendung heranzuziehen. IT-Sicherheit ist kein Zustand, den es einmalig zu erreichen gilt. Bedrohungen und Angreifende werden raffinierter, Informationssysteme wachsen um technische Komponenten oder Verbindungen und Technologie schreiten mit beispielsweise jüngsten Fortschritten in der Künstlichen Intelligenz voran, sodass sich die Bedrohungslage ständig verändert. Aus diesen Gründen beschäftigen sich auch eine Vielzahl von Institutionen wie bspw. das BSI mit Checklisten zu IT-Grundschutz[12], welche zur unterstützenden Orientierung dienen sowie Relevanz und Bedarf an Hilfsmitteln für eine sichere, datenschutzkonforme und ethische IT unterstreichen, die sich stets im Wandel befindet. Es ist also wichtig, dass IT-Sicherheit in den Organisationen und Institutionen gelebt, sowie periodisch geprüft und an neue Situationen angepasst wird. Der Leitfaden soll dafür als Einstieg für eine erfolgreiche IT-Sicherheit, als auch für höheren Datenschutz und eine verbesserte digitale Barrierefreiheit von Webportalen genutzt werden, sowie bei der Gleichstellung von Geschlechtern in der Gestaltung unterstützen.

10 ETSI (2021): EN 301 549 Accessibility requirements for ICT products and services, https://www.etsi.org/deliver/etsi_en/301500_301599/301549/03.02.01_60/en_301549v030201p.pdf, letzter Aufruf 28.08.23

11 Beauftragte der Bundesregierung für Informationstechnik (o.J.): Harmonisierte Europäische Norm (EN) 301 549, https://www.barrierefreiheit-dienstekonsolidierung.bund.de/Webs/PB/DE/gesetze-und-richtlinien/en301549/en301549-node.html, letzter Aufruf 05.08.23

12 Bundesamt für Sicherheit in der Informationstechnik (2021): Checklisten zum IT-Grundschutz-Kompendium (Edition 2021), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/checklisten_2021.html, letzter Aufruf 17.08.23

# 1. Security by Design

**Hintergrund**

Security by Design fordert IT-Sicherheit bereits beim Entstehungsprozess von Portalen miteinzubeziehen. Gerade im Bereich Gesundheitsversorgung, Pflege und entsprechender Beratungsangebote ist dies besonders wichtig, da erhöhter Schutzbedarf vorliegt. Dieser Ansatz bietet den Vorteil, dass IT-Sicherheit nicht umständlich und oft unzureichend nachgerüstet werden muss. Dieses Vorgehen dient einerseits der Reduzierung der Angriffsfläche und andererseits der Einhaltung der Schutz- und Gewährleistungsziele. Security by Design heißt, dass schon bei der Konzeption, Umsetzung und Konfiguration von Portalen Grundlagen gelegt werden, die nachfolgend betrachtete Aspekte unterstützen.

Dazu gehört auch die Festlegung der allgemeinen Schutzziele die für ein Portal relevant sind (auch als Sicherheitsaspekte bezeichnet): Vertraulichkeit/Zugriffsschutz, Authentizität, Integrität, Verfügbarkeit, Verbindlichkeit/Nachweisbarkeit, sowie die Schutz- und Gewährleistungsziele des Datenschutzes: Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit, Intervenierbarkeit, Nicht-Verkettbarkeit, Unverknüpfbarkeit, Transparenz und Revisionsfähigkeit. Hierzu gehört beispielsweise auch die Überlegung, welche Daten im Portal vorhanden sind sowie von Benutzer:innen eingegeben werden können und darauf basierend die Festlegung, welche dieser Daten welchem Personenkreis zugänglich sein sollen. Es kann beispielsweise gewünscht sein, dass diese Daten öffentlich zugänglich sein sollen oder vertraulich behandelt werden müssen. Diese Beobachtung dient als Grundlage für die Festlegung von für die Gewährleistung dieser Schutzziele angemessener Sicherheitsmechanismen.

**Beispiele für Handlungsmöglichkeiten**

- Identifizierung aller im Portal vorhandenen oder anfallenden Daten und Bestimmungen der Schutzziele für diese Daten; Dabei ist zu beachten, dass Daten aus den Bereichen Gesundheitsversorgung, Pflege, Sozialversorgung und entsprechender Beratungsangebote im Allgemeinen einen hohen Schutzbedarf haben. Wenn nötig, werden Schutzmechanismen zur Erreichung der Schutzziele angewandt (Zugangsschutz).
- Als Oberkategorie werden weitere Beispiele für Handlungsmöglichkeiten unter dem Oberbegriff „Security by Design“ gegeben. Diese sind Bestandteil der nachfolgenden Kategorien:
  - Prävention, Detektion, Reaktion
  - Entwurfsrichtlininen für Sichere Systeme
  - Forensic Readiness
  - Privacy by Design

**Exemplarische Prüfmöglichkeiten**

- IT-Sicherheit wurde bereits bei der Konzeption eines Portals in den Gestaltungsprozess eingezogen.
- Alle im Portal vorhandenen und anfallenden Daten wurden hinsichtlich ihres Schutzbedarfs betrachtet und dieser festgelegt.
- Es wurden Maßnahmen zur Prävention, Detektion und Reaktion mit einbezogen (siehe Kapitel 1.1).
- Es wurden die Entwurfsrichtlinien für Sichere Systeme beachtet (siehe Kapitel 1.2).
- Das Portal ist vorbereitet für forensische Untersuchungen (siehe Kapitel 1.3).
- Das Portal schützt die Privatsphäre von Nutzer:innen (siehe Kapitel 1.4).

## 1.1 Security by Design: Prävention, Detektion, Reaktion

**Hintergrund**

IT-Sicherheit bietet drei grundlegende Ansätze zum Umgang mit IT-Sicherheitsvorfällen: Prävention umfasst solche Maßnahmen, die das Eintreten eines Sicherheitsvorfalls von vornherein verhindern sollen. Detektion beschreibt die Möglichkeit einen IT-Sicherheitsvorfall zu identifizieren. Schließlich adressiert Reaktion alle Maßnahmen, die bei einem IT-Sicherheitsvorfall getroffen werden, was auch die Wiederherstellung von Daten oder den Wiederanlauf von Systemen umfasst.

Security by Design bezieht Maßnahmen zur Prävention, Detektion und Reaktion bereits während der Entstehung eines Portals mit ein und dient damit selbst als präventive Maßnahme, welche IT-Sicherheitvorfälle reduzieren kann.

Diese Maßnahmen müssen nicht rein technischer Natur sein – auch organisatorische Maßnahmen können der Prävention, Detektion und Wiederherstellung dienen.

**Beispiele für Handlungsmöglichkeiten**

- Planung von:
  - Maßnahmen zur Prävention von IT-Sicherheitvorfällen, wie beispielsweise Mechanismen zum Zugriffsschutz auf Daten respektive Netzwerke (durch Netzwerkseparierung).
  - Maßnahmen zur Detektion von IT-Sicherheitvorfällen, wie beispielsweise Virenscanner (zur Detektion von Schadsoftware) oder Intrusion Detection Systeme (IDS).
  - Mechanismen zur Reaktion auf IT-Sicherheitvorfälle (nach erfolgtem Angriff und noch während des Angriffs). Dies kann beispielsweise eine Backup-Strategie sein (damit notfalls ein älterer Stand vor einem IT-Sicherheitvorfall eingespielt werden kann) umfasst aber auch das Bereitstellen von organisatorischen Prozessen im Fall eines IT-Sicherheitvorfalls – Wer kann helfen? Wer ist zu informieren?

**Exemplarische Prüfmöglichkeiten**

- Maßnahmen zur Prävention von IT-Sicherheitvorfällen wurden während der Konzeptionierung aufgenommen, wie beispielsweise:
  - Maßnahmen zum Zugriffsschutz auf Daten.
  - Maßnahmen zum Zugriffsschutz auf Netzwerkwerke.
- Maßnahmen zur Detektion von IT-Sicherheitvorfällen wurden während der Konzeptionierung aufgenommen, wie beispielsweise:
  - Maßnahmen zur Detektion von Schadsoftware.
  - Maßnahmen zur Prüfung der Manipulation des Datenbestandes.
- Maßnahmen zur Reaktion im Fall von IT-Sicherheitvorfällen wurden während der Konzeptionierung aufgenommen, wie beispielsweise:
  - Strategie zur Erzeugung und Wiedereinspielung von Backups.
  - Technische/Organisatorische Prozesse für die Reaktion auf IT-Sicherheitvorfällen, inklusive der Möglichkeit zur Eskalation (Notwendigkeit forensischer Untersuchung) und/oder des Wiederanlaufs.

## 1.2 Security by Design: Entwurfsrichtlinien für Sichere Systeme

**Hintergrund**

Um den Grundgedanken IT-Sicherheit schon bei der Konzeption zu beachten und damit innerhalb des Portals zentral zu verankern, umfasst Security by Design einige zentrale Prinzipien, die bereits beim Entwurf eines Portals beachtet werden können. Diese Entwurfsrichtlinien bieten eine Entscheidungsgrundlage während der Konzeption und haben bei erfolgreicher Beachtung präventiven Charakter.

**Beispiele für Handlungsmöglichkeiten**

- OWASP schlägt zehn Sicherheitsprinzipien vor[13]:
  - Angriffsflächen minimieren: Das Design sollte nur Funktionen umfassen, die auch nötig sind. Zusätzliche Funktionen haben immer das Risiko eine weitere Angriffsfläche zu bieten (Minimize Attack Surface Area).
  - Sichere Grundeinstellungen (Secure Defaults) – die Standardeinstellung wählt immer die sicherste Option aus.
  - Beschränkungen – Bausteine und Entitiäten haben nur die für ihre Funktion nötigen Zugriffsmöglichkeiten und die für ihre Funktion notwendigen Daten (Principle of Least Privilege und Seperation of Duties).
  - Gestaffelte Verteidigung (Defense in Depth) – ein IT-Sicherheitsmechanismus ist gut, aber weitere können den Schutz verstärken. Beispielsweise ist es gut, den physikalischen Zugang zu dem Server, auf dem ein Portal läuft, zu beschränken, aber zusätzlich die Daten auf dem Server zu verschlüsseln erhöht dennoch das Sicherheitsniveau.
  - Methoden zur sicheren Fehlerbehandlung einplanen (Fail securily).
  - Kein automatisches Vertrauen für externe Dienste (Don’t trust Services) – eventuell eingebundene externe Dienste können ein anderes Sicherheitsniveau haben. Daher ist jede Datenübermittlung an solche Dienste zu hinterfragen. Das gilt auch für in Portalen eingebundene Drittanbieter.
  - Offenes Design – keine vermeintliche Sicherheit durch Verschleierung von Funktionsmechanismen. Besser ist es offenen Quellcode zu verwenden, der von einer breiten Menge an Interessenten untersucht und verbessert werden kann (Avoid Security through Obscurity).
  - Auch die Sicherheitsmechanismen sollten möglichst simpel entworfen und umgesetzt sein um das Potential von Fehlern zu reduzieren (Keep Security Simple)
  - Mechanismen zum Aufspüren und Beheben von IT-Sicherheitsproblemen einplanen (Fix Security Issues correctly) – Beispielsweise durch das Einplanen von Funktions- und Sicherheitstests. Diese Maßnahmen sind entsprechend nicht rein technischer Natur und umfassen auch organisatorische Maßnahmen wie klare Vorgaben wie ein Portal im Falle einer entdeckten Schwachstelle aktualisiert (gepatcht) werden soll, wie darauf reagiert werden soll (z.B. abschalten) oder wer für welche Aufgaben (z.B. Aktualisierungen) zuständig ist.
- Weitere Designprinzipien werden von Saltzer[14] aufgezeigt:
  - Geringste notwendige Privilegien für Prozesse/Nutzer:innen (Erforderlichkeits-orientiert, Need to Know – Originalbezeichnung: Principle of least privilege).

13 OWASP: Security by Design Principles, https://wiki.owasp.org/index.php/Security_by_Design_Principles, letzter Aufruf 21.09.2023

14 Design Principles from: Jerome H. Saltzer, Michael D. Schroeder: The Protection of Information in Computer Systems. Revidiertes Manuskript, University of Virginia, 17. April 1975

- „Nicht erlaubt“ als Voreinstellung (Principle of fail-safe defaults).
- Möglichst einfaches und schlichtes Programmdesign, dass leichter überprüft werden kann (Principle of economy of mechanism).
- Überprüfung jedes Zugriffs, ob dieser legitim ist (Principle of complete mediation)
- Mechanismen zur Prüfung offenlegen und so „Security through Obscurity“ vermeiden (Principle of open design).
- Erlaubniserteilung nach mehreren Prüfungen (beispielsweise Mehrfaktorauthentifizierung oder Vier-Augen-Prinzip, Originalbezeichnung: Principle of seperation of privilege).
- Mechanismen die auf Ressourcen zugreifen sollten nicht zwischen Funktionen geteilt werden (Principle of least common mechanism).
- Sicherheitsmechanismen dürfen den Anwender;innen nicht behindert, damit diese sie nicht böswillig umgehten– Sicherheitsmechanismen müssen akzeptiert werden (Principle of psychological acceptability).

**Exemplarische Prüfmöglichkeiten**

- Die Architektur ist so einfach wie möglich, um den gewünschten Anwendungszweck zu erfüllen.
- Die verschiedenen Bestandteile der Architektur haben keine unnötigen Zugriffsmöglichkeiten auf Daten oder Prozesse.
- Die Grundeinstellungen des Portals und etwaiger darin vorhandener Konten sind so sicher wie möglich eingestellt.
- Der Schutz von Daten und Netzwerken erfolgt wenn möglich durch mehrere gestaffelte Mechanismen.
- Externen Diensten wird nicht automatisch vertraut.
- Mechanismen zum Aufspüren und Beheben von Sicherheitsproblemen sind eingeplant.
- Die verwendeten Lösungen sind quelloffen (Open Source).

## 1.3 Security by Design: Forensic Readiness

**Hintergrund**

Die IT-Forensik dient der Vorfallsaufklärung und kommt dann zum Einsatz, wenn ein IT-Sicherheitsvorfall vermutet oder bemerkt wurde. Sie ist daher eine reaktive Maßnahme. Mithilfe von IT-Forensik kann bei einem IT-Sicherheitsvorfall der Angriffsweg sowie das Ausmaß des durch den Vorfall verursachten Schadens untersucht werden.
Einerseits wird untersucht, welche Teilsysteme und Schwachstellen für einen Angriff genutzt werden können, um das System gegen einen weiteren Angriff auf dem gleichen Weg schützen zu können.
Andererseits soll identifiziert werden, welche Sicherheitsaspekte verletzt wurden: Wurden Daten für Dritte zugänglich gemacht (Bruch der Vertraulichkeit)? Wurden Daten verändert (Bruch der Integrität)? Wie kritisch sind diese Daten? Betrifft eine Veränderung auch potentielle Backups?
IT-Forensik beruht dabei auf dem Vorhandensein von Spuren, welche während der Untersuchung ausgewertet werden können. Im Design, also bei der Konzeption eines Systems, können bereits Mechanismen miteinbezogen werden, die die Möglichkeit zur Spurenerhebung im Fall eines IT-Sicherheitsvorfalls unterstützen oder erst möglich machen als auch Möglichkeiten eröffnen, aus einem Vorfall zu lernen und entsprechende Schutznachbesserungen zu ermöglichen – Ist dies erfolgreich geschehen, spricht man von Forensic Readiness.

