Bestimmung des Vertrauensniveaus für digitale Verwaltungsleistungen am Beispiel einer kreisfreien Stadt

B a c h e l o r a r b e i t

an der Hochschule Meißen (FH) und Fortbildungszentrum

zum Erwerb des Hochschulgrades

Bachelor of Laws (LL. B.)

Vorgelegt von

Luise Dorenbusch

aus Leipzig

Meißen, 31.03.2022

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Abkürzung	Erläuterung
a. F.	alte Fassung
ABl.	Amtsblatt
ABl. EG	Amtsblatt der Europäischen Gemeinschaft
ABl. EU	Amtsblatt der Europäischen Union
Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
Ahg.	Anhang
Alt.	Alternative
Amtsbl. [SL]	Amtsblatt des Saarlandes
AO	Abgabenordnung
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BMI	Bundesministerium des Innern und für Heimat bzw. Bundesministerium des Innern, für Bau und Heimat
BNatSchG	Bundesnaturschutzgesetz
BR	Bundesregierung
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Drucksache des Deutschen Bundestags
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungen des Bundesverwaltungsgerichts
CIO	Chief Information Officer (IT-Leiter)
DESI	Digital Economy and Society Index (Index für die digitale Wirtschaft und Gesellschaft)
eID	Elektronische Identifizierung
eIDAS-VO	Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates
ELSTER	Elektronische Steuererklärung
EVerwFG	Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften
EGovG	E-Government-Gesetz
FITKO	Föderale IT-Kooperation
FS	Freistaat Sachsen

Abkürzung	Erläuterung
FStrG	Bundesfernstraßengesetz
GBl. [BW]	Gesetzblatt für Baden-Württemberg
GD Connect	Generaldirektion Kommunikationsnetze, Inhalte und Technologien
GG	Grundgesetz für die Bundesrepublik Deutschland
GV. NRW.	Gesetz- und Verordnungsblatt für das Land Nordrhein-Westfalen
GVBl. [BE]	Gesetz- und Verordnungsblatt für Berlin
GVBl. [BY]	Bayerisches Gesetz- und Verordnungsblatt
GVBl. LSA	Gesetz- und Verordnungsblatt für das Land Sachsen-Anhalt
GVBl. [RP]	Gesetz- und Verordnungsblatt für das Land Rheinland-Pfalz
GVBl. [TH]	Gesetz- und Verordnungsblatt für den Freistaat Thüringen
ICS	Industrial Control Systems
IoT	Internet of Things
ITSiV-PV	Verordnung zur Gewährleistung der IT-Sicherheit der im Portalverbund und zur Anbindung an den Portalverbund genutzten IT-Komponenten (IT-Sicherheitsverordnung Portalverbund)
KISA	Zweckverband Kommunale Informationsverarbeitung Sachsen
LeiKa	Leistungskatalog der öffentlichen Verwaltung
LT-Drs. NI	Drucksache des Niedersächsischen Landtags
LT-Drs. NRW	Drucksache des Landtags Nordrhein-Westfalen
LT-Drs. RP	Drucksache des Landtags Rheinland-Pfalz
MdI RLP	Ministerium des Innern und für Sport des Landes Rheinland-Pfalz
MIK BB	Ministerium des Innern und für Kommunales des Landes Brandenburg
NEGZ	Nationales E-Government Kompetenzzentrum e. V.
NKR-Nr. [...]	Stellungnahme des Nationalen Normenkontrollrates Nr. [...]
OZG	Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz)
PStG	Personenstandsgesetz

Abkürzung	Erläuterung
S.	Seite
SAKD	Sächsische Anstalt für kommunale Datenverarbeitung
SächsEGovG	Sächsisches E-Government-Gesetz
SächsEGovGDVO	Sächsische E-Government-Gesetz-Durchführungsverordnung
SGastG	Saarländisches Gaststättengesetz
SächsGVBl.	Sächsisches Gesetz- und Verordnungsblatt
SächsNatSchG	Sächsisches Naturschutzgesetz
SächsStrG	Sächsisches Straßengesetz
SächsVwVfZG	Gesetz zur Regelung des Verwaltungsverfahrens- und des Verwaltungszustellungsrechts für den Freistaat Sachsen
SchriftVG	Gesetz zum Abbau verzichtbarer Anordnungen der Schriftform im Verwaltungsrecht des Bundes
SK	Sächsische Staatskanzlei
SLKT	Sächsischer Landkreistag
SGB	Sozialgesetzbuch
SSG	Sächsischer Städte- und Gemeindetag
TKG	Telekommunikationsgesetz
VwVfG	Verwaltungsverfahrensgesetz

Hinweis zur gendergerechten Sprache

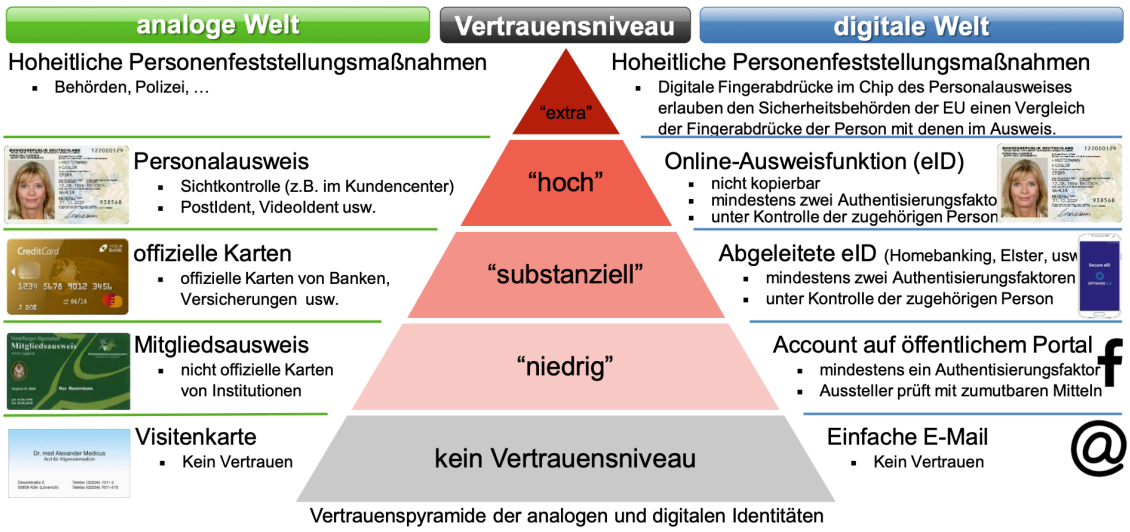
Bei allen Bezeichnungen, die auf Personen bezogen sind, sind grundsätzlich alle Geschlechteridentitäten gemeint. Aus Gründen der besseren Lesbarkeit werden das generische Maskulinum oder – wenn möglich – geschlechterunspezifische Sprachformen verwendet.

1 Einleitung

Der digitale Wandel stellt die öffentliche Verwaltung vor zahlreiche Herausforderungen. Mit Erlass des Onlinezugangsgesetzes (OZG) wurde die öffentliche Verwaltung rechtsverbindlich verpflichtet, sich einigen dieser Herausforderungen in einem relativ engen Zeitrahmen von fünf Jahren zu stellen

Auch kommunale Verwaltungen unterliegen der Verpflichtung aus dem OZG, bis Ende 2022 ihre Verwaltungsleistungen auf Verwaltungsportalen elektronisch anzubieten und Nutzerkonten zur Verfügung zu stellen, mittels derer sich die Verwaltungskunden auf verschiedenen sog. Vertrauensniveaus gegenüber Behörden authentisieren können.

Das Vertrauensniveau gibt an, wie sicher die Behörde sein kann, dass der Verwaltungskunde tatsächlich derjenige ist, als der er ihr gegenüber auftritt, und dass die Interaktion mit ihm tatsächlich so verläuft, wie sie sich augenscheinlich darstellt. Das Vertrauensniveau unterscheidet sich auf der Seite der technischen Umsetzung je nach eingesetztem Mechanismus, beispielsweise der verwendeten Methode der Authentisierung oder Datenübertragung. Umgekehrt unterscheiden sich Verwaltungsleistungen in ihren Anforderungen daran, welches Vertrauensniveau mindestens verlangt, um die Verwaltungsleistung erfolgreich und hinreichend sicher tätigen zu können. Das für eine Verwaltungsleistung erforderliche Vertrauensniveau richtet sich deshalb nach den möglichen Schäden, die entstehen können, falls Prozesse auf dem Weg zu dieser Verwaltungsleistung kompromittiert würden, etwa weil (Identitäts-)Daten nicht mit den Tatsachen korrespondieren oder in die Hände von Unbefugten gelangen. Umso größer und wahrscheinlicher die potenziellen Schäden, desto höher muss das Vertrauensniveau festgelegt werden und desto sicherer müssen die eingesetzten Mechanismen sein. Eine erste grobe Übersicht dazu gibt Abb. 1, die die Bedeutung der einzelnen Vertrauensniveaus anhand ihrer Entsprechungen in der „analogen Welt“ illustriert.



Vertrauenspyramide der analogen und digitalen Identitäten

Abbildung 1: Gegenüberstellung der verschiedenen Umsetzungen von Vertrauensniveau für die Identifizierung in der analogen und digitalen Welt (buergerservice.org e. V. 2021)

Im Unterschied zur „analogen Welt“, die direkte oder materielle Interaktion erfordert, laufen digitale Interaktionen stets elektronisch-medial vermittelt ab. Damit ist eine andere Risikolandschaft verbunden. Mit der Frage, wie man zu der Festlegung eines angemessenen Vertrauensniveaus für eine Verwaltungsleistung im digitalen Raum unter den Bedingungen des OZG gelangt, beschäftigt sich diese Arbeit (siehe Kap. 5 und 6).

Zunächst wird vor dem Hintergrund des Erlasses (siehe Abschn. 2.1 und 2.2) und der Umsetzung des OZG (siehe Abschn. 2.3–2.5) die oben erwähnte Verpflichtung zur Vertrauensniveaubestimmung herausgearbeitet (siehe Abschn. 2.6).

Im Zuge der OZG-Umsetzung sehen sich Behörden mit zahlreichen Problemen und Hindernissen konfrontiert. Zunächst stellt sich die Frage der grundsätzlichen Digitaltauglichkeit des Fachrechts: Verlangt eine Verwaltungsleistung die Schriftform (und damit regelmäßig ein papiergebundenes Format), kann sie nicht ohne Weiteres digitalisiert werden (siehe Kap. 3). Daher geht diese Arbeit den verschieden Möglichkeiten nach, die Schriftform elektronisch zu ersetzen (siehe Abschn. 3.3) oder auf die Anordnung der Schriftform zu verzichten (siehe Abschn. 3.5).

Auch mit Blick auf die Vertrauensniveaubestimmung kommt der Schriftform besondere Bedeutung zu, wie im Zusammenhang mit den Erläuterungen zur praktischen Vertrauensniveaubestimmung in Kap. 5 erläutert wird.

Vor der praktischen Betrachtung werden jedoch auch für das Konzept Vertrauensniveau zunächst die theoretischen Hintergründe vorgestellt (siehe Kap. 4).

Obwohl die Vertrauensniveaufestlegung bei der OZG-Umsetzung eine wesentliche Stellung einnimmt, spiegelt sich diese Bedeutung nicht in einer ausführlichen Behandlung in der Literatur wider. Ganz im Gegenteil: Zur Vertrauensniveaubestimmung gibt es äußerst wenige öffentlich zugängliche Informationen (siehe Abschn. 2.6). Ein Ziel dieser Arbeit ist es, diese Situation zu verbessern.

Dabei ist zu erwähnen, dass sich diese Arbeit in vielen Punkten auf eine inzwischen nicht mehr aktuelle Handreichung des IT-Planungsrates (IT-Planungsrat 2020) beziehen muss, in der Empfehlungen zur Festlegung von Vertrauensniveaus für Verwaltungsleistungen gegeben werden. Diese Handreichung befindet sich bereits seit Monaten in Überarbeitung und ist daher derzeit nicht verfügbar – die alte Fassung wird nicht mehr angeboten, und eine neue ist noch nicht veröffentlicht.[1]

Teilweise an ihre Stelle getreten ist ein Online-Tool, das bei der Vertrauensniveaubewertung unterstützen soll. Darstellung und kritische Betrachtung dieses Tools ist Gegenstand von Abschn. 5.4 und 5.5.

[1] Bereits Anfang des Jahres 2022 hieß es, die neue Version der Handreichung würde „zeitnah finalisiert und veröffentlicht“ (Johannes Volz, Koordination IT-Planungsrat, persönliche Kommunikation, 06.01.2022) – bisher ist dies allerdings nicht geschehen. Das BMI rät von einer Nutzung der letzten veröffentlichten Version der Handreichung ab, „da dies zu einer nicht mehr unterstützen [sic!] Nutzung von Vertrauensniveaus führen könnte“, und kam Bitte um Übersendung der alten Version daher nicht nach (Inga Greiner-Bild, Referat DV 3 – Bundesportal; Portalverbund; Geschäfts- und Koordinierungsstelle 115, BMI, persönliche Kommunikation, 06.01.2022). Auch die neue Version, bzw. alternativ angefragte Auszüge aus dem aktuellen Bearbeitungsstand, wollte man vor der amtlichen Veröffentlichung nicht herausgeben (vgl. Jan Porth, Projektmanagement zur Unterstützung Projektgruppe eID-Strategie des IT-Planungsrates, PricewaterhouseCoopers, persönliche Kommunikation, 23.02.2022). In Ermangelung besser geeigneter Quellen wurde im Rahmen der Erstellung dieser Arbeit daher dennoch auf die letzte veröffentlichte Version der Handreichung des IT-Planungsrates zurückgegriffen.

Anschließend gibt Abschn. 5.6 eine Übersicht zu Empfehlungen zur Vertrauensniveaubestimmung wie sie in der verfügbaren Literatur zum Thema zu finden sind.

Ein Ziel dieser Arbeit war die Erstellung eines Leitfadens für die Ermittlung des Vertrauensniveaus in der kommunalen Verwaltungspraxis. Basierend auf den in den vorhergehenden Kapiteln dargestellten Erkenntnissen gibt Kap. 6 daher Empfehlungen zum Verfahren und zur Durchführung einer Vertrauensniveaufestlegung in der Stadt Leipzig ab. Zusätzlich wurde eine digitale Arbeitshilfe[2] entworfen, die bei der Dokumentation der Bewertung praktisch unterstützt.

Die Verwendung dieser Arbeitshilfe wird an einigen OZG-Leistungen der Stadt Leipzig illustriert (Kap. 7). Ausgewählt wurden dabei aktuell umgesetzte bzw. sich kürzlich in Umsetzung befindliche Leistungen, für die noch keine strukturierte Vertrauensniveaubestimmung stattgefunden hatte (vgl. Cornelia Pflüger, Projektleitung Serviceportal Amt 24, Hauptamt, Stadt Leipzig, persönliche Kommunikation, 01.02.2022). Da sich während der Bearbeitungszeit dieser Arbeit dabei keine Leistung mit Schriftformerfordernis auftat, konnte hierfür in diesem Rahmen einstweilen noch keine Beispielbewertung angefertigt werden.

[2] Die Arbeitshilfe liegt dieser Arbeit in elektronischer Form bei. Der Abdruck in Anh. 8 vermittelt auch in der Druckfassung der Arbeit einen Eindruck von der Arbeitshilfe.

2 Einordnung des Themas in den Kontext des Verwaltungshandelns

2.1 Hintergrund Verwaltungsdigitalisierung

Im Jahr 2015 konstatierte ein Gutachten für den Nationalen Normenkontrollrat vernichtend: „E-Government in Deutschland gibt es nicht." (Fromm/Welzel/Nentwig/Mike Weber 2015: S. 5). Die Hälfte der damals untersuchten Kommunen bot maximal zwei Verwaltungsleistungen online an (Fromm/Welzel/Nentwig/Mike Weber 2015: S. 10). Damit schnitt Deutschland bei der digitalen Verwaltung im EU-Vergleich schlecht ab: Bei die Komponente „Digitale öffentliche Dienste" des Index für die digitale Wirtschaft und Gesellschaft erreichte Deutschland Rang 16 von 27 und lag damit unter dem EU-Durchschnitt (siehe Abb. 2).

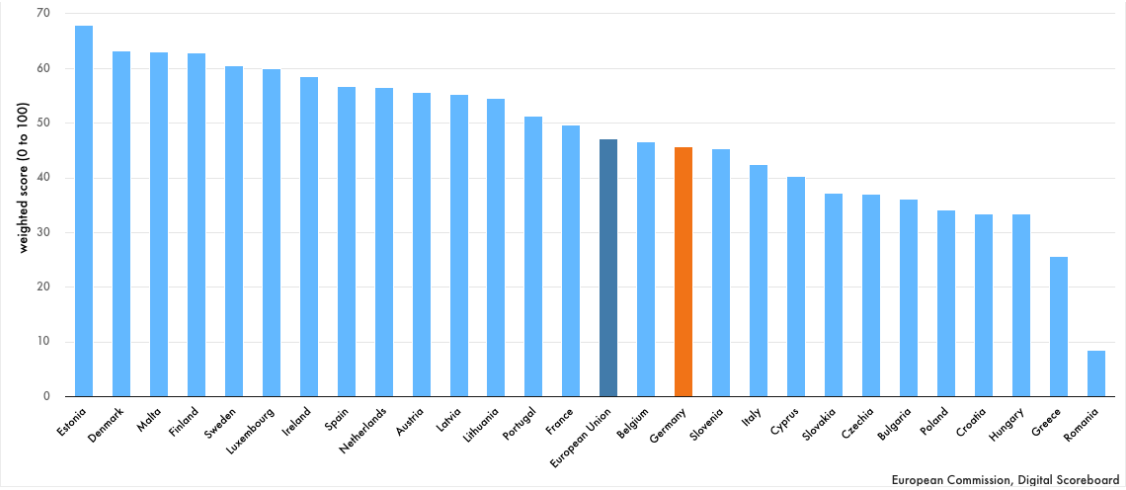


Abbildung 2: Rang Deutschlands im EU-Vergleich der DESI-Komponente Digitale öffentliche Dienste im Jahr 2016 (GD Connect 2020: generiert mit; Hervorhebung hinzugefügt)

Mit überdurchschnittlicher Digitalisierung (im Sinne des allgemeinen Vorhandenseins von digitalisierten Diensten sowohl innerhalb der Verwaltung als auch als Angebot für den Verwaltungskunden), aber zu niedriger Durchdringung (im Sinne der tatsächlichen Nutzung der Online-Angebote) ordnete die E-Government-Benchmark aus dem Jahr 2017 Deutschland der Gruppe der Länder mit „ausbaufähigem" E-Government zu (EU-Kommission 2017: S. 130; siehe Abb. 3).

Knapp zwei Drittel der Bürger waren damals mit den E-Government in ihrer Kommune mindestens etwas zufrieden (vgl. Initiative D21 2016: S. 10 f.). Diese Zahl bezog sich jedoch nur auf diejenigen, die die jeweiligen Angebote überhaupt kannten – was je nach Online-Dienst zwischen 74% und nur 21% der Befragten waren (vgl. Initiative D21 2016: S. 12 f.).