**Beispiele für Handlungsmöglichkeiten**

- Einbringen von Möglichkeiten, um bestimmte Ereignisse mit Relevanz für die IT-Sicherheit innerhalb des Portals zu protokollieren. Diese Ereignisse könnten beispielsweise das Löschen oder das Anlegen von Konten mit besonderen Privilegien sein. Die Identifikation solcher Ereignisse mit Relevanz für IT-Sicherheit ist ein wichtiger konzeptioneller Schritt und kann auch bei einer ggf. notwendigen forensischen Untersuchung nützlich sein.
- Eine Backup-Strategie kann auch den forensischen Prozess unterstützen, indem die Identifikation von Integritätsbrüchen vereinfacht wird.
- Erstellung eines Konzepts zur Sicherung der Beweiskraft (Integrität, Authentizität) von erhobenen Protokollen unter Wahrung des Datenschutzes in Anbetracht des besonderen Schutzbedarfs in den Bereichen Gesundheitsversorgung, Pflege und entsprechender Beratungsangebote.
- Erstellung eines Konzepts zur Zuständigkeit für die Durchführung von forensischen Untersuchungen im Rahmen eines Konzepts zur Reaktion auf IT-Sicherheitsvorfälle.

**Exemplarische Prüfmöglichkeiten**

- Identifizierung und Protokollierung von wichtigen Ereignissen, die für die IT-Sicherheit relevant sind ohne dabei den Datenschutz zu verletzen.
- Prozesse für die Erstellung von regelmäßige Backups sind umgesetzt.
- Prüfung und Sicherstellung von Integrität und Authentizität von Protokollen und Backups.
- Prüfung der etablierten technischen/organisatorischen Prozesse für die Reaktion auf IT-Sicherheitsvorfälle, inklusive der Möglichkeit eine forensische Untersuchung.

## 1.4 Security by Design: Privacy by Design

**Hintergrund**

Privacy by Design adressiert u.a. den Schutz der Privatsphäre durch die Technikgestaltung und wird wie alle anderen Security by Design-Maßnahmen bereits bei der Konzeption eines Portals miteinbezogen. Die Schutz- und Gewährleistungsziele des Datenschutzes sind Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit, Intervenierbarkeit, Nicht-Verkettbarkeit, Unverknüpfbarkeit, Transparenz und Revisionsfähigkeit. Manche Kategorien von Daten haben einen erhöhten Schutzbedarf bzw. sind in der Erfassung, Speicherung und Verarbeitung strenger geregelt, wie Daten zur Profilbildung, biometrische Daten oder Daten von und über Kinder.

Ein zentraler Aspekt von Privacy by Design ist die Datenminimierung. Das heißt, dass nur die Daten erhoben, gespeichert und/oder verarbeitet werden, die für den Zweck des Portals dringend notwendig sind. Daher ist es ein notwendiger Schritt eben diese Daten während der Konzeption zu identifizieren und für diese Schutzbedarfe festzulegen (siehe Abschnitt 1. Security by Design). Weitere technische Maßnahmen umfassen die Pseudonymisierung oder Anonymisierung von Daten, welche für den Zweck des Portals unerlässlich sind, aber einen besonderen Schutz verlangen.

Hinzukommen bei personenbezogenen Daten, die datenschutzrechtlichen Möglichkeiten für die Betroffenen der Datenerhebung – Mechanismen zur Auskunft, Korrektur und Löschung von personenbezogenen Daten sollten bereits früh in das Konzept mit aufgenommen werden, da es sehr schwierig ist, solche Mechanismen nachzurüsten und solche Nachrüstungen häufig mit IT-Sicherheitsschwachstellen einhergehen.

Weiterhin müssen auch etwaige extern eingebundene Dienste und die an diese übermittelten Daten betrachtet werden vor allem, wenn sich diese Dienste außerhalb des europäischen Rechtsraums befinden und damit die Datenschutzgrundverordnung (DSGVO) nicht eingehalten werden muss.

**Beispiele für Handlungsmöglichkeiten**

- Identifizierung von Daten welche für das Portal notwendig sind.
- Beachtung des besonderen Schutzbedarfs der Daten in den Bereichen Gesundheitsversorgung, Pflege und dazugehöriger Beratungsangebote.
- Konzeption zur Erhebung, Speicherung und Verarbeitung dieser Daten, gemäß geltender Datenschutzbestimmungen, wie z.B. gemäß Artikel 5 der DSGVO.
- Identifizierung von Daten, die pseudonymisiert oder anonymisiert genutzt werden müssen. Dies umfasst auch Daten, die nicht direkt durch die Funktionen des Portals selbst, sondern durch Aspekte der technischen Umsetzung hinzukommen, wie beispielsweise Cookies, um Sitzungen oder Einstellungen zu speichern.
- Festlegung geeigneter Löschfristen für alle erhobenen Daten (unter Beachtung von Aspekten wie gesetzlich vorgeschriebenen Aufbewahrungsfristen).
- Entwurf eines Konzeptes zur Wahrung von Betroffenenrechten in Bezug auf personenbezogene Daten (Auskunft, Korrektur, Löschung).
- Need-to-Know: Nur Informationen, die für die Bearbeitung der Anfrage benötigt werden, abfragen. Beachtung des besonderen Schutzbedarfs der Daten im Bereich Gesundheitsversorgung, Pflege und dazugehöriger Beratungsangebote.
- Einbindung von solchen externen Diensten, die keine Daten erheben.

**Exemplarische Prüfmöglichkeiten**

- Alle im Portal vorhandenen und anfallenden Daten wurden identifiziert und einer Zweckbetrachtung unterzogen – wenn nicht dringend benötigt, wird auf eine Erhebung, Speicherung und Bearbeitung verzichtet.
- Wo möglich werden personenbezogene Daten pseudonymisiert oder anonymisiert.
- Prüfung der Umsetzung von Löschfristen für Daten.
- Mechanismen und Verfahren zur Auskunft, Korrektur und Löschung von personenbezogenen Daten sind etabliert.
- Prüfung von externen Dienste und deren Konfiguration, sodass sie keine Daten zu diesen übermitteln.
- Prüfung von personenbeziehbaren Daten auf besonders schützenswerte Informationen bzw. Gruppen (z.B. Minderjährige).

# 2. Ethisches Design

**Hintergrund**

Der ethische Einsatz von Technik beginnt bereits beim Design. Diese Kategorie umfasst einige unterschiedliche Aspekte sowie Richtlinien, um diese zu adressieren.

Ein zentraler Punkt ist dabei die Wahrung der Menschenrechte, die mit einer Vermeidung von Diskriminierung durch Technik einhergeht. Ein solcher Fall von Diskriminierung ergibt sich beispielsweise dann, wenn ein System Personen basierend auf ethnischer Herkunft, Geschlecht, Religion, Behinderungen, chronischen Krankheiten, Alter oder sexueller Identität unterschiedlich behandelt. Hierbei ist auch ein Potential für Missbrauch zu beachten und entsprechend zu minimieren – Daten über die zuvor genannten Merkmale können leicht missbraucht werden und sind daher besonders schützenswert (siehe u.a. Kapitel Security by Design 1.1 und 1.4).

Ein weiterer relevanter Aspekt ist die Transparenz der technischen Lösung – Die Nutzenden sollen verstehen können was zu welchen Zweck mit ihren Daten geschieht und wer dafür die Rechenschaft trägt. Die Nachvollziehbarkeit von organisatorischen Prozessen und technischen Maßnahmen ist ein notwendiger Schritt für das Vertrauen durch die Nutzenden.

Generell sollte Technik, wenn sie ethisch eingesetzt ist, das Wohl der Menschheit im Allgemeinen verbessern. Hierzu ergeben sich weitere Aspekte – die Digitale Nachhaltigkeit und die Digitale Inklusion – welche in den folgenden Kapiteln erläutert werden (siehe Kapitel 2.2 und 2.3). Kommt künstliche Intelligenz zum Einsatz, müssen weitere Aspekte für einen sicheren, robusten und nachvollziehbaren Einsatz von KI beachtet werden. Informationen und Empfehlungen für Unternehmen und Organisatonen bietet beispielsweise das Bundesamt für Sicherheit in der Informationstechnik an[15]. Vorgaben wurden bereits mit dem vom Europäischen Parlament verabschiedeten „Artificial Intelligence Act“ vorgelegt[16].

**Beispiele für Handlungsmöglichkeiten**

- Identifikation von Stellen im Portal, an denen Daten mit Bezug auf besonders für Diskriminierung anfällige Merkmale erhoben, gespeichert oder verarbeitet werden und anschließende Überprüfung, ob diese Daten notwendig sind. Wenn diese Daten benötigt werden, sind sie besonders abzusichern.
- Verwendung von quelloffener Software, die von unabhängigen Experten überprüft wurde.
- Möglichst keine externen Dienste einbinden, deren Funktionsprinzip nicht offengelegt ist.
- Benennung von klaren Verantwortlichkeiten für die verschiedenen Aspekte des Portals, z.B. Auftragsverarbeitende im Rahmen der DSGVO[17] oder Personal in leitenden Positionen.
- Dokumentation und Offenlegung der Prozesse – beispielsweise, welche Daten wie und warum erhoben werden, wie lange die Speicherung erfolgt und wohin diese übermittelt werden. Dies umfasst auch eingebundene externe Dienste und die durch die Einbindung ausgelöste Datenübertragung zu diesen.

15 Bundesamt für Sicherheit in der Informationstechnik (o.J.): Künstliche Intelligenz, https://www.bsi.bund.de/dok/13394406 , letzter Aufruf 22.05.23

16 Europäisches Parlament und Rat (2021): Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021PC0206, letzter Aufruf 15.08.23

17 DSK (Datenschutzkonferenz) (2018): Kurzpapier Nr. 13, Auftragsverarbeitung, Art. 28 DSGVO, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf, letzter Aufruf 24.08.23

| **Exemplarische Prüfmöglichkeiten** |
| --- |
| • Bei der Betrachtung anfallender Daten wurde das Risiko einer Diskriminierung bei der Betrachtung von notwendigen Sicherheitsmaßnahmen aufgenommen.<br>• Prüfung auf verständliche und transparente Präsentation von erhobenen, gespeicherten und verarbeiteten Daten sowie deren Intervenierbarkeit durch Nutzer:innen. |

## 2.1 Nachhaltigkeit: Ressourcenverbrauch von/durch Technik

**Hintergrund**

Den Ressourcenverbrauch von Technik so weit wie möglich einzuschränken ist Teil der ethischen Techniknutzung. Dieser Ressourcenverbrauch ergibt sich sowohl aus dem Energiebedarf der betriebenen Systeme, dem Energiebedarf bei einer Datenübertragung sowie auch den notwendigen Rohstoffen für die Herstellung der beteiligten Computersysteme. Im allgemeinen ist es komplex, diesen Ressourcenverbrauch zu erfassen, da viele unterschiedliche Aspekte eine Rolle spielen. Vereinfacht kann man von einem ökologischen Fußabdruck sprechen und davon, dass das Internet eine große Menge Energie für die Kommunikation mit und den Betrieb von Diensten benötigt[18] [19].

Trotz der Komplexität gibt es Maßnahmen, die geeignet sind, den ökologischen Fußabdruck einer technischen Lösung in jedem Fall zu reduzieren. Dies ist einerseits eine Reduktion der notwendigen Rechenleistung und Datenübertragung dadurch, dass nur notwendige oder zumindest angeforderte Daten übertragen werden. Neben der Menge der übertragenen Daten spielt auch der Übertragungsweg eine Rolle – eine lokale Übertragung bindet eine weniger umfangreiche Netzwerkinfrastruktur ein, so das weniger Geräte an der Übertragung beteiligt sind.

Weiterhin gibt es Software und Hardware, welche besser dazu geeignet ist, den Energieverbrauch zu reduzieren. Das Thema der systematischen Untersuchung des Energieverbrauchs von Software ist in der Forschung noch vergleichsweise neu und bisher nur punktuell umgesetzt, aber es existieren Hardwarearchitekturen, welche den Strombedarf besser mit der Last skalieren und daher unter geringer Last nennenswert weniger Strom benötigen[20]. Einige Rechenzentren verfügen darüber hinaus über Mechanismen, um die beim Serverbetrieb entstehende Abwärme für andere Zwecke zu nutzen.

**Beispiele für Handlungsmöglichkeiten**

- Verwendung eines schlichten Designs, das auf das Nachladen umfangreicher Datenmengen verzichtet (Beispielsweise auf Hintergrundbilder, die sich in kurzer Zeitfolge aktualisieren).
- Reduzierung der automatisierten Übertragung von größeren Datenmengen (Beispielsweise sollten Videos nur geladen werden, wenn sie aktiv angeklickt werden).
- Betrachtung dieser Aspekte gilt auch für eingebundene externe Anbieter, wodurch die Übertragung von Daten an oder durch diese externen Anbieter nur bei einem expliziten Aufruf durchgeführt wird (Beispielsweise Kartendienste).

**Exemplarische Prüfmöglichkeiten**

- Betrachtung des Datenverkehrs bei der Nutzung des Portals und Identifizierung unnötiger Datenübertragungen.

18 Verivox: Wie fällt der Stromverbrauch im Internet aus?. https://www.verivox.de/strom/ratgeber/wie-faellt-der-stromverbrauch-durch-das-internet-aus-1118069/?awc=14797_1693832976_8968dc8e5f4ba5f70c9740b40e262607&source_id=153, letzter Aufruf 15.09.2023

19 Vattenfall: Ständig unter Strom: So viel verbraucht das Internet. https://www.vattenfall.de/infowelt-energie/energieverbrauch-internet, letzter Aufruf 15.09.2023

20 Siehe beispielsweise der Vergleich zwischen aktuellen Intel und AMD-Prozesses unter Anandtech: A Lighter Touch: Exploring CPU Power Scaling On Core i9-13900K and Ryzen 9 7950X. https://www.anandtech.com/show/17641/lighter-touch-cpu-power-scaling-13900k-7950x/4, letzter Aufruf: 15.09.2023

## 2.2 Nachhaltigkeit: Digitale Güter

**Hintergrund**

Die digitale Nachhaltigkeit betrachtet in Abgrenzung zum Ressourcenverbrauch von Technik die Nachhaltigkeit des digitalen Gutes selbst. Entsprechend ist das Ziel der Digitalen Nachhaltigkeit, dass ein bestimmtes Portal oder ein bestimmter Datensatz möglichst lange erhalten und nutzbar bleibt bzw. noch nutzbar ist.

Ein zentraler Aspekt hierbei ist die Verwendung offener Lösungen mit dokumentierten und standardisierten offenen Schnittstellen und Datenformaten, damit die entstehenden Systeme und Datensätze auch in Zukunft noch nutzbar sind. Dieser Ansatz erlaubt sowohl eine Wartung als auch eine Erweiterung oder Anpassungen der Lösungen sowie eine Weiterverwendung bestimmter Komponenten. Effekte wie die Abhängigkeit von proprietären Dateiformaten und daraus resultierenden Inkompatibilitäten in der Zukunft werden hier durch vermieden. Dadurch werden auch Abhängigkeiten, welche im Falle von rechtlichen Änderungen, Veränderungen an Lizenzen oder Kosten oder dem Einstellen eines Betriebs problematisch werden können umgangen – ein sogenannter Vendor Lock-In wird so verhindert.

Durch die Zurverfügungstellung geeigneter und ggf. anonymisierter Datensätze in offenen, standardisierten Formaten mittels einer aussagekräftigen Metabeschreibung kann ein möglichst hoher gesellschaftlicher Nutzen erzielt werden (Open Data).