Auch aus finanzieller Sicht war der damals festgestellte Zustand nachteilig: Die unzureichende Digitalisierung der Verwaltung verursachte einen (theoretischen) Verdienstausfall von 6,2 Mrd. € pro Jahr für die deutschen Bürger (vgl. Martini 2018: S. 14). Verwaltungsin-

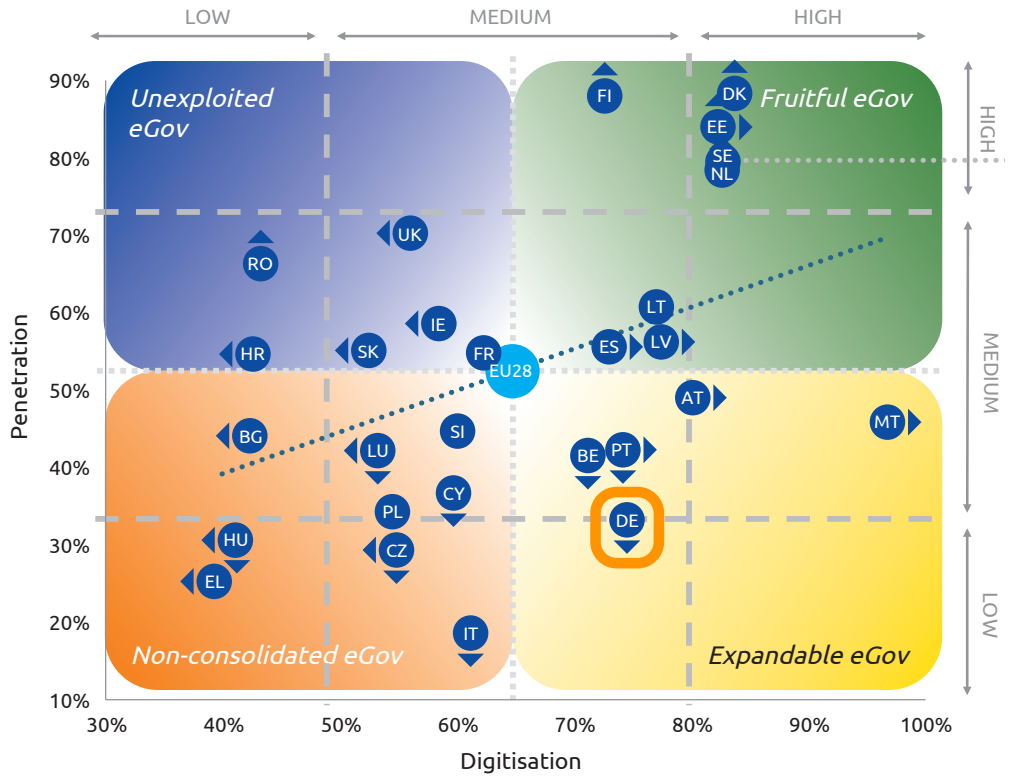


Abbildung 3: Position Deutschlands im EU-Vergleich zu Digitalisierung und Durchdringung beim E-Government (aus EU-Kommission 2017: S. 130; Hervorhebung hinzugefügt)

tern wurden ebenfalls große Vereinfachungs- und Einsparpotenziale nicht realisiert (vgl. Fromm/Welzel/Nentwig/Mike Weber 2015: S. 5; NKR 2017: S. 4).

Die im Vergleich unterdurchschnittliche Performance, die unzureichende Zufriedenstellung der Bürger und die finanziellen Nachteile sind nur einige der Gründe, die zu der Erkenntnis führten, dass der Ausbau des E-Government schnellstmöglichst vorangetrieben werden müsse. In seinem Jahresbericht 2017 urteilte der Nationale Normenkontrollrat bezüglich des Fortschritts der Verwaltungsdigitalisierung: „Es ist 5 vor 12 – oder später!“ (NKR 2017: S. 4).

Die Vielfalt der Verwaltungsleistungen, die auf verschiedenen föderalen Ebenen angeboten werden, stellen die Verwaltung beim Ausbau der Digitalisierung allerdings vor eine äußerst komplexe Aufgabe (vgl. Fromm/Welzel/Nentwig/Mike Weber 2015: S. 7). Um das Problem bewältigen zu können, wurde eine verbesserte Steuerung angemahnt (vgl. BT-Drs. 18/1113: S. 1, 6; Fromm/Welzel/Nentwig/Mike Weber 2015: S. 5)

2.2 Erlass und Ziel des OZG

Um eine verbesserte Steuerung zu ermöglichen, wurde mit der Grundgesetzänderung vom 13. Juli 2017 eine neue Gesetzgebungskompetenz für Gemeinschaftsaufgaben des Bundes geschaffen. Sie ermächtigt den Bund, mit einem Zustimmungsgesetz den „übergreifende[n] informationstechnische[n] Zugang zu den Verwaltungsleistungen von Bund

und Ländern“ zu regeln (Art. 91c Abs. 5 GG), und legt damit den Grundstein für den Erlass des OZG.

Hauptziel des OZG ist es, „den elektronischen Gang zur Behörde unkompliziert und sicher zu gestalten.“ (BT-Drs. 18/11135: S. 5)

§ 1 Abs. 1 OZG verpflichtet daher Bund und Länder, bis Ende 2022, ihre Verwaltungsleistungen auch elektronisch über Verwaltungsportale des Bundes und der Länder anzubieten. Als Teil der Länder sind Kommunen hierbei mit inbegriffen (vgl. BT-Drs. 18/1113: S. 91).

2.3 Aufgaben und Verantwortlichkeiten bei der OZG-Umsetzung

Aufgrund der Vielzahl der Leistungen, die von der öffentlichen Verwaltung in Deutschland angeboten werden, stehen Bund, Länder und Kommunen mit der OZG-Umsetzung vor einer beträchtlichen Herausforderung (vgl. Herrmann/Stöber 2017: S. 1401; siehe auch Abschn. 2.1).

Basierend auf dem Leistungskatalog der öffentlichen Verwaltung (BMI 2021g), der über alle föderalen Ebenen hinweg alle vorhandenen Verwaltungsleistungen auflistet, wurden die online anzubietenden Verwaltungsleistungen identifiziert und in aus Nutzersicht inhaltlich zusammenhängenden Leistungsbündeln, den sog. OZG-Leistungen[3], zusammengestellt (Stocksmeier/Hunnius 2018). Dabei kann eine OZG-Leistung aus bis zu mehreren Hundert einzelnen LeiKa-Leistungen bestehen (BMI 2021c).

Ursprünglich wurden 575 OZG-Leistungen gebildet, inzwischen sind auf der OZG-Informationsplattform 582 OZG-Leistungen aufgelistet (vgl. Stocksmeier/Hunnius 2018; BMI 2022b). Der OZG-Katalog bzw. die -Informationsplattform bilden eine wesentliche Grundlage für die OZG-Umsetzung.

Die OZG-Leistungen sind im OZG-Umsetzungskatalog aus Nutzersicht in 53 Lebenslagen (für Bürger) bzw. Geschäftslagen (für Unternehmen) gegliedert, die den Verwaltungskunden das Auffinden und die Abwicklung von Leistungen erleichtern sollen (vgl. BMI 2021c: S. 2; Herrmann/Stöber 2017: S. 1323)

Die Lebens- und Geschäftslagen sind ihrerseits nach inhaltlicher Zusammengehörigkeit in 14 Themenfelder sortiert (BMI 2021c: S. 6). Jedem Themenfeld ist ein Tandem aus einem Bundesland und dem fachlich zuständigem Bundesressort zugeordnet, das Informationen und Implementierungen der Online-Dienste des Themenfelds erarbeitet (BMI 2021c: S. 1). Diese arbeitsteilige Herangehensweise soll die Erreichung der Ziele der Digitalisierung im engen Zeitrahmen des OZG ermöglichen vgl. BMI 2021a; Berger 2018: S. 444. Andere Bundesländer können nach drei verschiedenen Modellen der Nachnutzung an den Arbeitsergebnissen teilhaben (vgl. BMI 2020: Kap. 10.1; BMI 2021a). Nach dem Modell „Einer für Alle“ können die von einem Bundesland erarbeiteten Lösungen von anderen Bundesländern nach- bzw. mitgenutzt werden. Es können auch länderübergreifend entwickelte Softwarelösungen im dezentralen Betrieb individuell nachgenutzt werden. Des Weiteren besteht die Möglichkeit, Eigenentwicklung zu betreiben, die auf vom

[3] In dieser Arbeit wurde die Bezeichnung „OZG-Leistung“ teilweise auch für einzelne Leistungen eines OZG-Leistungsbündel verwendet, da die Unterscheidung vorliegend nicht relevant ist.

umsetzenden Land zur Verfügung gestellten FIM-Informationen basieren (vgl. BMI 2020: Kap. 10.1).

Die Zuständigkeiten für die Umsetzung der OZG-Leistungen sind über alle föderalen Ebenen verteilt (siehe Abb. 4). Im LeiKa wurde eine genaue Kategorisierung und Typisierung nach Regelungs- und Vollzugskompetenz vorgenommen (siehe Tab. 1). Dabei war man zunächst davon ausgegangen, dass die Typen 2 und 3 regelmäßig nicht zu unterscheiden sind, weshalb zunächst der Typ 2/3 eingeführt wurde (vgl. IT-Planungsrat/Land SA 2014: S. 14). 2021 wurde entschieden, dass dieser Mischtyp nicht mehr verwendet werden soll, da eine Zuordnung zu Typ 2 oder 3 immer möglich sei (vgl. FITKO 2021). Übergangsweise gibt es den Typ 2/3 aber weiterhin – mit den Ergänzungen a oder b, die wie bei den anderen Typen die Vollzugszuständigkeit anzeigen (vgl. FITKO 2021; FITKO 2022a). Für die Umsetzung durch die kommunale Ebene relevant sein können also die Typen 2, 2/3, 3 und 4 – jeweils ggf. ergänzt um ein b – sowie 5.

Abbildung 4: Verteilung der OZG-Leistungen auf die föderalen Ebenen (aus BMI 2020: Abb. 5)

Da sich die Vollzugskompetenz für die meisten OZG-Leistungen bei den Kommunen befindet, spielen sie bei der OZG-Umsetzung eine große Rolle: Rund 80% der Verwaltungsleistungen werden von den knapp 11.000 Kommunen geschultert (Beyer 2021: S. 6).

In ihrer Rolle als Teil der Länder, aber gleichzeitig auch Träger der Selbstverwaltung stehen sie vor einer besonderen Herausforderung (Beyer 2021: S. 6). Zur Bewältigung dieser Aufgabe ist eine enge Kooperation zwischen Bund, Ländern und Kommunen nötig (vgl. Berger 2018: S. 441).