**Beispiele für Handlungsmöglichkeiten**

- Verwendung offener Formate zur Speicherung oder Zurverfügungstellung von Daten.
- Verwendung offengelegter, standardisierter Schnittstellen.
- Dokumentation aller informatischen Bestandteile des Portals, um zu einem späteren Zeitpunkt nachlesen zu können, ob auch in Zukunft das gesamte bzw. Teile des Portals trotz Änderungen weiterbetrieben und gewartet werden kann.
- Reduzierung von Abhängigkeiten externer Dienste, die aus verschiedenen Gründen in Zukunft nicht mehr verfügbar sein könnten.

**Exemplarische Prüfmöglichkeiten**

- Prüfung ob:
  - offene Formate zur Speicherung anfallender Datensätze verwendet werden.
  - offene Formate zum Herunterladen angebotener Inhalte verwendet werden.
  - Schnittstellen, die das Portal intern und extern nutzt, offen und standardisiert sind.
  - Schnittstellen des Portals dokumentiert sind.
  - Abhängigkeiten zu externen Diensten vorhanden sind. Durchführung einer Abschätzung, wie zuverlässig diese externen Dienste in Zukunft verwendet werden können.

## 2.3 Nachhaltigkeit: Aspekte der Konfigurierbarkeit

**Hintergrund**

Vor dem Hintergrund einer nachhaltigen Gestaltung von IT-Informationssystemen ist insbesondere die frühzeitig im Entstehungsprozess vorgesehene Konfigurierbarkeit eines Systems als ein Schlüssel zu betrachten. Bleibt ein System wartbar, sodass es auf neue Umweltbedingungen und Technologieveränderungen angepasst werden kann, wird verhindert, dass es schon frühzeitig nicht mehr einsatzbereit ist und der Return on IT-Investment geringer ausfällt.

Die Konfigurierbarkeit bedeutet auch, dass nicht notwendigerweise nur IT-Spezialisten das System konfigurieren können, sondern kleinere Anpassungen bereits durch eingewiesenes Personal erfolgen kann. So sind ebenfalls schnelle Reaktionen möglich.

Mit umweltschonender IT-Architektur, dessen mögliche Konfiguration und Monitoring hinsichtlich Datensparsamkeit als auch mit auf Energieeffizienz optimierte Prozesse, lassen sich zusätzlich Ressourcen einsparen und der Ausstoß von $CO^2$ verringern.

**Beispiele für Handlungsmöglichkeiten**

- Schaffung eines einfachen und verständlichen Modells vom IT-Informationssystem.
- Dokumention des Modells und insbesondere der zugehörigen Schnittstellen und Datenformate.
- Konfigurierbarkeit von Parametern erhalten, bspw. Dateipfade.
- Verwendung von Open Source Software.
- Ressourcenschonung durch eine Reduktion auf relevante Datenübertragungen. Der umweltbewusste Umgang kann den Stromverbrauch minimieren, wodurch wiederum auch Verbrauchgüter für neue Energie und dadurch $CO^2$ verringert werden können. Hierbei nehmen u.a. auch die Wahl des Providers, die Standorte der Server als auch die Einbeziehung von Drittanbietern samt ihrer Server einen Einfluss drauf. Ebenso hat die Rohstoffquelle des Stroms einen Einfluss auf die Produktion von $CO^2$[21].

**Exemplarische Prüfmöglichkeiten**

- Prüfung des Systems auf Nachhaltigkeit, beispielsweise anhand der Anforderungen für „Nachhaltige Software“ aus dem Kriterienkatalog des Umweltbundesamtes[22]. U.a.:
  - Ressourcenschonung von Hard- und Software durch unter- und miteinander kontinuierliche Kompatibilität.
  - Plattformunabhängigkeit durch Nutzung freier Software, die nicht an bestimmte Hardware gebunden ist.
  - Messung und Dokumentation des Energiebedarfs von Software, um die Energieeffizienz verschiedener Versionen miteinander zu vergleichen.
  - Messung und Dokumentation der Hardwarebelastung, um zu prüfen, wann es zu einer Abweichung in Form einer erhöhten Belastungen kommt.
  - Messung und Dokumentation der im Netz übertragenen Datenmenge.
  - Dokumentation der erarbeiteten Lösungen von Problemen, die während der Konfiguration eines IT-Systems aufgetaucht sind und Öffentlichmachung eben dieser.

21 Deutscher Bundestag (2007): CO2-Bilanzen verschiedener Energieträger im Vergleich, Seite 22, https://www.bundestag.de/resource/blob/406432/70f77c4c170d9048d88dcc3071b7721c/wd-8-056-07-pdf-data.pdf, letzter Aufruf 28.08.23

22 Umweltbundesamt (2015) Nachhaltige Software Dokumentation des Fachgesprächs am 28.11.2014, S. 43f, https://www.umweltbundesamt.de/sites/default/files/medien/378/publikationen/dokumentation_fachgespraech_nachhaltige_software.pdf, letzter Aufruf 16.08.23

## 2.3 Digitale Inklusion

**Hintergrund**

In einer vielfältigen Gesellschaft muss auch der Zugang zu Online-Portalen vielfältig sein. Nicht nur die Gestaltung und der Zugang der Informationen auf den Webportalen sollten barrierefrei sein, sondern auch die Dienste und Programme, die auf der Internetseite integriert sind. Zu einer umfassenden Inklusion zählen nicht nur z.B. physische oder geistige Beeinträchtigungen, sondern auch der Zugang unabhängig von kulturellen oder sozioökonomischen Hintergründen. Zudem sollte auch u.a. die Präsentationsform breit gefächert aufgestellt sein, um die Reproduktion von Stereotypen und Stigmatisierung derer zugunsten einer Geschlechtergleichstellung zu vermeiden.
Neben den allgemeinen und ersten Hinweisen zur Umsetzung in diesem Abschnitt, wird im Folgenden auf Beispiele zur Förderung von Gender Mainstreaming im Rahmen der Digitalisierung sowie auf die einzelnen WCAG Kategorien[23] zur Steigerung der Barrierefreiheit eingegangen.

**Beispiele für Handlungsmöglichkeiten**

- Vernetzung und Austausch mit Fachpersonal, das sich mit digitaler Inklusion beschäftigt. Auf diese Weise können Kenntnisse über mögliche Einschränkungen, die beim Besuch des Webportals bestehen sichtbar gemacht werden, sowie das Webportal um zusätzliche und andere Unterstützungsprogramme erweitert werden.
- Schaffung von Arbeitsplätzen für Menschen mit Behinderungen und gemeinsame Evaluation des Webportals.

**Exemplarische Prüfmöglichkeiten**

- Erstellung oder Nutzung von Checklisten, die auf eine barrierefreie Prüfung der Inhalte ausgelegt sind. Neben Textalternativen in einfacher und fremden Sprachen, können z.B. auch mögliche körperliche Einschränkungen, die die Motorik in Bezug auf Eingabe, Zugang und Navigation beeinträchtigen, berücksichtigt werden. Es können auch Seh- und Hörvermögen beeinträchtigt sein, so dass Skalierfunktionen, Untertitelung/ Gebärdensprache, Vorlesedienste oder Kontrast- bzw. Farbkorrekturen nötig werden können.
- Prüfung technischer Einschränkungen, die durch veraltete Medientechnik oder Software wie Browser der Endanwender:innen resultieren können.
- Prüfung, ob kostenfreie Informationen und Anlaufstellen für Menschen ohne Zugang zum Internet verfügbar sind.

Mögliche erste Ansätze und Werkzeuge:

- W3C Easy Checks – A First Review of Web Accessibility[24]
- Web Disability Simulator[25]
- Browser Erweiterung zur Darstellung von beeinträchtigten Weberfahrungen[26]

23 W3C (2018): Web Content Accessibility Guidelines (WCAG) 2.1, https://www.w3.org/TR/2018/REC-WCAG21-20180605/, letzter Aufruf 23.08.23

24 W3C (o.J.): W3C Easy Checks – A First Review of Web Accessibility, https://www.w3.org/WAI/test-evaluate/preliminary/, letzter Aufruf 06.06.2023

25 Metamatrix (o.J.): Web Disability Simulator, https://github.com/Metamatrix/Web-Disability-Simulator, letzter Aufruf 06.06.2023

26 Uni Bielefeld (o.J.): Digitale Barrierefreiheit, https://www.uni-bielefeld.de/einrichtungen/zab/digitale-barrierefreiheit, letzter Aufruf 06.06.2023

## 2.3.1 Barrierefreiheit: Wahrnehmbarkeit, Bedienbarkeit, Verständlichkeit, Robustheit

**Hintergrund**

In diesem Abschnitt wird die Barrierefreiheit im Kontext von Digitaler Inklusion thematisiert. Nach einer eingehenden Definition, werden nachfolgend die vier Prinzipien Wahrnehmbarkeit, Bedienbarkeit, Verständlichkeit und Robustheit genauer betrachtet und mit Beispielen für Handlungs- und Prüfmöglichkeiten bei der Gestaltung von Webportalen ergänzt.

**Was ist Barrierefreiheit?**

Wie im §4 des Behindertengleichstellungsgesetzes definiert, ist Barrierefreiheit gegeben, wenn gestaltete Lebensbereiche, die bauliche Anlagen, Verkehrsmittel, technische Geräte, Informations- und Kommunikationssysteme umfassen, für Menschen mit Behinderungen ohne Erschwernis und ohne fremde Hilfe auffindbar, zugänglich und nutzbar sind[27].

**Was ist Digitale Barrierefreiheit?**

Menschen müssen ohne Erschwernisse IT-Lösungen wie Software, Webseiten usw. auffinden und nutzen können[28]. Gerade bei der Gestaltung barrierefreier Webportale für Menschen mit Behinderung, gibt es einige Aspekte zu berücksichtigen. Erschwernisse können beispielsweise unzureichende Farbkontraste, Unzugänglichkeiten wie die Möglichkeit eine Webseite ohne Maus bedienen zu können oder fehlende Untertitel sein. Die digitale Barrierefreiheit umfasst dabei verschiedene Arten von Behinderungen, einschließlich visueller, auditiver, motorischer, sprachlicher kognitiver, Sprach-, Lern- und neurologischer Behinderungen. Aber nicht ausschließlich Menschen mit Behinderungen hilft eine digitale Barrierefreiheit - letztendlich profitieren alle davon. Sehfähigkeit, Lesefähigkeit oder Konzentrationsschwierigkeiten können auch Menschen ohne Behinderung betreffen, beispielsweise wenn im Alter der Sehsinn abnimmt. IT-Lösungen müssen deshalb bestimmte technischen Eigenschaften aufweisen, damit diese ohne Hürden genutzt werden können (vgl. ebd.). Laut Domingos de Oliveira helfen dabei auch Open-Source-Lösungen, welche für die Zugänglichkeit für alle von entscheidender Bedeutung ist[29]. Open-Source-Systeme bieten oft eine überlegene Barrierefreiheit im Vergleich zu kommerzieller bzw. properietärer Software. Sie werden von einer Gemeinschaft von Freiwilligen gepflegt, die sich für eine kontinuierliche Verbesserung einsetzen. Beispiele hierfür sind Content-Management-Systeme wie Typo3[30], WordPress[31] oder Joomla[32], Videokonferenzsysteme wie BigBlueButton[33] und Screenreader wie Orca[34]. Daher ist das Nutzen einer Open-Source-Software eine zukunftssichere Wahl für die Gestaltung barrierefreier digitaler

27 Der Beauftragte der Bundesregierung für Informationstechnik (o. J.): Behindertengleichstellungsgesetz (BGG), https://www.barrierefreiheit-dienstekonsolidierung.bund.de/Webs/PB/DE/gesetze-und-richtlinien/bgg/bgg-artikel.html;jsessionid=E894D8-BE4CBF5936106C2696DEDA26A3.1_cid373 , letzter Aufruf 24.07.2023

28 Der Beauftragte der Bundesregierung für Informationstechnik (o. J.): Digitale Barrierefreiheit, https://www.barrierefreiheit-dienstekonsolidierung.bund.de/Webs/PB/DE/anforderungen-an-die-it/digitale-barrierefreiheit/digitale-barrierefreiheit-node.html , letzter Aufruf 24.07.2023

29 Domingos de Oliveira (2022): WARUM DIE ZUKUNFT DER BARRIEREFREIHEIT OPENSOURCE SEIN SOLLTE, https://www.netz-barrierefrei.de/wordpress/ist-die-zukunft-der-barrierefreiheit-opensource/, letzter Aufruf 02.08.23

30 TYPO3 Association (o.J.): TYPO3, https://typo3.org, letzter Aufruf 25.08.23

31 WordPress Foundation (o.J.): WordPress.com, https://wordpress.com/de/, letzter Aufruf 25.08.23

32 Joomla.de (2023): Joomla.de, https://www.joomla.de/, letzter Aufruf 25.08.23

33 BigBlueButton Inc. (o.J.): BigBlueButton, https://bigbluebutton.org/, letzter Aufruf 25.08.23

34 The GNOME Project (o.J.): Orca, https://help.gnome.org/users/orca/stable/, letzter Aufruf 25.08.23

Erfahrungen.
Die Basis für die digitale Barrierefreiheit bilden die Anforderungen aus der BITV 2.0[35] sowie der harmonisierten europäischen Norm EN 301 549[36] und die internationalen Web Content Accessibility Guidelines in der aktuellen Version 2.1 (WCAG 2.1)[37].
Die WCAG spielen dabei eine besondere Rolle, sie geben die Standards vor, welche Webseiten vorweisen sollten, damit sie barrierefrei zugänglich sind. Erarbeitet wurden diese Standards von der Web Accessibillity Initiative (WAI) des World Wide Web Consortium (W3C). In den WCAG enthalten sind die Prinzipien Wahrnehmbarkeit, Bedienbarkeit, Verständlichkeit und Robustheit. Diese vier Prinzipien sollen sicherstellen, dass Webinhalte für alle Nutzer:innen zugänglich sind.
Die WCAG bewertet die Barrierefreiheitsanforderungen von Webseiten in drei verschiedenen Kategorien (A - Mindestanforderung, AA - Annehmbare Zugänglichkeit und AAA - Die höchste Stufe der Zugänglichkeit). Die Stufe AA ist der globale Standard, der für die meisten Benutzenden eine ausreichende Zugänglichkeit gewährleistet[38]. Für bestimmte Internetseiten ist dieses Niveau gesetzlich vorgeschrieben und wird oft als gutes Beispiel für barrierefreie Webportale herangezogen.
Das die Standards der WCAG eingehalten werden, wird auf einem Webportal in der Barrierefreiheitserklärung festgehalten. Grundsätzlich sollten alle Anbieter von Webportalen eine Barrierefreiheitserklärung abgeben, insbesondere öffentliche Stellen sind gesetzlich verpflichtet über die getroffenen Maßnahmen zu informieren[39]. Helfen können dabei Mustererklärungen und Vorlagen, die Unterstützung bieten, und zeigen, wie eine solche Erklärung umgesetzt werden muss[40].
Obwohl die Richtlinien der W3C bereits einen großen Bereich abdecken, bleibt es stets herausfordernd, sämtliche Arten, Ausprägungen und Kombinationen von Behinderungen umfassend zu berücksichtigen.