LeiKa-Typ	Verwaltungstyp	Regelungskompetenz	Vollzugskompetenz
1	Bundeseigene Verwaltung	Bundesebene	Bundesebene
2a	Bundesauftrags-verwaltung	Bundesebene	Landesebene
2b		Bundesebene Ausführungsvorschriften durch Landesebene	Kommunale Ebene
3a	Bundesaufsichts-verwaltung	Bundesebene	Landesebene
3b		Bundesebene Ausführungsvorschriften durch Landesebene	Kommunale Ebene
2/3a	Bundesauftrags oder -aufsichtsverwaltung	Bundesebene	Landesebene
2/3b		Bundesebene Ausführungsvorschriften durch Landesebene	Kommunale Ebene
4a	Landeseigene Verwaltung	Landesebene	Landesebene
4b			Kommunale Ebene
5	Kommunalverwaltung	Kommunale Ebene	Kommunale Ebene

Tabelle 1: Details zu den LeiKa-Typen (eigene Darstellung basierend auf: Stocksmeier/ Hunnius 2018: S. 8; FIMLeiKaTypisierung 20210831)

2.4 Aktueller Stand der OZG-Umsetzung

Der Zeitrahmen zur Umsetzung der ehrgeizigen Ziele des OZG – den die Bundesregierung im Gesetzentwurf als „angemessen“ bezeichnete (vgl. BT-Drs. 18/11135: S. 91) – war von Beginn an optimistisch gewählt: In nur fünf Jahren sollten sämtliche digitalisierungsfähigen Verwaltungsleistung flächendeckend zur Verfügung stehen.

Im Jahr 2018 sah Thomas Popp, damals Amtschef der Sächsischen Staatskanzlei und CIO, noch eine gute Chance für die fristgerechte OZG-Umsetzung in Sachsen, auch wenn er gleichzeitig einräumte, dass man dabei mit unvorhergesehenen Hindernisse zu rechnen habe (vgl. Schaeff 2018). Rezentere Einschätzungen führender Akteure zur Zielerreichung sind für Sachsen nicht auffindbar.

Bundesweit ist man mittlerweile weniger zuversichtlich (vgl. z. B. Schubert 2021; Schröder 2021; Wölbert/Bager/Gerber 2022: S. 61). Laut einer rezenten Einschätzung des Bundes-CIO Markus Richter „werden [wir] das quantitative Ziel [von 583 bis Ende 2022 digitalisierten Leistungen] deutlich verfehlen“ (Richter 2022).

In den Bundesländern gehen die Ansichten auseinander: Während man in Rheinland-Pfalz nicht mehr mit einer vollständigen Erreichung der OZG-Ziele rechnet (vgl. ZEIT ONLINE 2021), geht man in Bayern davon aus, dass zumindest die staatlichen Leistungen bis Ende 2022 OZG-konform digitalisiert sein werden (vgl. Gerlach 2022).[4]

[4] Wie weit die OZG-Umsetzung in den Kommunen vorangeschritten sei, ist aufgrund fehlender Daten unklar, und auch die Zielerreichung könne nicht abgeschätzt werden; man wolle aber weiter mit Förderung unterstützen (vgl. Gerlach 2022).

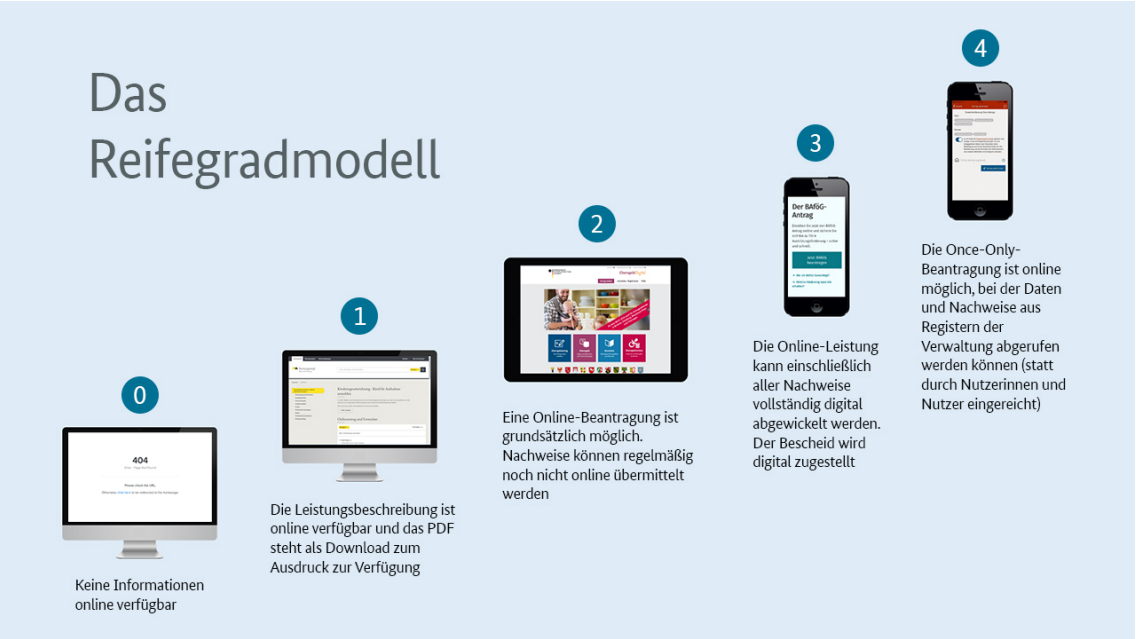


Abbildung 5: Verkürzte Darstellung des OZG-Reifegradmodells (aus BMI 2021f)

Messen lässt sich der tatsächliche Umsetzungsfortschritt am Reifegrad der OZG-Leistungen (siehe Abb. 5). Das Reifegradmodell kategorisiert die Leistungen auf einer Skala von 0 (komplett offline) bis 4 (Online-Transaktion nach dem Once-Only-Prinzip). Vollständig erreicht wären die OZG-Ziele, wenn alle OZG-Leistungen flächendeckend mindestens den Reifegrad 3 (Online-Leistung) erreicht hätten (BMI 2021f).

Gesicherte Informationen zu den Reifegraden aller einzelnen LeiKa-Leistungen lagen der Bundesregierung aufgrund der verteilten Umsetzungszuständigkeiten Anfang 2021 nicht vor (BT-Drs. 19/26311: S. 18). Eine Auswertung ergab, dass von ca. 1.100 erfassten LeiKa-Leistungen nur 35 flächendeckend online verfügbar waren (BT-Drs. 19/26311: S. 18). Im September 2021 resümierte der Normenkontrollrat nach einer Zusammenfassung des Bearbeitungsstand: „[Die OZG-Umsetzung] ist bis Ende 2022 nicht mehr zu schaffen“ (NKR 2021: S. 2).

Eine rezentere Untersuchung des Computermagazins c’t versucht, die für einen Gesamtüberblick fehlenden Informationen zusammenzutragen, und befragte dazu eine Reihe von deutschen Städten nach ihren Online-Angeboten (Wölbert/Bager/Gerber 2022). Bei den untersuchten Verwaltungsleistungen, die wegen ihrer hohen Bedeutung für die Verwaltungskunden ausgewählt wurden, klaffen weiterhin zahlreiche Lücken (siehe Abb. 6) – und das, obwohl auch nicht-OZG-konform digitalisierte Leistungen in dieser Übersicht als umgesetzt bewertet worden.

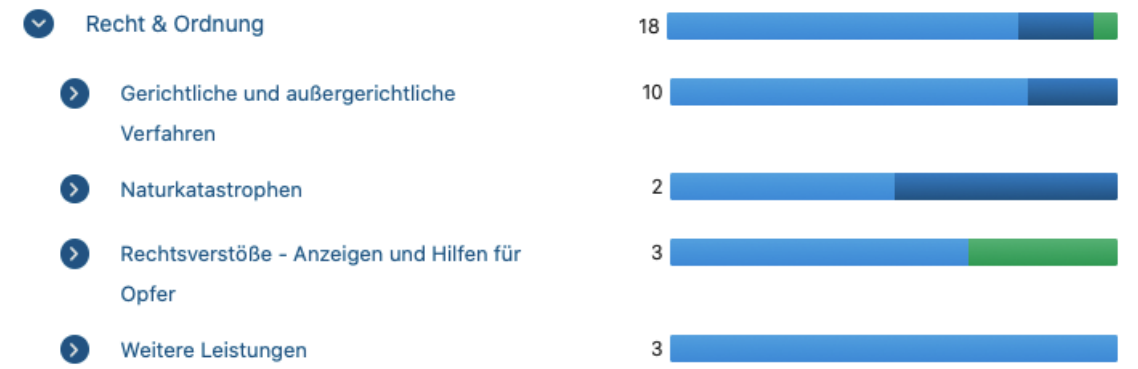
Aktuelle Informationen zum Umsetzungsstand der OZG-Ziele gibt auch das OZG-Dashboard (BMI 2022a). Dort werden, basierend auf den vorliegenden, unvollständigen Datensätzen, für die Bundesebene aktuell nur 77 Leistungen als „online verfügbar“ ausgewiesen.[5]

[5] Bei Veröffentlichung des Informationsportals reichte Reifegrad 2, der nicht OZG-konform ist, für eine Einordnung in die Kategorie der Leistungen aus, die „online verfügbar“ sind. Diese „großzügige Zählweise“, die 2020 schon 315 als „online verfügbar“ präsentierte und bei der es laut BMI „auch darum [ging] zu zeigen, was schon online verfügbar ist“, wurde nach Kritik (vgl. Punz 2020; NKR 2021: S. 2) scheinbar angepasst. In einer

Stadt	Antrag auf Abfall-behälter	Bauantrag	Bewohner-parkaus-weis	Bibliotheks-anmeldung	Führer-schein (Erstantrag)	Anforderung Geburts-urkunde	Anmeldung eines Hundes	Kfz-Neu-zulassung	Schwerbe-hinderten-parkausweis	Unterhalts-vorschuss	Anmeldung Gewerbe	Wohngeld	Vormerkung für Kita-Platz
Berlin	⊕	⊖	⊕	⊖	⊖	⊕	○	⊕	⊖	⊖	⊕	⊕	⊖
Hamburg	⊕	⊖	⊕	⊖	⊕	⊕	⊕	⊕	⊖	⊖	⊕	⊖	⊖
München	⊕	⊖	⊕	⊕	⊖	⊕	⊕	⊕	⊕	⊖	○	⊕	⊕
Köln	⊕	⊖	⊕	⊖	⊖	⊕	⊕	⊕	⊖	⊖	⊕	⊕	⊕
Frankfurt am Main	⊕	⊖	⊕	⊕	⊖	⊕	⊖	⊕	⊕	⊖	⊕	⊖	⊕
Stuttgart	⊕	⊕	⊕	⊖	⊖	⊕	⊕	⊕	⊖	⊖	⊕	⊖	⊕
Düsseldorf	⊕	⊖	⊕	⊖	⊖	⊕	⊕	⊕	⊕	⊖	⊕	⊕	⊕
Leipzig	⊕	⊖	⊕	⊕	⊖	⊕	⊖	⊕	⊖	⊖	○	⊖	⊕
Dortmund	⊕	⊖	⊕	⊖	⊖	⊕	⊕	⊕	⊖	⊖	⊕	⊕	⊕
Essen	⊕	⊖	○	⊖	⊖	⊕	⊕	⊖	○	⊖	⊕	⊕	⊕
Bremen	○	⊖	⊕	⊕	⊖	⊕	⊕	⊕	⊕	⊕	⊕	○	⊕
Dresden	⊕	⊖	○	⊕	⊖	⊕	⊖	⊕	⊖	⊖	○	⊖	⊕
Hannover	⊕[1]	⊖	⊕	⊖	⊖	⊕	⊕	⊕	⊖	⊖	⊕	⊖	⊕
Nürnberg	⊕	⊖	⊕	⊕	⊕	⊕	⊕	⊕	⊖	⊕	○	⊕	⊕
Duisburg	⊕	⊖	⊕	⊕	⊖	⊕	⊕	⊕	⊖	⊖	⊕	⊕	⊕
Bochum	⊕	⊖	⊕	○	⊖	⊕	⊕	⊕	⊖	⊖	⊕	⊕	⊕
Wuppertal	⊕	⊖	⊕	⊖	○	⊕	⊕	⊕	⊕	⊕	○	○	⊕
Bielefeld	⊖	⊖	⊕	⊖	⊖	⊕	⊕	⊕	⊖	⊖	⊕	⊖	⊕
Bonn	⊕	⊖	⊕	⊕	⊖	⊕	⊕	⊕	⊕	⊖	⊕	⊕	⊕
Münster	⊖	⊖	⊕	⊖	⊖	⊕	⊖	⊕	⊖	⊕	⊕	⊕	⊕
Mannheim	⊕	⊕	⊕	⊖	⊕	⊕	⊕	⊕	⊖	⊖	○	⊖	⊕
Karlsruhe	⊕	⊕	○	⊖	⊖	⊕	⊕	⊕	⊕	⊖	⊕	⊖	⊕
Augsburg	⊕	⊖	⊕	⊖	⊖	⊕	⊕	⊕	⊕	⊖	⊕	⊕	⊕
Wiesbaden	○	⊖	⊕	⊕	⊖	⊕	⊖	⊕	⊖	⊖	⊕	⊖	⊕
Mönchengladbach	⊕	⊖	⊕	○	⊖	⊕	○	⊕	⊖	⊖	⊕	⊕	⊕
Kiel	⊕	⊖	⊖	⊖	⊖	⊕	○	⊕	⊖	⊖	⊕	⊕	⊕
Magdeburg	○	⊖	⊖	⊖	⊖	⊕	⊕	⊖	⊕	⊖	○	⊖	⊕
Mainz	○	⊖	⊕	⊖	⊖	⊖[2]	⊖	⊕	⊖	⊖	○	⊖	⊕
Erfurt	⊖	⊖	⊕	⊕	⊖	⊕	⊖	⊕	⊖	⊖	○	⊖	⊕
Potsdam	○	⊖	⊖	○	⊖	⊖	○	⊕	○	○	⊕	⊖	⊖
Saarbrücken	⊕	⊖	⊕	⊕	⊖	⊕	○	⊕	○	⊖	⊕	⊖	⊕
Schwerin	⊕	⊕	⊕	⊖	⊖	⊕	⊕	⊖	⊖	⊖	⊕	⊖	⊖

⊕ = Antrag kann online gestellt werden (z. B. Onlineformular, E-Mail, De-Mail) ○ = der Antrag muss ausgedruckt und von Hand unterschrieben werden, kann jedoch gescannt per E-Mail eingereicht werden
⊖ = der Antrag muss per Post oder persönlich gestellt werden; Stand: 11. Februar 2022 [1] in Zuständigkeit der Region Hannover [2] seit November 2021 nicht mehr möglich

Abbildung 6: Übersicht zur Möglichkeit der digitalen Antragstellung in ausgewählten deutschen Städten (aus Wölbert/Bager/Gerber 2022: S. 62)



Legende: *hellblau:* Reifegrad < 2; *dunkelblau:* Reifegrad 2; *grün:* Reifegrad 3–4

Abbildung 7: Stand der OZG-Umsetzung des Themenfelds Recht & Ordnung unter der Federführung Sachsens (aus BMI 2022b)

Auf Landesebene zeigt die OZG-Informationsplattform die unter Federführung des Freistaates Sachsen umzusetzenden Leistungen des Themenfelds Recht & Ordnung als größtenteils noch nicht OZG-konform digitalisiert (siehe Abb. 7).

Der sog. Marktplatz der OZG-Informationsplattform, der einen Überblick zu laufenden Digitalisierungsaktivitäten und bereits entwickelten Lösungen gibt, bietet derzeit[6] 20 Leistungen mit einem Reifegrad von mindestens 3 zur Nachnutzung an. Im FIT-Store, der EfA-Leistungen zur Nach-/Mitnutzung präsentiert, sind zwei Leistungen verfügbar (FIT-KO 2022b).

Insgesamt zeigt sich aktuell ein Bild, das sich mit der Einschätzung des NKR vom September 2021 deckt: Von der Erreichung der OZG-Ziele ist Deutschland noch weit entfernt, und es erscheint unmöglich, die bisher gesetzten Termine zu halten.

2.5 OZG-Umsetzung bei der Stadt Leipzig

Inzwischen sind Sachsens Behörden durch das OZG verpflichtet, auf die elektronische Zurverfügungstellung ihrer Verwaltungsleistungen hinzuarbeiten (siehe Abschn. 2.2); doch schon 2014 formulierte Sachsens IT-Strategie Ziele wie ständige Verfügbarkeit des elektronischen Zugangs zu Behörden und vollständige elektronische Verfahrensabwicklung (vgl. FS 2014: S. 11 f.). Bei der Umsetzung dieser Ziel bedient man sich damals wie heute des bereits seit dem Jahr 2005 bestehenden Portals Amt24, abrufbar unter www.amt24.sachsen.de (vgl. FS 2014: S. 11; SK 2017a; SK 2019a: S. 129; CDU/Grüne/SPD 2019: S. 59).

Amt24 stellt eine der 14 durch die Sächsische Staatskanzlei zentral bereitgestellten E-Government-Anwendungen (Basiskomponenten) dar (vgl. § 10 Abs. 1 S. 1 SächsEGovG; § 1 Abs. 1 S. 1, § 4 Abs. 1 SächsEGovGDVO). Es handelt sich um ein sachsenweites, verwaltungsebenenübergreifendes Portal: Die Nutzung der staatlich betriebenen Plattform durch die Gemeinden, Landkreise und kreisfreien Städte wurde 2011 in einer

anderen Übersicht werden Reifegrad-2-Leistungen aber weiterhin etwas realitätsverschleiernd als umgesetzte OZG-Leistungen präsentiert („Go-Lives“, im Unterschied zu Leistungen „im Umsetzung“ bzw. „in Planung“).

[6] Stand: 27.03.2022.

Mitnutzungsvereinbarung geregelt, die 2014 und 2018 verlängert wurde und aktuell bis Ende 2022 läuft (vgl. SK 2017b; SAKD 2018; SK 2019a: S. 129).

Amt24 fungierte zunächst als Zuständigkeitsfinder und Informationsportal, um die Nutzer als zentrale Schnittstelle bei der Recherche zu Verwaltungsleistungen zu unterstützen (vgl. SK 2017a; SK 2019a: S. 129). Inzwischen stellt es es als E-Government-Serviceportal, auf dem gebündelt Verwaltungsleistungen angeboten werden und das rund um die Uhr zur Verfügung steht, eine Ausprägung eines Hochleistungsportals i. S. v. Lucke (2006: S. 645 ff.) dar. Sowohl staatliche (gem. § 11a Abs. 1 S. 3 SächsEGovG) als auch kommunale Behörden (gem. § 15a SächsEGovG) sind verpflichtet, ihre OZG-Leistungen auf Amt24 anzubieten.

Basierend auf einer gemeinsamen Entwicklung mit dem dem Land Baden-Württemberg wurde Amt24 im Jahr 2018 um die neuen Komponenten Servicekonto und Verfahrensmanagement erweitert (vgl. SK 2019a: S. 129; SK/Seitenbau 2020: S. 5). Während das Verfahrensmanagement als Bestandteil von Amt24 verstanden wird, wurde das Servicekonto als eigene Basiskomponente in § 1 Abs. 11 S. 1 SächsEGovGDVO verankert (vgl. SK 2019a: S. 129; Weiße/Martin 2019: S. 143).[7]

Das Verfahrensmanagement ist ein System zur Ent- und Abwicklung von elektronischen Verwaltungsverfahren (vgl. SK 2019a: S. 129; Weiße/Martin 2019: S. 143; SK/Seitenbau 2020: S. 10). Zum ihm gehören ein Formulareditor und eine Prozessverarbeitungskomponente (vgl. SK 2019c; SK/Seitenbau 2020: S. 10).

Das Servicekonto dient der Speicherung und Verwaltung der digitalen Identitäten von Verwaltungskunden und wird zur elektronischen Antragstellung benötigt (vgl. SK 2019b; SK 2022). Für natürliche Personen existiert es in der Ausprägung des persönlichen Servicekontos, für juristische Personen in der des Organisationskontos (vgl. SK 2019b; SK 2022). Behörden haben die Möglichkeit, ein Behördenkonto zu beantragen, über das sie mit Verwaltungskunden kommunizieren können (vgl. SK 2022). In das Servicekonto ist auch ein Postfach integriert, mit dem Bürger und Verwaltung sicher elektronisch kommunizieren können (vgl. SK 2019b).

Wie in Abschn. 2.6 erläutert, verpflichtet das OZG Bund und Länder, ihre Verwaltungsportale zu einem Portalverbund zu verknüpfen. Das Servicekonto stellt nach § 1 Abs. 11 S. 2 SächsEGovGDVO das Nutzerkonto nach § 3 Abs. 2 OZG dar, über das sich Nutzer für andere im Portalverbund verfügbare elektronische Verwaltungsleistungen identifizieren können (§11a Abs. 2 S. 1 SächsEGovG).