35 Bundesministerium der Justiz (2011): Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie-Informationstechnik-Verordnung - BITV 2.0), https://www.gesetze-im-internet.de/bitv_2_0/BJNR184300011.html, letzter Aufruf 28.08.23

36 ETSI (2021): EN 301 549 Accessibility requirements for ICT products and services, https://www.etsi.org/deliver/etsi_en/301500_301599/301549/03.02.01_60/en_301549v030201p.pdf, letzter Aufruf 28.08.23

37 Der Beauftragte der Bundesregierung für Informationstechnik (o. J.): EN 301 549, https://www.barrierefreiheit-dienstekonsolidierung.bund.de/Webs/PB/DE/gesetze-und-richtlinien/en301549/en301549-node.html , letzter Aufruf 24.07.23

38 Der Beauftragte der Bundesregierung für Informationstechnik (o. J.): Web Content Accessibility Guidelines 2.1 (WCAG 2.1)https://www.barrierefreiheit-dienstekonsolidierung.bund.de/Webs/PB/DE/gesetze-und-richtlinien/wcag/wcag-node.html, letzter Aufruf 24.07.23

39 Landesrecht Sachsen-Anhalt (2019): Gesetz des Landes Sachsen-Anhalt zur Gleichstellung von Menschen mit Behinderungen (Behindertengleichstellungsgesetz Sachsen-Anhalt - BGG LSA) Vom 16. Dezember 2010 - § 16b Erklärung zur Barrierefreiheit, https://www.landesrecht.sachsen-anhalt.de/bsst/document/jlr-BehGleichGST2010V4P16b/part/S, 28.08.23

40 Bitvtest (o.J.): Die Erklärung zur Barrierefreiheit, https://www.bitvtest.de/bitv_test/das_testverfahren_im_detail/vertiefend/die_erklaerung_zur_barrierefreiheit.html, letzter Aufruf 28.08.23

## Wahrnehmbarkeit

**Hintergrund**

Das erste der vier Prinzipien der WCAG ist die Wahrnehmbarkeit. Es besagt, dass Informationen und Funktionen für alle Nutzenden in einer Weise präsentiert werden müssen, die sie erkennen und verstehen können. Für Menschen mit Hör- oder Sehbeeinträchtigung kann es herausfordernd sein, wenn Inhalte ausschließlich in visuellen oder auditiven Formaten verfügbar sind. Daher muss sichergestellt sein, dass diese Informationen über unterschiedliche Sinneskanäle wahrgenommen werden können. Viele Menschen mit Behinderungen nutzen Hilfsmittel wie Bildschirmlesegeräte oder Brailledisplays, um Inhalte wahrzunehmen. Sie sind darauf angewiesen, dass Webseiten mit diesen Technologien kompatibel sind. So müssen etwa Informationen, die sehend erfasst werden können auch hörbar gemacht werden und umgekehrt. Dies gelingt, wenn bereits bei der Erstellung der Webportale die Erfolgskriterien der WCAG eingehalten werden[41].

**Beispiele für Handlungsmöglichkeiten**

- Verwendung von aussagekräftigen Alternativ-Texten für Bilder (alt-Tags) und präzise Beschreibung vom Inhalt des Bildes, ohne dabei zu lang oder verwirrend zu werden (vgl. Erfolgskriterium 1.1.1 der WCAG Nicht-Text-Inhalt).
- Bereitstellung von Transkripten für Audioinhalte, um es Nutzer:innen zu ermöglichen, den Inhalt in schriftlicher Form wahrzunehmen (vgl. Erfolgskriterium 1.2.1 der WCAG Reine Audio- und Videoinhalte (aufgezeichnet)).
- Erstellung von Untertitel für Videos oder Audioinhalte, um diese für hörgeschädigte Nutzer:innen zugänglich zu machen (vgl. Erfolgskriterium 1.2.2 der WCAG Untertitel (aufgezeichnet)).
- Verwendung von Überschriftenformaten (h1-h6). Es sollte nur eine Hauptüberschrift (h1) geben, gefolgt von Untertiteln (h2), (h3) und so weiter. (vgl. Erfolgskriterium 1.3.1 der WCAG Info und Beziehungen).
- Vermeidung von Farbkombinationen, die für Menschen mit Farbsehbeeinträchtigungen schwierig zu erkennen sind[42] (vgl. Erfolgskriterium 1.4.1 der WCAG Benutzung von Farbe).
- Gewährleistung der Lesbarkeit durch ausreichende Kontraste zwischen Texten und Hintergründe. (vgl. Erfolgskriterium 1.4.3 der WCAG Kontrast (Minimum)).
- Gewährleistung der Skalierbarkeit von Schriften, so dass ein Text ohne technologische Hilfe bis zu 200 Prozent vergrößert werden kann, ohne dass Inhalte unlesbar werden (vgl. Erfolgskriterium 1.4.4 der WCAG Textgröße ändern).

**Exemplarische Prüfmöglichkeiten**

- Prüfung des Portals auf kritische Kontraste durch Nutzung von Analysewerkzeugen, wie z.B. der kostenlosen Browser-Erweiterung Contrast Checker von WebAIM[43].
- Prüfung ob:
  - für Audiomedien Alternativen in Form von Transkriptionen vorliegen
  - für informationstragende visuelle Videoinhalte eine Audiodeskription oder Volltext-Alternative vorliegt.
  - Videos, deren Tonspur Informationen enthalten, mit Untertiteln versehen sind.
- Nutzung von Werkzeugen wie z.B. WAVE Web Accessibility Evaluation Tools oder

41 Barrierefreies Webdesign (o.J.): Erfolgskriterien und Konformitätsbedingungen der Web Content Accessibility Guidelines (WCAG) 2.1, https://www.barrierefreies-webdesign.de/richtlinien/wcag-2.1/erfolgskriterien/, letzter Zugrif 22.08.23

42 Gattiker, Urs E. (2022): Farbenblindheit: 5 Webdesign Tipps für ein barrierefreies Internet, https://drkpi.com/de/farbenblindheit-und-webdesign-tipps-und-tools/, letzter Aufruf 08.08.2023

43 WebAIM Institute for Disability Research, Policy, and Practice (o.J.): Contrast Checker, https://webaim.org/resources/contrastchecker/, letzter Aufruf 08.08.23

HTML-Codesniffer[44], um zu überprüfen, ob Bilder auf dem Webportal einen Alt-Text haben[45].

44 Squizlabs.github.io (o.J.): HTML_CodeSniffer, http://squizlabs.github.io/HTML_CodeSniffer, letzter Aufruf 25.08.23

45 WebAIM Institute for Disability Research, Policy, and Practice (o.J.), https://wave.webaim.org/extension/, letzter Aufruf 14.08.2023

## Bedienbarkeit

**Hintergrund**

Die Bedienbarkeit ist das zweite der vier Prinzipien der WCAG. Nutzende mit unterschiedlichen Fähigkeiten und technischen Kenntnissen müssen in der Lage sein Online-Portale so effektiv wie möglich verwenden zu können. Das Prinzip der Bedienbarkeit zielt darauf ab, dass Aspekte wie die intuitive Navigation, die klare Informationsstruktur, die konsistente Benutzerführung und die optimale Darstellung von Inhalten in der Überlegung für barrierefreie Internetangebote berücksichtigt werden. Beispielsweise sollten Webseiten so gestaltet sein, dass sie auch mit Tastatur oder Sprachbefehlen bedient werden können, um Menschen mit motorischen Einschränkungen zu unterstützen.

**Beispiele für Handlungsmöglichkeiten**

- Zugänglichkeit aller Inhalte des Portals mit der Tastatur gewährleisten (vgl. Erfolgskriterium 2.1.1 Tastatur).
- Vermeidung von Zeitdruck, indem Nutzer:innen ausreichend Zeit zur Verfügung gestellt wird, um Inhalte auf dem Portal lesen sowie Aktionen wie z.B. Eingaben ausführen zu können (vgl. Richtlinie 2.2 Ausreichend Zeit).
- Verwendung aussagekräftiger Metadaten, indem Title-Tags und Meta-Description befüllt werden, wodurch Inhalte besser auffindbar sind und die Nutzer:innen dadurch den Inhalt und Zweck einer Seite besser verstehen, bevor sie das Portal besuchen (vgl. Erfolgskriterium 2.4.2 Seite mit Titel versehen).
- Sichtbarmachung des Tastaturfokus, indem er in einer logischen Reihenfolge durch die Seitenelemente führt und so eine klare Navigation ermöglicht (vgl. Erfolgskriterium 2.4.7 Fokus sichtbar).
- Unterstützung verschiedener Eingabemethoden, um Interaktionen mit verschiedener Hardware wie Maus, Tastatur oder Touchscreen gleichwertig ausführen zu können (vgl. Erfolgskriterium 2.5.6 Gleichzeitig verfügbare Eingabemechanismen).

**Exemplarische Prüfmöglichkeiten**

- Überprüfung der Einhaltung der logischen Reihenfolge bei Nutzung der Tabulatortaste und Erreichbarkeit aller Elemente des Webportals. Z.B. mit Hilfe der Browser-Erweiterung taba11y[46] oder dem WAVE Web Accessibility Evaluation Tools.
- Überprüfung der Einstellungen für Zeitlimits und automatischen Aktualisierungen.
- Überprüfung der Möglichkeit für Benutzer:innen, Zeitlimits anzupassen oder zu deaktivieren.

46 Peter Gould, (2022): Chromium Browsererweiterung tabally, https://chrome.google.com/webstore/detail/taba11y/aocppmckdocdjkphmofnklcjhdidgmga, letzter Aufruf 14.08.2023

## Verständlichkeit

**Hintergrund**

Um sicher zu stellen, dass digitale Inhalte einer vielfältigen Nutzerschaft verständlich sind, wurde das Prinzip der Verständlichkeit in die WCAG aufgenommen. Menschen mit kognitiven Beeinträchtigungen haben möglicherweise Schwierigkeiten komplexe Sprache oder komplizierte Informationen zu verstehen. Daher sollten Angebote so gestaltet werden, dass die Inhalte klar, präzise und auf eine leicht verständliche Weise präsentiert werden und das nicht nur für die Nutzenden, sondern auch für unterstützende Technologien wie Bildschirmlesegeräte.

**Beispiele für Handlungsmöglichkeiten**

- Implementierung von automatischer Spracherkennung auf dem Webportal (vgl. Erfolgskriterium 3.1.1 Sprache der Seite).
- Bestimmung der Sprache eines jeden Abschnitts oder Satzes durch Software ermöglichen, mit Ausnahme von bspw. Eigennamen oder technischen Fachbegriffen. U.a. können dadurch Bildschirmlesegeräte oder andere Technologien Inhalte korrekt darstellen bzw. wiedergeben (vgl. Erfolgskriterium 3.1.2 Sprache von Teilen).
- Verwendung von klarer und einfacher Sprache, welche immer an diverse Zielgruppen anpassbar ist (vgl. u.a. Erfolgskriterium 3.1.5 Leseniveau).
- Vermeidung von Fachjargon und technischen Begriffen, es sei denn, sie sind notwendig und werden erklärt (vgl. Erfolgskriterium 3.1.3 Ungewöhnliche Wörter).
- Gewährleistung einer vorhersehbaren Darstellung und Funktionalität des Webportals, bspw. durch klar gekennzeichnete und leicht zu findende Menüs, Suchfelder oder Links zu wichtigen Bereichen des Webportals (Erfolgskriterium 3.2.3 Konsistente Navigation).
- Bereitstellung klarer und eindeutiger Beschriftungen und Anweisungen, u.a. Beispiele für erwartete Datenformate oder eindeutigen Kennzeichnung von Pflichtfeldern (vgl. Erfolgskriterium 3.3.2 Beschriftungen (Labels) oder Anweisungen).
- Hilfestellung bei Eingabefehlern, bspw. durch Bereitstellung klarer Anweisungen in Formularen, nachdem eine eingegebene Information nicht akzeptiert wurde (vgl. Erfolgskriterium 3.3.3 Fehlerempfehlung).

**Exemplarische Prüfmöglichkeiten**

- Prüfung ob:
  - voreingestellte menschliche Sprache durch den Browser erkannt werden kann.
  - Bildschirmlesegeräte die menschliche Sprache jedes Abschnitts oder jedes Satzes erkennt.
  - Navigationsmechanismen und Bestandteile mit der gleichen Funktionalität konsistent erkannt werden und in der gleichen relativen Reihenfolge auftreten.
  - Fehler automatisch erkannt und den Nutzer:innen in Textform beschrieben werden.

## Robustheit

**Hintergrund**

Die Robustheit bezieht sich auf die Fähigkeit, mit der Webportale und deren Anwendungen widerstandsfähig gegenüber verschiedene und sich verändernde Technologien werden. Dadurch wird eine konsistente und zuverlässige Zugänglichkeit sichergestellt. Hierbei werden Aspekte wie die Unterstützung verschiedener Browser wie z.B. Firefox[47] und Ungoogled Chromium[48], Betriebssysteme wie z.B. Linux Mint oder Assistenztechnologien wie Screenreader, Vergrößerungssoftware, Gestensteuerung u.ä. berücksichtigt.

**Beispiele für Handlungsmöglichkeiten**

- Trennung von Inhalt, Struktur und Design (vgl. Erfolgskriterium 4.1.1 Syntaxanalyse).
- Gewährleistung der ordnungsgemäßen Funktion des Webportals auf verschiedenen gängigen aber auch älteren Webbrowsern (vgl. Erfolgskriterium 4.1.1 Syntaxanalyse).
- Durchführung regelmäßiger Tests mit verschiedenen Browser-Versionen zur frühzeitigen Erkennung und Behebung möglicher Inkompatibilitäten.
- Sicherstellung der korrekten Darstellung und Funktion Ihrer Inhalte auf verschiedenen Betriebssystemen (vgl. Erfolgskriterium 4.1.1 Syntaxanalyse).
- Durchführung von Tests des Webportals auf verschiedenen Geräten zur Gewährleistung einer konsistenten Funktion (vgl. Erfolgskriterium 4.1.1 Syntaxanalyse).
- Sicherstellung, dass Inhalte von Assistenztechnologien wie Screenreadern, Vergrößerungssoftware oder Spracheingabe-Tools interpretiert und genutzt werden können (vgl. Erfolgskriterium 4.1.2 Name, Rolle, Wert).
- Sicherstellung, dass der Code und Markup den aktuellen Webstandards entsprechen und fehlerfrei sind (vgl. Erfolgskriterium 4.1.1 Syntaxanalyse).
- Verwendung von ARIA-Rollen (Accessible Rich Internet Applications) oder Live-Regionen, um Statusmeldungen zu kennzeichnen, die durch ein Skript erzeugt werden. Dies ermöglicht es Screenreadern und anderen Assistenztechnologien solche Meldungen zu erkennen und vorzulesen, ohne dass Nutzer:innen den Fokus verschieben müssen (vgl. Erfolgskriterium 4.1.3 Statusmeldungen).

**Exemplarische Prüfmöglichkeiten**

- Prüfung ob das Webportal:
  - in verschiedenen Webbrowsern mit unterschiedlichen Versionen korrekt funktioniert.
  - auf verschiedenen Geräten wie z.B. Laptops, Tablets oder Smartphones korrekt angezeigt wird.
  - mit verschiedenen Hilfstechnologien wie Bildschirmlesegeräten, Spracheingabesoftware und speziellen Eingabegeräten kompatibel ist.
- Validierung des HTML/CSS-Codes z.B. mit Hilfe des WAVE Web Accessibility Evaluation Tools.

47 Mozilla Foundation (o.J): Firefox Browser, https://www.mozilla.org/de/firefox/, letzter Aufruf 24.08.23

48 Eloston (o.J.): Ungoogled Chromium, https://github.com/ungoogled-software/ungoogled-chromium, letzter Aufruf 24.08.23

## 2.3.2 Gender Mainstreaming

**Hintergrund**

Gender Mainstreaming ist ein politisches Konzept und Instrument, dessen Ziel es ist, Geschlechtergerechtigkeit und faire Lebens- und Arbeitsbedingungen zu schaffen[49]. Der Begriff wurde erstmals auf der 3. Weltfrauenkonferenz der Vereinten Nationen in Nairobi 1985 als politische Strategie vorgestellt[50]. Es basiert auf der Vorstellung, dass bei der Bewertung der möglichen Auswirkungen von politischen, sozialen und wirtschaftlichen Entscheidungen, die unterschiedlichen Lebensbedingungen von Männern, Frauen und Menschen mit anderen Geschlechtern berücksichtigt werden müssen, da es keine geschlechtsneutrale Wirklichkeit gibt[51] [52]. Ziel ist die Anerkennung der vielfältigen Interessen und Lebenslagen von Männer und Frauen[53]. Das bedeutet nicht, dass alle Geschlechter gleich sind, sondern vielmehr, dass alle Geschlechter gleich behandelt werden sollten, indem die Unterschiede zwischen den Geschlechtern anerkannt werden und sichergestellt wird, dass Unterschiede und Vielfalt in Entscheidungsprozessen berücksichtigt werden.

**Beispiele für Handlungsmöglichkeiten**

- Verwendung gendersensibler Sprache, beispielsweise durch Verwendung der Paarform, Sparform oder von geschlechtsneutralen Formulierungen[54].
- Verwendung geschlechtsneutraler Formulare: z.B. sollte bei Anmelde- oder Kontaktformularen darauf geachtet werden, dass diese geschlechtsneutral sind. Anstatt nur “männlich” und “weiblich” als Optionen anzubieten, können auch ein offenes Textfeld oder weitere Optionen wie “nicht-binär”, “intersexuell” oder “bevorzuge nicht zu sagen” hinzugefügt werden.
- Verwendung geschlechtsneutraler Interaktionen, indem diese und Funktionen auf dem Webportal für alle Geschlechter z.B. gleich einladend und ansprechend sind, indem sie nicht auf Stereotypen basieren oder bestimmte Geschlechter bevorzugen.
- Implementierung eines Feedback-Systems, um Rückmeldungen von Nutzer:innen zu sammeln und kontinuierlich die Geschlechtergerechtigkeit der Webseite zu verbessern.
- Einbindung von Diversität in Bildern und Grafiken.

**Exemplarische Prüfmöglichkeiten**

- Prüfung ob:
  - geschlechtergerechte Sprache verwendet wird, die Männer, Frauen und Menschen mit anderen Geschlechtsidentitäten anspricht.
  - Geschlecherstereotypen vermieden werden (bspw. Frauen sind emotional, sensibel, modeinteressiert. Männer sind stark, mutig, sportinteressiert).
  - Geschlechtervielfalt abgebildet ist und stereotypen vermieden werden (siehe dazu Anhang A „Analyse zur deskriminierungsfreien Bildsprache“).

49 Gender Mainstreaming 2000 - 2017, https://leitstelle-frauen-geschlechtergleichstellung.sachsen-anhalt.de/gleichstellung-als-querschnittsaufgabe/gender-mainstreaming-2000-2017/page, letzter Aufruf 21.08.23

50 Council of Europe (o.J.): What is Gender Mainstreaming, https://www.coe.int/en/web/genderequality/what-is-gender-mainstreaming letzter Aufruf 21.08.2023

51 BmFSFJ (2021): Gender Mainstreaming, https://www.bmfsfj.de/bmfsfj/themen/gleichstellung/gleichstellung-und-teilhabe/strategie-gender-mainstreaming/gender-mainstreaming-80436, letzter Aufruf: 22.08.2023

52 Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (2023): Gender, https://www.bmz.de/de/service/lexikon/gender-57490, letzter Aufruf: 22.08.2023

53 Bundeszentrale für politische Bildung (o.J.): Gender Mainstreaming, https://www.bpb.de/kurz-knapp/lexika/politiklexikon/17522/gender-mainstreaming/, letzter Aufruf: 22.08.2023

54 Magistratsdirektion – Geschäftsbereich Organisation und Sicherheit (MD-OS), Dezernat Gender Mainstreaming und MA 53 (2011): Leitfaden für geschlechtergerechtes Formulieren und eine diskriminierungsfreie Bildsprache, https://www.digital.wienbibliothek.at/wbrup/download/pdf/3302346?originalFilename=true letzter Aufruf 18.08.23

## 3.1 Datensparsamkeit

**Hintergrund**

Mit der Datensparsamkeit wird eine Minimierung der zu erhebenden Informationen angestrebt. Dies hat nicht nur datenschutzkonforme Ziele, sondern trägt auch zur IT-Sicherheit für Nutzer:innen bei, und wirkt sich auch auf die digitale Nachhaltigkeit aus, da ein datensparsamer Prozess ein ressourcenschonender ist. Des Weiteren verfolgt dieses Ziel auch rechtliche Vorgaben, die u.a. aus dem DSG (u.a. §25 und §71) und aus EU-Gesetzen wie der DSGVO (z.B. Art. 5 insb. Abs. 1c, Art. 7 insb. Abs. 1 u. 3, Art. 25 insb. Abs. 2) hervorgehen.

**Beispiele für Handlungsmöglichkeiten**

- Verarbeitung von Daten, die systemseitig abgefragt werden, auf das Minimum reduzieren - ggf. unnötige Erhebungen, die nicht zielführend sind, zu streichen/entfernen.
- Minimierung von Abfragen und Speicherungen von personenbezogenen Daten, die nicht benötigt werden, damit diese nicht von Dritten während der Übermittlung bzw. von der Datenbank gestohlen werden können.
- Anwendung des Need-to-Know-Prinzips: Nur Informationen, die für die Bearbeitung einer Anfrage benötigt werden, erfragen. Dabei Beachtung des besonderen Schutzbedarfs der Daten im Bereich Gesundheitsversorgung, Pflege und für zugehörige Beratungsangebote.
- Gültigkeit von Cookies auf ein Minimum und Hinterfragung von Notwendigkeit von darin gespeicherten Daten[55].
- Deaktivierung von standardmäßiger Verarbeitung persönlicher Daten im Cookie-Manager (Opt-In statt Opt-Out). Z.B. Konfiguration des Cookie-Managers so, dass by Default lediglich die technisch und forensisch notwendigen Daten gespeichert werden (ebd.).
- Konfiguration von Gestaltung und Funktionen des Webportals, auf eine Weise, damit die Navigation kurzwegig ist und zielführende Bezeichnungen enthält. Vermeidung von redundanten Inhalten auf mehreren Seiten, sowie die zu ladenden Datenmenge auf einzelnen Seiten minimalistisch halten.
- Verkleinerung von Datengrößen bei Bild- und Audio-Dateien, indem diese vor dem Hochladen in einem Open Source-Bearbeitungsprogramm auf eine dem Zweck angemessene Auflösung reduziert werden.
- Nutzung trackingfreier Alternativen, damit Daten Dritter nicht geladen werden müssen, bspw. durch Einbetten von iFrames bzw. youtube-nocookie (Achtung: Nur mit zusätzlichem Cookie Layer mit weiterem Hinweis auf Google weitestgehend noch DSGVO-konform). Videos können z.B. auch alternativ über invideous.io abgerufen werden.

**Exemplarische Prüfmöglichkeiten**

- Untersuchung des Webportals auf weitere mögliche Dateneinsparungen durch statische Analysen über Privacy Score Beta (https://Privacy Score Beta.org/) und Webbkoll Dataskydd (https://webbkoll.dataskydd.net/) sowie durch dynamische Analyse mit Wireshark (https://www.wireshark.org/).
- Prüfen ob:
  - Konfigurationen von Video- und Audio-Software by Default so eingestellt sind, dass Bild- und Tonübertragungen sowie Mikrofone zu Beginn deaktiviert sind und nur nach Bedarf aktiviert werden.
  - lokale bzw. nationale Anwendung als Alternative für Online-Dienste zur Verfügung

55 IONOS SE (2022): Die Umsetzung der EU-Cookie-Richtlinie in Deutschland, https://www.ionos.de/digitalguide/websites/online-recht/cookie-richtlinie/, letzter Aufruf 24.02.23

gestellt werden können: Z.B. OpenStreetMap[56] für Kartenmaterial, metager[57] als Suchmaschine, DeepL[58] für Übersetzungen oder Jitsi[59] bzw. BigBlueButton[60] für Videokonferenzen.

In Anhang C „Checkliste zu Datensparsamkeit für Webportale“ befindet sich eine kommentierte Spurenkarte, die als Grundlage für eigene Untersuchungen in Bezug auf Datensparsamkeit dienen kann.

56 OpenStreetMap: https://www.openstreetmap.org, letzter Aufruf 22.08.23
57 SUMA-EV (2023): MetaGer, https://metager.de/, letzter Aufruf 24.08.23
58 Lingee GmbH (2017): DeepL, https://www.deepl.com/translator, letzter Aufruf 24.08.23
59 Jitsi: https://jitsi.org/, letzter Aufruf 22.08.23
60 BigBlueButton, https://bigbluebutton.org/, letzter Aufruf 24.08.23

## 3.2 Drittanbieterfreiheit

**Hintergrund**

Für einen langfristigen Betrieb von Portalen, sollte vermieden werden, dass dafür verwendete Dienste und andere Soft- bzw. Hardware-Lösungen zu sehr von den Leistungen Dritter abhängig sind. Denn diese Nutzung bedeutet, dass Veränderungen, welche sich auf die weitere Systemlandschaft auswirken, meist außerhalb des Einflusses des Portalbetreibenden liegen. Dies kann zu hohen Aufwänden und Kosten wegen nötiger Anpassungen und Wechsel von peripheren Faktoren führen (siehe z.B. auch Vendor Lock-In in Kapitel 2.2). Unter Umständen können derartige Lösungen auch die Datensouveränität der Besucher:innen gefährden. Dies besteht insbesondere dann, wenn Dienste von Unternehmen involviert werden, bei denen die Kommerzialisierung von Nutzungsdaten Teil der Firmenpolitik ist.

**Beispiele für Handlungsmöglichkeiten**

- Aufrechterhaltung von Kontakten zu Vertragspartnern:innen und eigenem Fachpersonal, um über neue Abschlüsse und Änderungen informiert zu sein. Besprechung von Unklarheiten bzw. Planung von Alternativen mit allen beteiligten Personen.
- Dokumentation über laufende Programme und Dienste sowie deren Prozesse und Zusammenhänge, damit Abhängigkeiten zwischen ihnen erkannt und durch Wechsel absehbar werden können.
- Definition von Standards, Bedingungen sowie Anwendungszwecke und -ziele für Software, die genutzt wird.
- Nutzung von Open Source Alternativen, deren Quellcodes einseh- und bei Bedarf anpassbar sind.
- Verwendung lokaler Anwendungen (on-premises) auf dem Portal
- Exemplarische Regelungen für Clouds[61]:
  - Nachvollziehbarkeit durch Transparenz: Datenschutzrechtliche Pflichten im Sinne der Nutzenden effektiv, nachprüfbar und dauerhaft umsetzen.
  - Datenhoheit und Steuerung: Nutzer:innen ermöglichen bei der Verwendung von Clouds die Kontrolle über ihre Daten zu behalten.

**Exemplarische Prüfmöglichkeiten**

- Regelmäßige Prüfung der Verbindlichkeiten und Laufzeiten bzw. Änderungen in Verträgen, AGBs und Datenschutzerklärungen von externen Dienstleistern.
- Nutzung der Browsererweiterung "NoScript", das Webseiten-Analysetool "webbkoll.dataskydd", "Privacy Score" und lokale Werkzeuge zur Netzwerkanalyse, um Dienste und Datenpakete Dritter auf dem Online-Portal sichtbar werden zu lassen und diese damit ggf. gezielt zu entfernen.
- Einrichtung von Programmen, die zum Blockieren von unerwünschten bzw. schadhafter Daten genutzt werden (z.B. Pi-Hole durch Raspberry Pi), womit auch ein Monitoring der (abgelehnten) externen Dienstanfragen möglich ist[62].

61 DSK (Datenschutzkonferenz) (2023): Kriterien für Souveräne Clouds, Positionspapier der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 11. Mai 2023, https://www.datenschutzzentrum.de/uploads/dsk/2023-05-11_DSK-Positionspapier_Kritierien-Souv-Clouds.pdf , letzter Aufruf 11.08.23

62 Kuketz, Mike (2017): Pi-hole: Schwarzes Loch für Werbung – Raspberry Pi Teil1, https://www.kuketz-blog.de/pi-hole-schwarzes-loch-fuer-werbung-raspberry-pi-teil1/, letzter Aufruf 16.08.23

## 3.3 Kontrolle und Information der Nutzer:innen

**Hintergrund**

Im Mittelpunkt des Webportals steht die Nutzenden, die den Dienst in Anspruch nehmen. Der vertrauliche und selbstbestimmte Umgang von Nutzer:innen mit dem Webportal setzt voraus, ihnen Informationen an die Hand zu geben und Möglichkeiten einzuräumen, die Weitergabe und Erfassung der eigenen Daten zu kontrollieren.

Darüber hinaus ist es auch interessant, Nutzenden an dieser Stelle die Möglichkeit zu geben, Missbrauch der eigenen Daten oder eines Zugangskontos zu melden, um schnellstmöglich zu reagieren und den Schaden zu begrenzen.

Neben strengeren Regeln in Bezug auf Transparenz von Werbung, sollen mit dem DSA (Digital Service Act)[63] des Europäischen Parlaments und des Rates voraussichtlich ab 2024 auch strafrechtlich relevante Inhalte zielführender verfolgt werden. Daher sollten u.a. Kommentare und andere Beträge von Nutzer:innen regelmäßig auf illegale Inhalte geprüft und diese unter Beachtung des Zusammenspiels von Meinungsfreiheit und Zensur geeignet behandelt und ggf. konsequent gelöscht oder partiell kommentiert werden.

**Beispiele für Handlungsmöglichkeiten**

- Schaffung von Interventionsmöglichkeiten, die z.B. die informationelle Selbstbestimmung vor und nach Einwilligungen unterstützen[64].
- Ermöglichung eines Zugangs zu Informationen zur Erkundigung und Kontrolle über Preisgabe und Weiterleitung von Daten für Portalnutzende.
- Überlassung der Datenhoheit bei Nutzer:innen.
- Löschung von unangebrachten und strafrechtlich relevanten Inhalten, z.B. Beeinflussung/Gefährdung der öffentlichen Sicherheit oder von Wahlprozessen, Hate Speech, Risiken für Minderjährige.
- Einrichtung von bedienerreundlichen Verfahren, mit denen Nutzer:innen illegale Inhalte melden können.

**Exemplarische Prüfmöglichkeiten**

- Prüfung ob Mechanismen zur Wahrung der informationellen Selbstbestimmung im Bezug auf personenbezogene Daten vorhanden und funktionsfähig sind. Diese Mechanismen können technischer oder organisatorischer Natur sein.
- Prüfung ob Mechanismen zum Melden (durch Nutzer:innen) und Entfernung (durch Moderator:innen) von unangebrachten und strafrechtlich relevanten Inhalten vorhanden und funktionsfähig sind.