Derzeit ist auf Amt24 die Anmeldung mittels Benutzername und Passwort sowie mit der eID-Funktion des Personalausweises bzw. des elektronischen Aufenthaltstitels möglich. Damit kann das Vertrauensniveau normal bzw. hoch erreicht werden (vgl. Abschn. 4.3). Eine weitere Anmeldemöglichkeit unter Nutzung des ELSTER-Zertifikats ist noch in Planung (vgl. SK/Seitenbau 2020: S. 5; Kretschmer 2021: S. 150).

Damit kann Amt24 aktuell die Vertrauensniveaus „normal“ und „hoch“ umsetzen, während eine Nutzung auf dem Vertrauensniveau „substanziell“ grundsätzlich (noch) nicht möglich ist (siehe Abschn. 4.3).

[7] SK (2019a: S. 218) und SK (2019c) erwähnen trotzdem auch noch Pläne, das Verfahrensmanagement ebenfalls als separate Basiskomponente zu führen.

Eine Schutzbedarfsfeststellung für Amt24 aus dem Jahr 2016 bewerte den Schutzbedarf für die Schutzziele Vertraulichkeit und Integrität als normal, den für das Schutzziel Verfügbarkeit als hoch (SK 2016). Eine aktuellere Bewertung des Schutzbedarfs, die die 2018 integrierten Komponenten Servicekonto und Verfahrensmanagement mit einschließt wurde bisher nicht öffentlich gemacht. Es existiert aber ein Informationssicherheitskonzept gemäß BSI 200-2 (vgl. SK/Seitenbau 2020: S. 20). Die Sicherheit des Sächsischen Verwaltungsnetzes, dessen Dienste-Plattform auch die Basiskomponenten wie Amt24 und das Servicekonto zur Verfügung stellt, wurde 2020 vom BSI mit einem Zertifikat bestätigt (Sächsische Staatskanzlei 2020: vgl.). Für Amt24 an sich ist die Sächsische Staatskanzlei für das Datenschutzkonzept zuständig, für die Online-Verwaltungsverfahren liegt die Verantwortung bei den jeweils zuständigen Stellen (vgl. SK/Seitenbau 2020: S. 20).

Der aktuelle Stand der OZG-Umsetzung in Leipzig (siehe Abb. 8), macht deutlich, dass noch zahlreiche Leistungen digitalisiert werden müssen – wobei jeweils auch eine Vertrauensniveaubestimmung notwendig ist.

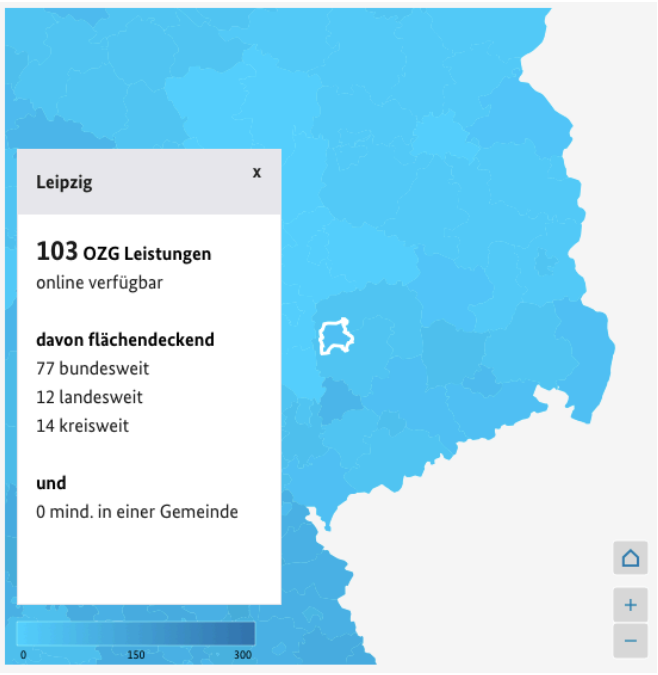


Abbildung 8: Stand der OZG-Umsetzung in der Stadt Leipzig (aus BMI 2022b)[8]

2.6 Bedeutung der Vertrauensniveaubestimmung für die OZG-Umsetzung

Wie bereits in Abschn. 2.2 erläutert, verpflichtet § 1 Abs. 1 OZG Bund und Länder (einschließlich der Kommunen), bis spätestens Ende 2022 ihre Verwaltungsleistungen auch elektronisch über Verwaltungsportale anzubieten. Nach § 1 Abs. 2 OZG sind diese Verwaltungsportale zu einem Portalverbund zu verknüpfen, über den gem. § 3 Abs. 2 OZG Nutzerkonten bereitgestellt werden, „über die sich Nutzer für die im Portalverbund verfügbaren elektronischen Verwaltungsleistungen von Bund und Ländern einheitlich identi-

[8] Der Umstand, dass es sich bei der Stadt Leipzig um eine kreisfreie Stadt handelt bedingt die eigenartig anmutende Information in der Grafik, dass in Leipzig keine OZG-Leistungen auf Gemeindeebene verfügbar sind.

fizieren und authentifizieren können“. Die Identifizierung des Nutzers eines solchen Nutzerkontos kann gem. § 8 Abs. 1 OZG „auf unterschiedlichen Vertrauensniveaus erfolgen und muss die Verwendung des für das jeweilige Verwaltungsverfahren erforderlichen Vertrauensniveaus ermöglichen“.

Für jede Verwaltungsleistung muss also im Zuge der OZG-Umsetzung das passende Vertrauensniveau ermittelt werden, was dann entsprechend im Nutzerkonto umgesetzt wird. Dabei gilt es zu bedenken, dass es innerhalb der OZG-Leistungsbündel zu unterschiedlichen Bewertungen für einzelne Prozesse kommen kann; es ist also eigentlich für jede LeiKa-Leistung das Vertrauensniveau zu bestimmen.

Der Bestimmung des Vertrauensniveaus wird bisher gemeinhin keine große Bedeutung zugemessen. So hat das Thema in der Fachliteratur (noch) keine Beachtung gefunden.

Auch Anleitungen zur praktischen Umsetzung des OZG gehen auf die Vertrauensniveaubestimmung nicht weiter ein (vgl. z. B. SAKD/KISA/SSG/SLKT 2019). Wird die Notwendigkeit der Vertrauensniveaubestimmung überhaupt erwähnt, so beschränkt man sich auf diese Festlegung, ggf. unterlegt durch einen Verweis auf die Empfehlungen des IT-Planungsrat und/oder das Praxistool Vertrauensniveau (vgl. z. B. MIK BB 2020: S. 11 f.; BMI 2020; BMI 2021i: S. 15[9]). Weiterführende Erläuterung, Beispiele für bereits bewertete Verwaltungsleistungen oder Begründungen für Vertrauensniveauzuordnungen finden sich keine.

Die OZG-Informationsplattform, die nach eigener Einschätzung „die wichtigsten Informationen zum Stand und Fortschritt der Umsetzung des OZG bereit[hält]“ (BMI 2020), bietet neben einer Tabelle mit Steckbrief-Informationen – die keine Eintragung eines Vertrauensniveaus vorsieht – auch die Möglichkeit an, ausführlichere Steckbriefdokumente hochzuladen. Untersucht man alle OZG-Leistungen mit mindestens Reifegrad 3, für die solche Steckbriefdokumente vorhanden sind, kann man feststellen, dass sich auch dort bei der übergroßen Mehrheit keine Informationen zum festgelegten Vertrauensniveau finden. Offensichtlich stuft man diese Information als nicht relevant ein.

Auch im FIM-Portal lassen sich nur sehr vereinzelt Informationen zum Vertrauensniveau finden (siehe auch Abschn. 5.6.2).

Die im Rahmen der Erstellung dieser Arbeit befragten OZG-Fachexperten fühlten sich zum Thema Vertrauensniveau laut eigener Aussage alle nicht auskunftsfähig oder reagierten nicht auf Anfragen.

Die SAKD vertritt aufgrund der geringen gesetzlichen Verankerung des Vertrauensniveaus gar die Meinung, dass die Vertrauensniveaubestimmung „eine untergeordnete Rolle“ spiele (Heiko Richter-Schuppan, Referent Kommunale Digitalisierung, SAKD, persönliche Kommunikation, 16.03.2022).

Trotzdem ist zu betonen, dass dieser Vorgang für eine OZG-konforme Umsetzung von digitalen Verwaltungsleistungen unabdingbar ist.

[9] Der EfA-Wegweiser des BMI, der sich selbst als „ein handlungsorientierter Leitfaden für die Umsetzung von Digitalisierungsprojekten und die Nachnutzung im Modell ‚Einer für Alle‘ (EfA)“ versteht, empfiehlt zwar die Nutzung des Praxistools Vertrauensniveau, aber nur zur Bestimmung des „Niveau[s] des Schutzbedarfs“ durch „die für das Thema Datenschutz verantwortlichen Projektteilnehmer:innen“; die Notwendigkeit der Festlegung des Vertrauensniveaus und Zuständigkeit der Fachverantwortlichen finden keinerlei Erwähnung (BMI 2021i)[S. 15]. Dieser Umstand illustriert erneut, wie wenige Bedeutung dem Thema Vertrauensniveaubestimmung zugeschrieben wird.

3 Schriftformersatz und -verzicht im Verwaltungsrecht

Max Weber (1922: S. 220) hob das Prinzip der Aktenmäßigkeit der Verwaltung als Charakteristikum legaler und rationaler Herrschaft hervor: Nur schriftlich Fixiertes kann zu einem späteren Zeitpunkt überprüft werden. In Ermangelung anderer praxistauglicher Möglichkeiten war die Verwaltung daher jahrhundertelang papiergebunden – schriftliche Unterlagen mit Unterschrift stellen den Normalfall dar (vgl. BT-Drs. 18/9177: S. 6). Viele Rechtsnormen fordern die Schriftform sogar explizit (siehe Abschn. 3.1).

Charakteristisch für die Schriftform ist eine „mittels lesbare[r] Schriftzeichen auf einem Substrat – regelmäßig ist dies Papier – verkörpert[e] und auf Dauer fixiert[e]“ Erklärung (BT-Drs. 18/9177: S. 6). Elektronisch kann eine solche verkörperte Erklärung nicht erstellt werden. Vor dem Hintergrund der verpflichtend umzusetzenden Anforderungen des OZG (siehe Abschn.2.2) steht die Verwaltung damit vor einem Problem. Die verschiedenen Möglichkeiten, durch den Einsatz von Schriftformsurrogaten mit diesem Problem umzugehen, erläutert Abschn. 3.3.