63 Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) und zur Änderung der Richtlinie 2000/31/EG, 52020PC0825, https://eur-lex.europa.eu/legal-content/de/TXT/?uri=COM%3A2020%3A825%3AFIN, letzter Aufruf 17.08.23

64 Degeling, Martin / Herrmann, Thomas (2018): Intervenierbarkeit zum Schutz informationeller Selbstbestimmung, In: Roßnagel, Alexander / Friedewald, Michael / Hanson, Marit (Hrsg.) (2018): Die Fortentwicklung des Datenschutzes - Zwischen Systemgestaltung und Selbstregulierung, S. 193-208, https://link.springer.com/content/pdf/10.1007/978-3-658-23727-1.pdf, letzter Aufruf 27.07.23

## 3.4 Verschlüsselte Kommunikation

**Hintergrund**

Mit der Verschlüsselung[65] der Kommunikation zwischen zwei oder mehr Rechnern, wird die Vertraulichkeit der Daten sicher gestellt. Mittels einer Ende-zu-Ende Verschlüsselung kann dem Ausspähen von (Meta)Daten oder Man-in-the-middle-Angriffe vorgebeugt werden.

**Beispiele für Handlungsmöglichkeiten**

- Implementierung von TLS (Transport Layer Security)[66] [67] bzw. SSL Protokolle[68], um Kommunikation zwischen Webclient und Webserver per HTTPS zu ermöglichen.
- Sicherung der E-Mails mit PGP-Verschüsselung bzw. durch Verwendung der POP3S- und SMTPS-Protokolle.
- Verschlüsselung sensibler Daten wie z.B. Passwörter, die auf dem Server gespeichert werden, vorab mit Hash- und Salt-Algorithmen.
- Anpassung des Umfangs von Algorithmen je nach Sensibilität und Lebensdauer der Daten. Dies kann ausschlaggebend für die Rechenzeit und Datensparsamkeit sein.
- Verschlüsselung von "Data-in-motion" asymmetrisch und "Data-in-rest" symmetrisch.
- Sicherstellung, dass Verschlüsselungen von Zeit zu Zeit erneuert werden können.
- Anpassung von Verschlüsselungsalgorithmen und -längen auf aktuellen Stand der Technik sicherstellen (Verschlüsselungsagilität[69]).
- Überprüfungsprotokolle führen, um bspw. den Verlauf, den Zyklus und Zugriffszeiten von Kommunikationsdaten zu überwachen, sowie Erstellungs- und Enddatum von Schlüsseln im Überblick zu behalten.
- Verwendung von lokalem Verwaltungsdienst in einem Hardware Security Module (HSM)[70] zur Verwaltung und Sicherung der Schlüssel sowie Durchführung regelmäßiger Backups[71]

**Exemplarische Prüfmöglichkeiten**

- Prüfung, dass den URLs in der Adressleiste ein "https://" vorangestellt ist.
- Prüfung des Systems auf ein geeignetes Schlüsselmanagement sowie Einflussfaktoren für kryptografische Verfahren und Produkte[72].

65 Bundesamt für Sicherheit in der Informationstechnik (o.J.): Datenverschlüsselung, https://www.bsi.bund.de/dok/6682166, letzter Aufruf 20.07.23

66 Bundesamt für Sicherheit in der Informationstechnik (o.J.): Mindeststandard des zur Verwendung von Transport Layer Security (TLS), https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html, letzter Aufruf 19.07.23

67 Bundesamt für Sicherheit in der Informationstechnik (2023): Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=6, letzter Aufruf 19.07.23

68 Bundesamt für Sicherheit in der Informationstechnik (o.J.): (Secure Sockets Layer) SSL, https://www.bsi.bund.de/SharedDocs/Glossareintraege/DE/S/SSL.html, letzter Aufruf 19.07.23

69 Bundesamt für Sicherheit in der Informationstechnik (2019): TR-03107-1 Elektronische Identitäten und Vertrauensdienste im E-Government Teil 1, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.html, letzter Aufruf 17.08.23

70 Schwichtenberg, Holger (o.J.): Hardware Security Module (HSM), https://www.it-visions.de/glossar/components/8964/Hardware_Security_Module.aspx, letzter Aufruf 20.07.23

71 Bundesamt für Sicherheit in der Informationstechnik (o.J.): Back-up: Doppelt gesichert hält besser, https://www.bsi.bund.de/dok/10655274, letzter Aufruf 20.07.23

72 Bundesamt für Sicherheit in der Informationstechnik (2021): Checklisten zum IT-Grundschutz-Kompendium (Edition 2021), ITGS-Check_CON.1 Kryptokonzept, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/checklisten_2021.html, letzter Aufruf 17.08.23

## 3.5 Passwörter

**Hintergrund**

Passwörter bieten oftmals Zugangsdaten zu einer Vielzahl an sensiblen und persönlichen Daten. Daher sollte diese Zeichenreihenfolge geheim gehalten werden, als auch komplex und abstrakt sein, damit sie möglichst schwierig her- oder ableitbar sind. Seitenbetreibende stehen in der Verantwortung, derartige Daten möglichst schwer zugängig und die Zeichenreihenfolge verfremdet gesichert werden. Damit wären Passwörter selbst im Fall eines Datendiebstahls nutzlos[73] [74].

**Beispiele für Handlungsmöglichkeiten**

- Festlegung von Mindestanforderungen für ein Passwort wie z.B. Zeichenlänge, Sonderzeichen und Zahlen fest. Und Einrichtung eines visuellen Feedbacks für Nutzer:innen über die Sicherheitsstufe des favorisierten Passworts.
- Passworteingabe mit verdeckten Zeichen auf dem Bildschirm als Voreinstellung.
- Festlegung von Ablaufzeiten, nach denen Nutzer:innen ihr Passwort ändern können. Und darlegen, wann es geändert werden sollte[75].
- Integrierung einer Zweifaktorauthentifizierung bei Passwortabfragen.
- Verwendung von sicheren „gesalzenen“ Hash-Funktionen wie z.B. SHA um Passwörter von Nutzer:innen in einer zufälligen Zeichenketten auf dem Server zu speichern[76].
- Erstellung einer Passwortrichtlinie als Standard und Orientierungshilfe für alle interne und externe Nutzer:innen.
- Einrichtung von Brute-Force-Schutzmechanismen wie z.B. Rate-Limiting oder tem-poräre Account-Sperrung ein.

**Exemplarische Prüfmöglichkeiten**

Eine Prüfung mittels technischer Maßnahmen ist hier schwierig.

73 Bundesamt für Sicherheit in der Informationstechnik (oJ.): Sichere Passwörter erstellen, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html, letzter Aufruf 24.07.23

74 Bundesamt für Sicherheit in der Informationstechnik (oJ.): Passwörter Schritt-für-Schritt merken, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/Umgang-mit-Passwoertern/umgang-mit-passwoertern_node.html, letzter Aufruf 24.07.23

75 Bundesamt für Sicherheit in der Informationstechnik (2023): IT-Grundschutz- Kompendium - ORP.4.A8 Regelung des Passwortgebrauchs (ORP.4, S. 3), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf, letzter Aufruf 24.07.23

76 Bundesamt für Sicherheit in der Informationstechnik (2023): Technische Richtlinie TR-02102-4 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-4.pdf, letzter Aufruf 24.07.23

## 3.6 Anonymisierung und Schutz der Identität

**Hintergrund**

Wenn Eingaben von personenbezogenen Daten aus verschiedenen Gründen verlangt und gespeichert werden, ist man aus der Sicht der Portalbetreibenden in der Verantwortung, diese Eingaben z.B. zu anonymisieren, damit sie nicht mehr unter den Grundsätzen des Datenschutzes fallen (vgl. DSGVO, Erwägungsgrund 26, insb. Satz 5).

Zu personenbezogenen Daten gehören u.a. Vor- und Nachname, Postleitzahl, sowie kulturelle Herkunft, politische als auch religiöse Überzeugungen, Gesundheit und Sexualität. Die verbleibenden Daten dürfen durch Kombination mit anderen Datenquellen nicht wiederbringlich vervollständigt werden können. Nach Urteil des EuGH handelt es sich auch bei dynamischen IP-Adressen von Besuchenden der Internetseite um personenbezogene Daten (vgl. Rechtssache C-582/14).

Mit Anonymisierungen von Datensätzen wird es Dritten erschwert, die darin enthaltenen sensiblen und personenbeziehbaren Daten abzuleiten und darauf gespeicherten Identitäten vor ihnen zu schützen.

**Beispiele für Handlungsmöglichkeiten**

- Aggregierung von Dateien, um unterschiedliche Daten schwerer voneinander trennen zu können.
- Vergröbern von konkreten Details in Daten, z.B. durch Anlegen weiterer ähnlicher Daten, damit sie weniger zielführend auf einen bestimmten Datensatz zurückzuführen ist (z.B. bei auffälligen Persönlichkeitsmerkmalen im Kontext zur restlichen Datenbank). Dies kann bspw. dadurch erreicht werden, indem genaue Angaben lediglich in eine weniger detaillierte Bereichsangabe erfasst bzw. umgewandelt wird (z.B. Körpergröße zwischen 160-170cm).
- Bilddateien für Außenstehende bzw. für Unautorisierte verpixeln.
- Entpersonalisieren: partielle Unkenntlichkeit von Gesichtspartien oder vollständiges verpixeln.
- Pseudonomisierung oder Anonymsierung von personenbezogenen Daten[77] [78].
- Datenbanken lediglich für konkrete Verantwortungsbereiche zugängig machen und Listen über Datenbanken und Autorisierungen führen.

**Exemplarische Prüfmöglichkeiten**

- Überprüfung, welche Daten als (nicht) angemeldeter Nutzer:innen auf ihrem Webportal einsehbar sind und welche nicht.
- Überprüfung, ob sensible Daten über Suchmaschinen auffindbar sind.
- Nutzung von Suchmaschinen, um nach Dokumenten zu suchen, die nicht für die Öffentlichkeit bestimmt sein sollten.
- Prüfung der Datensätze, ob die Erstellung von Profilen durch plattformübergreifende Informationen durch Dritte verbindbar bzw. hergeleitet werden können (Linkability und Inferenz).

77 EDPB (2014): ARTICLE 29 DATA PROTECTION WORKING PARTY - THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, https://iapp.org/media/pdf/resource_center/wp216_Anonymisation-Techniques_04-2014.pdf, letzter Zufriff 24.08.23

78 BfDI (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit) (2020): Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, letzter Aufruf 25.08.23

# Anhang A: Analyse zur diskriminierungsfreien Bildsprache[79]

| Kategorie | Kriterium | Beispiele | Messung |
|---|---|---|---|
| Geschlecht | Gleichwertige Abbildung von Frauen und Männern in visuellen Medien und Grafiken. | Mann, der mit dem Kind auf den Spielplatz geht; Mann als pädagogische Fachkraft in der Kita; Frauen in höheren beruflichen Positionen oder Frauen in technischen Berufen. | Prüfung der dargestellten Personen auf Körperhaltung, Anordnung der Personen (wer steht im Vordergrund) oder Blicke (wer schaut in die Kamera, wer schaut weg). |
| Alter | Differenzierte Darstellung von jungen und älteren Menschen. | Ältere Menschen, die sich um Kinder kümmern, einen Computerkurs besuchen oder Fahrrad fahren; junge Menschen beim Lernen, beim Helfen anderer Menschen oder beim Wählen. | Überprüfung der Altersverteilung der dargestellten Personen sowie der Vielfalt der dargestellten Aktivitäten und Rollen. |
| Menschen mit Behinderung | Differenzierte Darstellung von Menschen mit Behinderungen. | Bei der bildlichen Anordnung von Menschen mit und ohne Behinderung begegnen sich die Personen auf gleicher Augenhöhe. | Überprüfung, ob Menschen mit Behinderungen in einer Vielzahl von Kontexten und auf gleicher Augenhöhe mit anderen dargestellt werden. |
| Sexuelle Orientierung | Vermeidung klischeebehafteter Bilder und Verwendung differenzierter Darstellungen. | Lesbische Frauen und schwule Männer in einer Vielzahl von Rollen und Kontexten, beispielsweise beim Einkaufen, Sport treiben oder Kinderbetreuung. | Überprüfung, ob die Bilder Klischees vermeiden und eine Vielzahl von Rollen und Kontexten für lesbische Frauen und schwule Männer darstellen. |
| Menschen unterschiedlicher Herkunft/ Kultur/Religion | Differenzierte Darstellung von unterschiedlicher Herkunft/Kultur/Religion. | Junge Menschen aus unterschiedlichen Ländern an der Universität; Künstler:innen mit Migrationshintergrund; eine afrikanische Geschäftsfrau. | Überprüfung, ob die Bilder eine Vielzahl von Kulturen, Religionen und Herkünften repräsentieren und ob sie Klischees vermeiden. |

79 Magistratsdirektion – Geschäftsbereich Organisation und Sicherheit (MD-OS), Dezernat Gender Mainstreaming und MA 53 (2011): Leitfaden für geschlechtergerechtes Formulieren und eine diskriminierungsfreie Bildsprache, https://www.digital.wienbibliothek.at/wbrup/download/pdf/3302346?originalFilename=true letzter Aufruf 18.08.23

## Anhang B: Analyse von Webportalen bezügl. WCAG mit W3C Easy Check

Testseite: [URL des Webportals eintragen]
Testdatum: [Datum des Tests eintragen]
Browser: [genutzten Browser inkl. Version eintragen]
Tool: [Verwendete Tools eintragen (bspw. Bookmarklet HTML-Codesniffer; Plugins: Wave, WCAG Color Contrast Checker, HeadingsMap, taba11y)]

Die nachfolgenden Checks enthalten nur einige Aspekte der digitalen Barrierefreiheit und sind an den Easy Checks der W3C angelehnt[80]. Für eine vollständige Überprüfung sollten manuelle Tests durch Expert:innen durchgeführt werden und Feedback der Nutzer:innen eingeholt werden.

Beispieltools zur Überprüfung der Barrierefreiheit

1. HTML-Codesniffer[81]
   - Ursprung: squizlab
   - Version: 2.5.1

2. WAVE Web Accessibillity Evaluation Tool[82]
   - Ursprung: WebAIM – Firefox Extension
   - Version: 3.2.4.1

3. taba11y[83]
   - Ursprung: Peter Gould
   - Version: 1.20

4. HeadingsMap[84]
   - Ursprung: Jorge Rumoroso
   - Version: 4.5.5

5. WCAG Contrast checker[85]
   - Ursprung: Jorge Rumoroso
   - Version: 3.7.2

80 W3C (2023) Easy Checks – A First Review of Web Accessibility, https://www.w3.org/WAI/test-evaluate/preliminary/, letzter Aufruf 28.08.23
81 Squizlab, HTML-Codesniffer, ttp://squizlabs.github.io/HTML_CodeSniffer/, letzter Aufruf 06.07.23
82 WebAIM, WAVE Web Accessibillity Evaluation Tool, https://addons.mozilla.org/en-US/firefox/addon/wave-accessibility-tool/, letzter Aufruf 06.07.23
83 Peter Gould, taba11y, https://chrome.google.com/webstore/detail/taba11y/aocppmckdocdjkphmofnklcjhdidgmga, letzter Aufruf 16.08.23
84 Jorge Rumoroso, HeadingsMap, https://chrome.google.com/webstore/detail/headingsmap/flbjommegcjonpdmenkdiocclhjacmbi, letzter Aufruf 16.28.23
85 Ders., WCAG Contrast checker, https://addons.mozilla.org/de/firefox/addon/wcag-contrast-checker/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search, letzter Aufruf 16.08.23

| Fehlerkategorie | Beschreibung des Fehlers | Methodik | Anzahl der Fehler | Fehlerort | Fehlercode nach WCAG 2.1 | Metrik / Bewertung | Standard / Optimaler Zustand | Empfohlene Lösung |
|---|---|---|---|---|---|---|---|---|
| **Seitentitel** | Wenn der Seitentitel nicht relevant oder genau ist, kann dies für Nutzer:innen verwirrend sein und die Auffindbarkeit der Seite in Suchmaschinen beeinträchtigen. | Seitentitel-Überprüfung mit dem WAVE-Plugin. | [Anzahl der gefundenen Fehler eintragen] | [Eintragung Fehlerort]<br><br>Beispiel:<title> Titelname </title> im <head>-Bereich des HTML-Dokuments | 2.4.2 – Seitentitel – Level A | [Beschreibung von Unterschieden zwischen Spalte „Fehlerort“ und optimalen Zustand (siehe Spalte rechts) in Form eines gemessenen Wertes oder Texts.]<br><br>Beispiel:<br>“Seite 1” oder “Unbenanntes Dokument” (Da Seitentitel den Inhalt der Seite nicht relevant beschreibt) | Der Seitentitel beschreibt den Inhalt der Seite genau und ist relevant (konform). | Sicherstellung, dass jeder Seitentitel den Inhalt der Seite genau beschreibt und für Nutzer:innen relevant ist. |
| **Alt-Text** | Bilder ohne Alternativtext sind für Benutzer:innen, die Bildschirmlesegeräte verwenden oder Bilder deaktiviert haben, nicht zugänglich. | Bildalternativtext-Überprüfung mit dem WAVE-Plugin oder HTML_CodeSniffer. | [Anzahl der gefundenen Fehler eintragen] | [Eintragung Fehlerort]<br><br>Beispiel:<br><img src="beispiel.jpg"> | 1.1.1 – Nicht-Text-Inhalt – Level A | [Beschreibung von Unterschieden zwischen Spalte „Fehlerort“ und optimalen Zustand (siehe Spalte rechts) in Form eines gemessenen Wertes oder Texts.]<br><br>Beispiel:<br>3 Bilder auf der Landing Page haben keinen Alternativtext (nicht konform) | Bilder, die keinen Inhalt vermitteln, dekorativ sind oder Inhalte enthalten, die bereits durch Text vermittelt werden, erhalten einen leeren Alternativtext (alt="") ansonsten sollten sie beschreiben, was auf dem Bild zu sehen ist | Hinzufügen von Alternativtexten zu allen Bildern, die den Inhalt und den Zweck jedes Bildes genau beschreiben |

| Fehlerkategorie | Beschreibung des Fehlers | Methodik | Anzahl der Fehler | Fehlerort | Fehlercode nach WCAG 2.1 | Metrik / Bewertung | Standard / Optimaler Zustand | Empfohlene Lösung |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| **Überschriften** | Eine unklare oder inkonsistente Überschriftenstruktur kann die Navigation und das Verständnis der Seite erschweren. | Überschriftenstruktur-Überprüfung mit dem WAVE-Plugin oder HTML_CodeSniffer oder Browsererweiterung HeadingsMap | [Anzahl der gefundenen Fehler eintragen] | [Eintragung Fehlerort]<br>Beispiel:<br><h1>Überschrift 1</h1><br><br><h3>Überschrift 3</h3><br><br><h2>Überschrift 2</h2> | 2.4.6 – Überschriften und Beschriftungen – Level AA | [Beschreibung von Unterschieden zwischen Spalte „Fehlerort“ und optimalen Zustand (siehe Spalte rechts) in Form eines gemessenen Wertes oder Texts.]<br><br>Beispiel:<br>Die Überschriftenstruktur ist unklar und inkonsistent. In diesem Beispiel wird die Überschriftenebene 2 nach der Überschriftenebene 3 verwendet, was gegen die logische Reihenfolge verstößt. (nicht konform) | Die Überschriftenstruktur ist klar und konsistent, wobei jede Überschrift den Inhalt des entsprechenden Abschnitts genau beschreibt, indem nur eine Hauptüberschrift (h1) existieren darf, auf die eine Überschrift (h2) und im weiteren Verlauf des Inhalts wiederum entweder eine weitere h2 oder eine h3 folgen darf. | Überarbeitung der Überschriftenstruktur, um Klarheit und Konsistenz zu gewährleisten, wobei jede Überschrift den Inhalt des entsprechenden Abschnitts genau beschreibt. |
| **Kontraste** | Text mit unzureichendem Kontrast zur Hintergrundfarbe kann für Benutzer:innen mit Sehbehinderungen schwer zu lesen sein. | Kontrastverhältnismessung mit dem HTML_CodeSniffer oder automatische Messung mit dem WAVE-Plugin. | [Anzahl der gefundenen Fehler eintragen] | [Eintragung Fehlerort]<br><br>Beispiel Fehlerort:<br><br><a href="https://beispielseite.de/beispiel/">Beispiel...</a> | 1.4.3 – Kontrast (Minimum) – Level AA | [Beschreibung von Unterschieden zwischen Spalte „Fehlerort“ und optimalen Zustand (siehe Spalte rechts) in Form eines gemessenen Wertes oder | Das Kontrastverhältnis zwischen Text und Hintergrund ist mindestens 4.5:1 für normalen Text und 3:1 für großen Text | Anwendung des WCAG Color Contrast Checkers zur Überprüfung und Anpassung des Kontrastverhältnisses, bis es mindestens 4.5:1 für normalen Text und 3:1 für großen |

| Fehlerkategorie | Beschreibung des Fehlers | Methodik | Anzahl der Fehler | Fehlerort | Fehlercode nach WCAG 2.1 | Metrik / Bewertung | Standard / Optimaler Zustand | Empfohlene Lösung |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Texts.]<br><br>Beispiel: Kontrastverhältnis 1.5:1 | | Text beträgt. |
| **Textvergrößerung** | Wenn der Text bei Vergrößerung Informationen verliert oder unzugänglich wird, ist dies ein Zeichen dafür, dass die Seite nicht richtig auf verschiedene Bildschirmgrößen und Zoomstufen reagiert. werden kann1. | Manueller Test, indem Seite mit der Zoomfunktion des Browser auf Skalierbarkeit überprüft wird | [Anzahl der gefundenen Fehler eintragen] | [Eintragung Fehlerort]<br><br>Beispiel:<br>Unterer Drittel der Landing Page | 1.4.4 – Textgröße ändern – Level AA | [Beschreibung von Unterschieden zwischen Spalte „Fehlerort“ und optimalen Zustand (siehe Spalte rechts) in Form eines gemessenen Wertes oder Texts.]<br><br>Beispiel:<br>Informationen von Texten bei einer Vergrößerung ab 175% | Der Text bleibt bei Vergrößerung auf bis zu 200% ohne Informations- oder Funktionsverlust zugänglich | Durchführung von Tests auf verschiedenen Zoomstufen und Bildschirmgrößen, um sicherzustellen, dass der Text bei Vergrößerung immer noch zugänglich ist. |
| **Tastaturbedienbarkeit** | Wenn Interaktionselemente nicht über die Tastatur erreichbar oder sichtbar sind, können sie für Benutzer:innen, die keine Maus verwenden können oder wollen, unzugänglich sein. | Tastaturzugriffs- und visueller Fokus-Test mit dem WAVE-Plugin oder HTML_CodeSniffer oder Brwosererweiterung taba11y | [Anzahl der gefundenen Fehler eintragen] | [Eintragung Fehlerort]<br><br>Beispiel:<br>Spezifisches Interaktionselement (z.B. Link, Schaltfläche, Formulareingabe) | 2.4.7 – Fokus sichtbar – Level AA | [Beschreibung von Unterschieden zwischen Spalte „Fehlerort“ und optimalen Zustand (siehe Spalte rechts) in Form eines gemessenen Wertes oder Texts.]<br><br>Beispiel:<br>Verlinktes Video | Alle Interaktionselemente sind über die Tastatur erreichbar und der visuelle Fokus ist deutlich sichtbar | Durchführung einer Überprüfung mit der Tastatur, um sicherzustellen, dass alle Interaktionselemente erreichbar sind und der visuelle Fokus deutlich sichtbar ist. |

| Fehlerkategorie | Beschreibung des Fehlers | Methodik | Anzahl der Fehler | Fehlerort | Fehlercode nach WCAG 2.1 | Metrik / Bewertung | Standard / Optimaler Zustand | Empfohlene Lösung |
|---|---|---|---|---|---|---|---|---|
| | | | | | | ist nicht über die Tastatur erreichbar | | |
| **Formulare** | Unklare oder fehlende Beschriftungen (Labels) und Fehlermeldungen können die Benutzung von Formularen erschweren. | Formular-, Beschriftungs (Labels)- und Fehlerüberprüfung mit dem WAVE-Plugin oder HTML_CodeSniffer. | [Anzahl der gefundenen Fehler eintragen] | [Eintragung Fehlerort]<br><br>Beispiel:<br>Spezifisches Interaktionselement (z.B. <label for="email">Geben Sie Ihren Namen ein:</label> <input type="email" id="email" name="email">) | 3.3.2 – Beschriftungen (Labels) oder Anweisungen – Level A | [Beschreibung von Unterschieden zwischen Spalte „Fehlerort“ und optimalen Zustand (siehe Spalte rechts) in Form eines gemessenen Wertes oder Texts.]<br><br>Beispiel:<br>Ein Texteingabefeld, das Nutzer:innen auffordert, die eigene E-Mail-Adresse einzugeben hat den Label <label>-Element lautet “Geben Sie Ihren Namen ein” | Alle Formulare haben klare und sichtbare Beschriftungen (Labels) und Fehlermeldungen, die Benutzer:innen helfen, Informationen korrekt einzugeben | Überprüfung aller Formulare auf der Website, um sicherzustellen, dass sie klare und sichtbare Beschriftungen (Labels) und Fehlermeldungen haben. |
| **Bewegte Inhalte** | Wenn bewegte, blinkende oder animierte Inhalte nicht gestoppt, pausiert oder ausgeblendet werden können, kann dies für Benutzer:innen, die von sol- | Identifizierung aller Inhalte, die sich bewegen, blinken oder animiert sind. Dies können Bilder, Videos, Animationen, und andere ähnliche Elemente sein. Prüfung ob diese ge- | [Anzahl der gefundenen Fehler eintragen] | [Eintragung Fehlerort]<br><br>Beispiel:<br><br> <img [...]</p>  | 2.2.2 – Pause, Stopp, Ausblenden – Level A | [Beschreibung von Unterschieden zwischen Spalte „Fehlerort“ und optimalen Zustand (siehe Spalte rechts) in Form eines gemessenen Wertes oder | Alle bewegten, blinkenden oder animierten Inhalte können von Benutzer:innen gestoppt, pausiert oder ausgeblendet wer- | Hinzufügen einer Option zum Stoppen, Pausieren oder Ausblenden der bewegten, Inhalte. |

| Fehlerkategorie | Beschreibung des Fehlers | Methodik | Anzahl der Fehler | Fehlerort | Fehlercode nach WCAG 2.1 | Metrik / Bewertung | Standard / Optimaler Zustand | Empfohlene Lösung |
|---|---|---|---|---|---|---|---|---|
| | chen Inhalten abgelenkt oder überwältigt werden, problematisch sein. | stoppt, pausiert oder ausgeblendet werden können. | | | | Texts.]<br><br>Beispiel:<br>Slideshow als Karussel auf Landing Page lässt sich nicht pausieren. | den | |
| **Videos mit Untertitlung** | Videos ohne Untertitel für gesprochenen Inhalt und wichtige Geräusche sind für Benutzer:innen, die hörgeschädigt sind oder den Ton nicht hören können, nicht zugänglich. | Manuelle Überprüfung, ob Untertitel für die Videos verfügbar sind. | [Anzahl der gefundenen Fehler eintragen] | [Eintragung Fehlerort]<br><br>Beispiel:<br>Spezifische Videos auf dem Portal<br><br><iframe src="https://player.vimeo.com/video/76979871?[…] ></iframe> | 1.2.2 – Untertitel (aufgezeichnet) – Level A | [Beschreibung von Unterschieden zwischen Spalte „Fehlerort“ und optimalen Zustand (siehe Spalte rechts) in Form eines gemessenen Wertes oder Texts.]<br><br>Beispiel:<br>Video auf Landing Page ohne Untertitlung | Alle Videos enthalten Untertitel für gesprochenen Inhalt und wichtige Geräusche | Hinzufügen von Untertiteln bei gesprochenen Inhalt und wichtige Geräusche in allen Videos. |
| **Lesereihenfolge** | Wenn die Reihenfolge, in der Inhalte gelesen werden, nicht sinnvoll ist, kann dies für Benutzer:innen verwirrend sein und das Verständnis der Seite erschweren | Überprüfung der Lesereihenfolge mit der Browsererweiterung taba11y | [Anzahl der gefundenen Fehler eintragen] | [Eintragung Fehlerort]<br><br>Beispiel:<br> <br><h2>Überschrift 1</h2><br><h2>Überschrift 2</h2><br><h2>Überschrift 3</h2> | 1.3.2 – Sinnvolle Reihenfolge – Level A | [Beschreibung von Unterschieden zwischen Spalte „Fehlerort“ und optimalen Zustand (siehe Spalte rechts) in Form eines gemessenen Wertes oder Texts.]<br><br>Beispiel:<br>Lesereihenfolge | Die Reihenfolge, in der Inhalte gelesen werden, ist logisch und sinnvoll, unabhängig davon, ob sie visuell oder durch ein Screenreader gelesen werden | Überprüfung der Reihenfolge, in der Inhalte gelesen werden, sowohl visuell als auch durch ein Screenreader, um sicherzustellen, dass sie logisch und sinnvoll ist. |

| Fehlerkategorie | Beschreibung des Fehlers | Methodik | Anzahl der Fehler | Fehlerort | Fehlercode nach WCAG 2.1 | Metrik / Bewertung | Standard / Optimaler Zustand | Empfohlene Lösung |
|---|---|---|---|---|---|---|---|---|
| | | | | <br> Inhalt zu Überschrift 1 <br> Inhalt zu Überschrift 2 <br> Inhalt zu Überschrift 3 <br> | | des Inhalts ist nicht sinnvoll. Screenreader liest zuerst die Überschriften vor und dann erst die Hauptinhalte. | | |

## Anhang C: Checkliste zu Datensparsamkeit für Webportale

Für die Analyse von Datensparsamkeit existieren diverse digitale Hilfswerkzeuge. U.a. können dazu Online-Tools wie Privacy Score Beta (https://Privacy Score Beta.org/) und Webbkoll Dataskydd (https://webbkoll.dataskydd.net/) unterstützen.

Zudem bietet der Web Evidence Collector (WEC)[86] der European Commission eine lokal installierte Alternative, mit dem Informationen über Verbindungen von einer Internetseite in Form einer HTML-Datei ausgegeben werden können. Um den Netzwerkverkehr breitflächig zu erfassen, können Daten mit dem Monitoring-Tool Wireshark (https://www.wireshark.org/) dokumentiert werden. Letzteres erfasst jedoch nicht ausschließlich den Datenstrom einer einzelnen Internetseite, sondern den gesamten ein- und ausgehenden Netzwerkverkehr des Rechners.

Des Weiteren können Browsererweiterungen bzw. Plugins/Addons von Browsern zur Sichtbarkeit von Verbindungen zu Servern und Drittanbietern unterstützen. Dazu zählen z.B. uBlock Origins (https://ublockorigin.com/) und NoSkript (https://noscript.net/). Die Installation derartiger Analysetools allein reicht jedoch oftmals nicht aus. Häufig müssen diese noch konfiguriert werden. Diverse Browser bieten zudem integrierte Funktionen als „Werkzeuge für Web-Entwickler“, mit dem Netzwerkanalysen auf der besuchten Internetseite ausgeführt werden können.