Noch besser als Schriftformersatz ist allerdings Schriftformverzicht – zumindest im Hinblick auf die Einfachheit der Digitalisierung einer Verwaltungsleistung (vgl. BR 2014: S. 15). In Abschn. 3.5 werden frühere und aktuelle Vorhaben des Schriftformabbaus im Verwaltungsrecht und deren Bedeutung für die OZG-Umsetzung vorgestellt.

3.1 Schriftformerfordernis

Für das bürgerliche Recht ist die Schriftform in § 126 Abs. 1 BGB definiert: „Ist durch Gesetz schriftliche Form vorgeschrieben, so muss die Urkunde von dem Aussteller eigenhändig durch Namensunterschrift [...] unterzeichnet werden.“ Es wird grundsätzlich eine Unterschrift auf Papier gefordert.

Nicht so jedoch im Verwaltungsrecht: „Die Vorschrift des § 126 Abs. 1 BGB, die die eigenhändige Unterschrift des Ausstellers fordert, gilt im öffentlichen Recht nicht“ (BVerwG, Urteil vom 5. Juni 1974 – VIII C 1.74 –, BVerwGE 45, 189–197, Rn. 21). Mit dem Fehlen einer Definition der Schriftform wird den Besonderheiten des Verwaltungsverfahrens Rechnung getragen (BMI 2016: S. 4).

Grundsätzlich ist das Verwaltungsverfahren gem. § 10 VwVfG[10] nämlich von Nichtförmlichkeit geprägt.[11] Ist nichts anderes angeordnet, besteht also kein Formzwang für Verfahrenshandlungen, und z. B. mündliche Erklärungen sind ebenso wirksam wie schriftliche (vgl. Mann/Sennekamp/Uechtritz 2019: § 10 Rn. 12).[12]

Explizite Schriftformerfordernisse sind im Bereich des Verwaltungsrechts mit über 3000 Vorkommen allein im Bundesrecht allerdings sehr häufig (vgl. BT-Drs. 18/10183: S. 1). Die genauen Anforderungen an die Schriftform sind dabei durch Auslegung für jede Rechts-

[10] Das VwVfG gilt aufgrund § 1 SächsVwVfZG u. a. auch für die öffentlich-rechtliche Verwaltungstätigkeit der sächsischen Kommunen.

[11] Eine Ausnahme vom Grundsatz der Nichtförmlichkeit bilden z. B. öffentlich-rechtliche Verträge (gem. § 57 VwVfG).

[12] Die Verpflichtung zur „einfach[en], zweckmäßig[en] und zügig[en]“ Durchführung des Verwaltungsverfahrens aus § 10 S. 2 VwVfG weist aber laut Maurer/Waldhoff (2017: S. 514 f.) auf das elektronische Verfahren hin. Trotz grundsätzlicher Formfreiheit sollte möglichst die Form gewählt werden, mit der sich das Verfahren effizient und effektiv abwickeln lässt – aktuell ist diese Form die elektronische.

norm einzeln zu ermitteln (vgl. BT-Drs. 18/9177: S. 6; siehe auch Abschn. 3.2). Auch wenn eine eigenhändige Unterschrift durch ein verwaltungsrechtliches Schriftformerfordernis nicht zwingend gefordert ist, gilt es jedenfalls dann als gewahrt, wenn diese vorhanden ist, und damit den Anforderungen des § 126 BGB entsprochen wird (vgl. BVerwG, Urteil vom 05. Juni 1974 – VIII C 1.74 –, BVerwGE 45, 189–197, Rn. 21; BT-Drs. 18/9177: S. 6).

3.2 Funktionen der Schriftform

Der Schriftform werden zahlreiche Funktionen zugeschrieben. Im Folgenden werden die am häufigsten genannten kurz dargestellt.

Die eigenhändige Unterschrift schließt eine Erklärung in Schriftform räumlich ab und zieht damit eine Grenze zu rechtlich unverbindlichen Inhalten; dies bezeichnet man als Abschlussfunktion (vgl. BT-Drs. 14/4987: S. 16). Eine schriftliche Erklärung ist in einer Urkunde fortdauernd verkörpert, was eine dauerhafte Überprüfung ermöglicht (Perpetuierungsfunktion; vgl. BT-Drs. 14/4987: S. 16; BT-Drs. 17/10720: S. 4). Der Akt des Unterzeichnens einer Erklärung in Schriftform macht dem Unterzeichnenden die rechtliche Verbindlichkeit und – zumal da mit Namen unterzeichnet wird – persönliche Zurechenbarkeit bewusst (vgl. BT-Drs. 14/4987: S. 16; BT-Drs. 17/10720: S. 4). Diese sog. Warnfunktion der Schriftform bietet Schutz vor übereilten Rechtsgeschäften (vgl. BT-Drs. 14/4987: S. 16; BT-Drs. 17/10720: S. 4).

Bei einer schriftlichen Erklärung besteht ein räumlicher Zusammenhang zwischen Unterschrift und Urkunde. Mit der sog. Echtheitsfunktion soll eine inhaltliche Zuordnung der Erklärung zum Unterzeichner gewährleistet und eine nachträgliche Verfälschung ausgeschlossen werden (vgl. BT-Drs. 14/4987: S. 16; BT-Drs. 17/10720: S. 4).

Durch die eigenhändige Namensunterschrift entsteht eine unzweideutige, verifizierbare Verbindung zwischen der Erklärung in Schriftform und der Person des Unterzeichners (sog. Identitätsfunktion; vgl. BT-Drs. 14/4987: S. 16: BT-Drs. 17/10720: S. 4). Im engen Zusammenhang damit steht die Verifikationsfunktion, die die Möglichkeit der Überprüfung der Echtheit der Unterschrift, z. B. durch Unterschriftenvergleich, bezeichnet (vgl. BT-Drs. 14/4987: S. 16). Damit verknüpft ist die Beweisfunktion: Durch Unterzeichnung einer Erklärung, wird ein verkörpertes Beweismittel geschaffen, mit dem mittels der Verifikationsfunktion bewiesen werden wer sie abgegeben hat (vgl. BT-Drs. 14/4987: S. 16; BT-Drs. 17/10720: S. 4).

3.3 Schriftformersatz

Dass Formerfordernisse, die die – wie erläutert papierzentrierte – Schriftform oder gar persönliches Erscheinen anordnen, den Ausbau der digitalen Verwaltung behindern, liegt auf der Hand (vgl. BMI 2016: S. 1). Vor dem Hintergrund der damaligen Weiterentwicklungen im Bereich der elektronischen Kommunikation wurde 2003 mit der Neufassung des VwVfG die rechtliche Grundlage für die elektronische Kommunikation als Alternative zur Schriftform geschaffen (vgl. BT-Drs. 14/9000: S. 26).

Während aufgrund der Formfreiheit der Verwaltung die Möglichkeit der elektronischen Kommunikation grundsätzlich bereits bestand, war sie in ihrer Anwendung durch zahlrei-

che Schriftformerfordernisse eingeschränkt (siehe Abschn. 3.1). Abhilfe sollte § 3a VwVfG a. F. schaffen: Die Schriftform konnte damit – soweit durch Rechtsvorschrift nichts anderes bestimmt war – durch die elektronische Form ersetzt werden. Als elektronische Form war dabei ein elektronisches Dokument mit einer qualifizierten elektronischen Signatur i. S. d. (damals noch gültigen) Signaturgesetzes zu verstehen (Stelkens/Bonk/Sachs 2018: § 3a Rn. 20 f.).[13]

Aufgrund der hohen finanziellen und technischen Hürden bei Beschaffung und Benutzung einer qualifizierten elektronischen Signatur und der daraus resultierenden sehr begrenzten Verbreitung entfaltete diese Regelung in der Praxis aber kaum Bedeutung (vgl. Roßnagel 2019: S. 623; Mann/Sennekamp/Uechtritz 2019: § 3a Rn. 4, 27).

Durch das Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften wurden daher im Jahr 2013 weitere Möglichkeiten des Schriftformersatzes geschaffen: Gem. § 3a Abs. 2 VwVfG können nun – kurz zusammengefasst – zusätzlich auch Erklärungen in einem elektronischen Formular der Behörde, bei Zugriff über das Internet mit Authentisierung per eID (Nr. 1), De-Mail-Nachrichten (Nr. 2 und 3) oder sonstige sichere, vom IT-Planungsrat empfohlene Verfahren (Nr. 4) zum Einsatz kommen.[14]

Für OZG-konform umzusetzenden Leistung relevant ist dabei Nr. 1: Bei über Verwaltungsportale angebotenen Verwaltungsleistungen kann die Schriftform über das Ausfüllen eines Formulars und einem zusammenhängenden Identitätsnachweis über eID realisiert werden (siehe Abschn. 5.2).

3.4 „Gefühlte“ Schriftform

Behördliche Formulare enthalten meist Unterschriftsfelder, auch wenn sich im Fachrecht keine explizite Anordnung der Schriftform findet (vgl. BT-Drs. 17/1473: S. 63; Denkhaus/Richter/Bostelmann 2019: § 13 EGovG Rn. 1 ff.). Häufig wird dann im Umkehrschluss aus dem Vorhandensein eines Unterschriftsfeld eine entsprechende gesetzliche Vorschrift abgeleitet (vgl. BT-Drs. 17/1473: S. 44 f.).

Da Schriftformerfordernisse die Verwaltungsdigitalisierung erschweren, wirkt das EGovG mit § 13 dieser unangebrachten Rechtspraxis entgegen, die zwar in Rechtsprechung und Fachliteratur keine Begründung findet, aber trotzdem weit verbreitet ist (vgl. Denkhaus/Richter/Bostelmann 2019: § 13 EGovG Rn. 3). Darin wurde festgelegt, dass alleine aus der Vorschrift zur Verwendung eines bestimmten Formulars mit Unterschriftsfeld kein Schriftformerfordernis entsteht und dass bei einem für die elektronische Versendung bestimmten Formular das Unterschriftsfeld entfällt.