Um ein möglichst umfassendes Ergebnis zu erhalten, sollten mehrere Werkzeuge eingesetzt werden und ihre Funde untereinander verglichen werden, da häufig ein einziges Tool nicht alle Verbindungen erfasst. Außerdem können Dopplungen von Ergebnissen zur Verifikation des Fundes beitragen.

Die nun folgende Tabelle soll exemplarisch eine Spurensicherung hinsichtlich Datensparsamkeit illustrieren und bei der eigenen Untersuchung unterstützen. Die Erklärungen innerhalb einer Klammer sollen eine Orientierungshilfe für die einzutragende Information im entsprechenden Feldes bieten.

86 Website Evidence Collector, https://joinup.ec.europa.eu/collection/free-and-open-source-software/solution/website-evidence-collector, letzter Aufruf 20.07.23

| Webseite | **[Name der Internetseite eintragen]** | | |
|---|---|---|---|
| Analysetool | **Privacy Score Beta**<br><br>[Gewünschte URL-Webseite im Feld von https://privacyscore.org eingeben]<br><br>[Privacy Score Beta wertet hauptsächlich potentielle Angriffsarten auf Web- und Mailserver aus. Das Tool weist jedoch in den oberen Ergebnissen auch Drittanbieter und potentielle Tracker aus] | **Webbkoll Dataskydd**<br><br>[Gewünschte URL-Webseite im Feld von https://webbkoll.dataskydd.net/de/ eingeben)]<br><br>[Webbkoll Dataskydd wertet neben Drittanbieter auch Cookies und deren Speicherdauer aus. Außerdem prüft es die Header einer Internetseite u.a. auf Richtlinien bezüglich Referrer und Sicherheitsfunktionen] | **EDPS Inspection Software**<br><br>Website-Evidence-Collector (Teil der EDPS Inspection Software)<br><br>Lokale Installation über: https://edps.europa.eu/press-publications/edps-inspection-software_en<br><br>[Das Programm wird nach Installation über die Linux-Terminal ausgeführt. Dazu muss zunächst der Ausgabeort gewählt werden. Anschließend können dort mit einem Befehl die Analysedaten abgelegt werden.<br>Der Befehl lautet bspw. „website-evidence-collector http://beispielsseite.de -newoutput o“<br>(URL muss nach Wunsch angepasst werden)] |
| Bericht | [Vermerk der URL-Webseite, die nach der Analyse in der Adressleiste des Browser steht, um sie später wieder aufrufen zu können, z.B. „https://privacyscore.org/site/6868483825551/] | [Vermerk der URL-Webseite, die nach der Analyse in der Adressleiste des Browser steht, um sie später wieder aufrufen zu können, z.B. https://webbkoll.dataskydd.net/en?url=http%10B%3T%2Ftest-webseite%2F] | [Der Bericht von EDPS WEC befindet in einem neu erstellten Ordner namens „newoutput“. Dieser befindet sich unter dem Pfad, in dem das Programm über die Konsole ausgeführt wurde. Die Ergebnisse sind in der HTML-Datei namens „inspection.html“ zu finden] |
| Geladen aus/ von (URL und Zeitangabe) | [Datum und Uhrzeit des Scans angeben] | [Datum und Uhrzeit des Scans angeben] | [Datum und Uhrzeit des Scans angeben] |
| Bereiche des Webportals | [Um den Überblick über die gesamte Seitenstruktur und Unterseiten zu er- und behalten, sollen hier die einzelnen Menüpunkte und darüber erreichbare Untermenüs der Internetpräsenz eingetragen werden] | | |

<table>
<tr><td></td><td colspan="3">[Z.B.<br>• Willkommen<br>  • Über uns<br>  • Kontaktmöglichkeiten<br>  • Aktuelles<br>  • … weitere Unterseiten des Menüpunkts „Willkommen“<br>• Services<br>  • Formulare<br>  • So finden Sie uns<br>  • Stellenausschreibungen<br>  • … weitere Unterseiten des Menüpunkts „Services“<br>• Veranstaltungen<br>• Barrierefreiheitserklärung<br>• Datenschutzerklärung<br>• Impressum<br>]</td></tr>
<tr><td>Liste mit potentiellen Trackern und Details</td><td><u>Sub Domains -potentielles CNAME- Tracking:</u><br><br>Z.B.<br><br><u>Third party:</u><br>[Eintragen der von Privacy Score Beta gefundenen Drittanbieter]<br>[Siehe in den Ergebnissen unter dem Punkt „Check if 3rd using party embeds are being used“]<br><br><u>Davon lt. Privacy Score Beta bekannte Tracker:</u><br>[Siehe in den Ergebnissen unter dem Punkt „Check if embedded 3rd parties are known trackers“]</td><td><u>Sub Domains -potentielles CNAME- Tracking:</u><br><br>Z.B.<br><br><u>Third party:</u><br>[Eintragen der von Webbkoll gefundenen Drittanbieter]<br><br>[Siehe in den Ergebnissen unter dem Punkt „Third-party requests“]</td><td><u>Sub Domains - potentielles CNAME- Tracking:</u><br><br>Z.B:<br><br><u>Third party:</u><br>[Eintragen der von EDPS WEC gefundenen Drittanbieter]<br><br>[Siehe in den Ergebnissen unter dem Punkt „Third-Party Hosts“]</td></tr>
<tr><td>Cookie-manager</td><td colspan="3">[Eintragen von Einstellungsmöglichkeiten, Inhalten und eigene/fremde Dienste]<br>[Z.B. grundsätzliches Vorhanden sein bzw. Auswahlmöglichkeiten wie (alle) akzeptieren/ abhlehnen, nur notwendige, welche Dienste/Anbieter können (nicht) abgewählt werden. Außerdem können die Funktionen der Anbieter/Dienste vermerkt werden]<br><br>[Jeder Dienst und jede Verbindung von Drittanbietern sollte hier ein- bzw. ausschaltbar sein. Optimal sind „Opt-out“ Einstellungen, bei denen Nutzende dem Dienst / der Verbindung aktiv zustimmen müssen]</td></tr>
</table>

| | | | |
|---|---|---|---|
| Cookies (1st & 3rd Party) und Beacon Hosts | - keine Funktionalität | Ergebnisse und ggf. Unterschiede zu anderen Analyse-Tools<br><br>[Auflistung der Cookies, die gefunden wurden. Vergleich von Funden von Privacy Score Beta und EDPS WEC]<br><br>[siehe „Third-party cookies“]<br><br>[Z.B. Beispielseite.org (Host: beispiel-seite.de), Datei- bzw. Dienstname, (Speicherdauer: 7 Tage bzw. Datum des Verfalls)] | Ergebnisse und ggf. Unterschiede zu anderen Analyse-Tools<br><br>[Auflistung der Cookies, die gefunden wurden. Vergleich von Funden von Privacy Score Beta und Webbkoll]<br><br>[siehe „Cookies linked to Third-Party Hosts“]<br><br>[Z.B. Suchmaschine.com, Art: Recaptcha, (Speicherdauer: 7 Tage bzw. Datum des Verfalls)]<br><br>„Third-Party Web Beacons“ lt. EDPS:<br><br>[Im Gegensatz zu den anderen Tools biete EDPS WEC eine Analyse auf Beacons]<br><br>[siehe „Third-Party Web Beacon Hosts“]<br><br>[Z.B. Beispielseite.org (Host: beispiel-seite.de) (Speicherdauer: 7 Tage)] |
| Vergleich: Unterschiede bei bisherigen Funden mit diversen Analysen | Unterschiede bei potentiellen Tracker:<br><br>[Eintragen von Unterschieden zu webbkoll und Website-Evidence-Collector, um Funde zu verifizieren | Unterschiede bei potentiellen Tracker:<br><br>[Eintragen von Unterschieden zu Privacy Score Beta und EDPS Website-Evidence-Collector] | Unterschiede bei potentiellen Tracker:<br><br>[Eintragen von Unterschieden zu Privacy Score Beta und Webbkoll]<br><br>Unterschiede bei Cookies und Beacons inkl. Speicherdauer:<br><br>[siehe „Third-Party Web Beacon Hosts“. Anschließend vergleichen mit „Cookies linked to Third-Party Hosts“]<br><br>[Z.B. wwww.beispielseite.com (Third Party Beacon) (Speicherdauer: 30 Tage)] |

| | |
|---|---|
| Ergebnisse und Vergleiche durch uBlock | [Diverse Browser bieten über ihre Einstellungen sogenannte Plugins/Addons/Erweiterungen an, mit denen die akutell besuchte (Unter)Seite auf Verbindungen zu First und Third Parties analysiert werden. Dazu zählt auch uBlock Origins.]<br><br>[Um mit uBlock Origins möglichst viele Drittanbieter zu finden, muss der Dienst konfiguriert werden, sowie NoScript als auch der Browserschutz deaktiviert werden. Alternativ sollte die Untersuchung mit einem privaten Browser-Tab wiederhot werden.]<br><br>[Eintragen von Verbindungsanfragen, die mit der Browsererweiterung uBlock festgestellt wurden. Z.B.<br><br><u>Durch uBlock Origins festgestellte Verbindungsaufbauten:</u><br><br><u>„Name der (Unter)Seite“:</u><br>First-Party.com<br>Suchmaschine.com<br>Video-Stream.com<br>Social-Media.org<br>….<br><br><u>„Name der (Unter)Seite“:</u><br>First-Party.com<br>Server-von-Schriftart.org<br>Social-Media.com<br>….<br><br>]<br><br>[Verbindungen in blauer Schrift weisen auf CNAME-Tracker hin. Derartige Verbindungen sind mit zwei Namen angegeben: Einer ist die vorgegebene Adresse, die andere ist die tatsächliche Ursprungsadresse]<br><br><u>Von uBlock Origins identifizierte CNAMES:</u><br>[Z.B. InternetseiteNummer1.com (internet.seite-Nummer2.com)]<br><br>[Optional: Einfügen von Funden, die weder von Privacy Score Beta, noch von Webbkoll und EDPS Web-Evidence-Collector erkannt wurden]<br>[Z.B. „Neu erkannte Verbindungen, die von Webkoll/Privacy Score Beta/EDPS, nicht identifiziert wurden: Suchmaschine.com, Analysetool.org, video-cdn.com] |
| Ergebnisse und Vergleiche durch noscript | [Um mit NoScript möglichst viele Drittanbieter zu finden, muss der Dienst konfiguriert werden als auch der Browserschutz deaktiviert werden. Als Ausgangspunkt sollten alle Verbindungen blockiert werden und erst nach und nach wieder freigegeben werden, um Abhängigkeiten rekonstruieren zu können. Zudem lässt sich so leichter nachvollziehen, welche First oder Third Party für welche HTML-Elemente zuständig sind.]<br><br><u>Durch noscript festgestellte Verbindungsaufbauten:</u><br><br><u>„Name der (Unter)Seite“:</u><br>First-Party.com<br>Suchmaschine.com<br>Videoplattform.com<br>Newsletter-info.org<br>…. |

| | |
|---|---|
| | [Optional: Einfügen von Funden, die weder von Privacy Score Beta, noch von Webbkoll und EDPS Web-Evidence-Collector erkannt wurden]<br>[Z.b. „Neu erkannte Verbindungen, die von Webkoll/Privacy Score Beta/EDPS, nicht identifiziert wurden: suchmaschine.com, Analyse.org, video-cdn.com] |
| Funktions-einschränkungen durch Block-Dienste uBlock und nocscript | [Hier kann festgehalten werden, ob eine adäqate Darstellung der Seite außschließlich durch Verbindungen zwischen Client und Server bzw. der Besuch einer Seite ohne Drittanbieter ermöglicht wird.]<br><br>Bedarf an Anpassungen in der Gestaltung, da durch Blockierungen teilweise bzw. starke Einschränkungen in der Funktionalität vorhanden sind<br><br>Ja ☐ Nein ☐ |
| Wireshark-Ergebnisse und Vergleich | [Wireshark ist ein lokales Monitoirng-Programm mit dem alle ein- und ausgehenden Datenpakete in einem Netzwerk erfasst werden können. Neben vielen anderen Datenströmen, zeichnet das Tool auch den Datenaustausch zwischen Client und Webseiten-Server einer Internetseite auf. Der dokumentierte Datenverkehr kann in einer pcap- oder csv-Datei exportiert werden.] |
| Abgleich mit Datenschutzerklärung der Website | [Prüfung der Datenschutzerklärung auf Nennung und Hinweise zu den Funden (Tracker/ Cookies und Cookiedauer)]<br><br><u>- Welche werden (nicht) benannt:</u><br>[Z.B. „Erwähnungen von: provider.de (Server-Provider), drittanbieter-fuer-schriftarten.org, analystic-tool.com]<br><br><u>- Drittanbieter, die genutzt aber nicht genannt werden:</u><br>[Z.B. „Fehlende Erwähnungen: video-streaming-dienst.com, newsletter-info.com, socialmedia-plattform.de]<br><br><u>Nur durch uBlock/NoScript angezeigt:</u><br>[Erwähnungen von URLs zu Diensten, die nur durch Browsererweiterungen angezeigt werden, aber nicht in der Datenschutzerklärung erwähnt werden, noch durch die Analyse-Tools Privacy Score Beta, Webbkoll und EDPS WEC angezeigt werden]<br><br>[Prüfen und notieren von expliziten Angaben zu Speicherdauer der Cookies]<br><br>Weitere Feststellungen:<br>[Ausgewiesene Angaben zu Provider und die vom Server gespeicherten Informationen über die Besuchenden eintragen<br><br>Z.B.<br>Provider: Beispiel-Webseiten-provider AG<br><br>Datenverarbeitung (Server-Log-Dateien:):<br>- Browsertyp und Browserversion<br>- verwendetes Betriebssystem<br>- Referrer URL<br>- Hostname des zugreifenden Rechners<br>- Uhrzeit der Serveranfrage<br>- IP-Adresse ] |

| | |
|---|---|
| Impressumangaben | [Eine Angabe des Impressums ist Pflicht und muss auf der Landing Page klar ersichtlich sein.]<br>[Notieren der URL zum Impressum sowie Angaben zum Betreiber]<br><br>Z.B.<br>https://beispiel-seite.de/impressum<br><br><br>siehe Angaben gemäß § 5 TM<br>Verein e.V.<br>Beispielsstr. 20<br>00000 Stadt<br>Eintragung im Vereinsregister.<br>Registergericht: Amtsgericht Stadt: Registernummer<br>Finanzamt Stadt, Steuernummer: 000/001000101<br>Vertreten durch:<br><br>Herr/Frau Mustermann<br>Verantwortlich für den Inhalt nach § 55 Abs. 2 RSTV<br>Herr/Frau Mustermann<br>Beispielsstr. 20<br>0000 Stadt<br>Webdesign: Herr/Frau Mustermann<br>Programmierung: Ggf. extern beauftragte Agentur und Ansprechpartner:in<br>Layout-Beratung, Logo & Keyvisuals: Ggf. extern beauftragte Agentur und Ansprechpartner:in |
| Verantwortlichkeiten nach Datenschutzerklärung | [Eintragen der Adresse und Anprechpartner:innen für Rückfragen und Hinweise an Betreibende]<br><br>Verein e.V., Beispielsstr. 20, 00000 Stadt<br>Name, Vorname<br>Telefon, E-Mail |