Nach § 1 Abs. 2 EGovG gilt § 13 EGovG für Kommunen zwar nur bei der Ausführung von Bundesrecht, § 2a SächsEGovG enthält jedoch eine wortgleiche Regelung, die aufgrund von § 1 Abs. 1 SächsEGov auch für die Verwaltungstätigkeit der Kommunen verbindlich ist.

[13] Inzwischen hat die eIDAS-VO die Signaturrichtlinie, deren Umsetzung das Signaturgesetz diente, abgelöst. Trotzdem wird teilweise auch in aktueller Literatur noch darauf Bezug genommen, z. B. in Stelkens/Bonk/Sachs (2018: § 3a Rn. 20 ff.).

[14] § 87a Abs. 3 AO und § 36a Abs. 2 SGB I enthalten analoge Regelungen für das Abgaben- und Sozialrecht.

Bei der Bestimmung des Vertrauensniveaus einer Verwaltungsleistung gilt es daher, das tatsächliche Vorhandensein eines Schriftformerfordernisses sorgfältig zu prüfen.

3.5 Schriftformverzicht

Statt mittels mehr oder minder komplizierter Verfahren zu versuchen, die Schriftform elektronisch zu ersetzen, bietet es sich an, zunächst zu prüfen, ob stattdessen auch einfach ein Verzicht auf die Anordnung der Schriftform bzw. die Ergänzung der Zulässigkeit der elektronischen Form in Frage kommt. Der einfachste Weg, mit Schriftformerfordernissen umzugehen, ist – wo immer möglich – deren Abbau (vgl. BR 2014: S. 15). Um den weiteren Ausbau der digitalen Verwaltung voranzutreiben, gab es daher in den letzten zehn Jahren auf allen föderalen Ebenen Initiativen zur Rechtsbereinigung.

3.5.1 Bundesebene

Mit dem Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften wurde 2013 die Verpflichtung rechtlich verankert, das Verwaltungsrecht des Bundes bis 2016 auf verzichtbare Schriftformerfordernisse und Anordnungen des persönlichen Erscheinens zu überprüfen (Art. 30 Abs. 2 EVerwFG).

Ziel der Überprüfung war es, Schriftformerfordernisse „im Idealfall ersatzlos [zu streichen]“, was neben der schriftlichen auch eine mündliche, fermündliche oder elektronische Verfahrensabwicklung erlaubt, oder durch zusätzliche Zulassung möglichst einfacher elektronischer Verfahren zu ersetzen (BT-Drs. 18/9177: S. 4). Hierbei ist zu betonen, dass mit „möglichst einfachen elektronischen Verfahren“ nicht die elektronische Form aus § 3a Abs. 2 VwVfG, sondern etwa eine E-Mail gemeint ist (vgl. BT-Drs. 18/10183: S. 64).[15]

Im Rahmen eines entsprechenden Normenscreenings wurden 2872 verwaltungsrechtliche Rechtsvorschriften des Bundes überprüft. Die Ergebnisse wurden 2016 in einem Bericht der Bundesregierung veröffentlicht: 3 % der Schriftformerfordernisse sollten ersatzlos gestrichen werden, 17 % waren zugunsten einer elektronischen Verfahrensabwicklung verzichtbar (vgl. BT-Drs. 18/9177: S. 4).

In der Folge wurde 2017 das Gesetz zum Abbau verzichtbarer Anordnungen der Schriftform im Verwaltungsrecht des Bundes verabschiedet. 464 Rechtsvorschriften, verteilt auf 68 Gesetze und 114 Rechtsverordnungen, wurden damit „zum weiteren Ausbau einfacher elektronischer Verwaltungsdienste und zum Abbau unnötiger Bürokratie“ angepasst (vgl. BT-Drs. 18/10183: S. 2).

3.5.2 Länderebene

Im Jahr 2019 fanden sich laut Denkhaus/Richter/Bostelmann (2019: § 17 EGovG Rn. 41) im Landesrecht noch keine entsprechenden Regelungen. Aber bereits 2015 – also noch vor Erlass des SchriftVG – hatte der Freistaat Bayern eine ähnliche Regelung in sein E-Government-Gesetz eingefügt (§ 9a BayEGovG a. F.). Auch das Land Berlin hatte 2018

[15] Zur Gewährleistung größtmöglicher Verfahrensflexibilität sind auch aktuell noch unbekannte elektronische Verfahren erfasst (vgl. BT-Drs. 18/10183: S. 64).

ein vergleichbares Gesetz erlassen[16], nachdem in einem umfassenden Normenscreening ca. 1.350 Formanforderungen geprüft wurden waren (AG „Attraktivität des E-Government" 2015: S. 14). Denkhaus/Richter/Bostelmann (2019: § 17 EGovG Rn. 42 f.) bewerten diese Initiativen jedoch als weniger umfänglich als die bundesrechtliche Rechtsbereinigung und daher als nicht vergleichbar.

Inzwischen sind auch in Sachsen-Anhalt (2020)[17], in Baden-Württemberg (2020)[18], im Saarland (2021)[19] und in Nordrhein-Westfalen (2022)[20] ähnliche Gesetze erlassen worden.

In Rheinland-Pfalz hat aufgrund einer entsprechenden in § 30 EGovGRP normierten Pflicht zumindest ein Normenscreening zum Abbau von Formerfordernissen bereits stattgefunden (vgl. MdI RLP 2018: S. 43). Auf den resultierenden Bericht sollen nun Gesetzesänderungen folgen (vgl. LT-Drs. RP 18/1908).

In Thüringen wurde ein entsprechender Antrag der FDP-Fraktion am 23. September 2021 vom Landtag abgelehnt; „ein Artikelgesetz mit einer abstrakten Prüfung von Normen zum Verzicht auf das Schriftformerfordernis [ist] nach Einschätzung der Landesregierung nicht zielführend". Eine Änderung von Gesetzen mit unnötiger Schriftformerfordernis im Zuge der geplanten Novellierung des ThürEGovG wird aber in Betracht gezogen (vgl. Plenarprotokoll [TH] 7/58: S. 31).

In Niedersachsen hielt man 2015 ein Normenscreening nach Vorbild des Bundes für nicht notwendig (vgl. LT-Drs. NI 17/3195: S. 82). Dafür, dass sich inzwischen an dieser Auffassung etwas geändert hätte, liegen keine Anhaltspunkte vor.

In den restliche Bundesländern scheint es bisher ebenfalls keine entsprechenden Initiativen zu geben. Auch in Sachsen gibt bisher kein mit dem SchriftVG vergleichbares Gesetz, doch der aktuelle Koalitionsvertrag (CDU/Grüne/SPD 2019: S. 59 f.) kündigt zumindest entsprechende Bestrebungen an: „Rechtliche Hürden, wie Schriftformerfordernisse, bauen wir weiter ab."

3.5.3 Kommunale Ebene

Durch die Ausführung von Bundes- oder Landesrecht ist die kommunale Ebene direkt von den auf diesen Ebenen durchgeführten Rechtsbereinigungen betroffen. Doch auch auf der kommunalen Ebene selbst erfolgt teilweise ein Normenscreening.[21]

Der Kreis Unna, der anscheinend bereits in der Vergangenheit eine Überprüfung seiner Rechtsvorschriften vorgenommen hatte, hat unter dem Titel „Normen-Screening plus" eine „erneute, ehrgeizige Überprüfung der Schriftformerfordernisse" in seine Digitalisierungsstrategie aufgenommen (vgl. Kreis Unna 2019: S. 9). Zum Stand der Umsetzung wurden bisher keine Informationen veröffentlicht.

[16] Gesetz zur Anpassung der Formanforderungen im Berliner Landesrecht.

[17] Gesetz zum Abbau verzichtbarer Anordnungen der Schriftform im Verwaltungsrecht des Landes Sachsen-Anhalt.

[18] Gesetz zum Abbau verzichtbarer Formerfordernisse.

[19] Gesetz zur Förderung der Digitalisierung durch Abbau von Formerfordernissen im Landesrecht des Saarlandes.

[20] Gesetz zur Stärkung der medienbruchfreien Digitalisierung; Normenscreening gefordert durch § 25 EGovG NRW.

[21] Da eine Recherche hierzu kaum Ergebnisse liefert, kann man davon ausgehen, dass ein umfassendes, zielgerichtetes Normenscreening noch eher die Ausnahme darstellt.

In der Stadt Jena wurde beschlossen, bis zum 4. Quartal 2021 eine umfängliche Überprüfung aller Rechtsvorschriften (Verordnungen, Richtlinien, Satzungen, Vollzugshinweisen usw.) durchzuführen, mit dem Ziel „das Schriftformerfordernis auf Papier auf das unabweisbar notwendige Minimum [zu] reduzier[en]“ (Abl. Jena 19/21: S. 148). Da seitdem keine Beschlussvorlagen mit entsprechenden Ergebnissen in den Stadtrat eingebracht wurden (Stadt Jena 2022), kann man davon ausgehen, dass sich diese Maßnahme noch in Umsetzung befindet.

Auch in der Stadt Leipzig fanden Rechtsbereinigungen statt, wenn auch punktueller: Im Jahr 2020 sind die Marktsatzung[22] und die Sondernutzungssatzung[23] sowie 2022 die Baumschutzsatzung[24] angepasst worden, sodass neben der schriftlichen auch eine elektronische Antragstellung möglich ist (vgl. Cornelia Pflüger, Projektleitung Serviceportal Amt 24, Hauptamt, Stadt Leipzig, persönliche Kommunikation, 04.02.2022).

3.5.4 Bedeutung für die OZG-Umsetzung

Inwieweit diese Rechtsbereinigungen jedoch direkte Auswirkungen auf die OZG-Umsetzung haben, ist nicht klar.

Auf Bundeseben wurden nach Einschätzung des NKR mit dem SchriftVG hauptsächlich solche Rechtsvorschriften angepasst, die mit jährlichen Fallzahlen unter 1.000 nur geringe Relevanz für Bürger und Unternehmen haben (vgl. NKR-Nr. 3703: S. 3). Größeres Potenzial für die Verwaltungsvereinfachung wurde in denjenigen Verfahren gesehen, die im Rahmen des Normenscreenings als nicht anpassbar eingestuft worden waren (vgl. NKR-Nr. 3703: S. 3). Für die OZG-Umsetzung bedeutet das, dass wahrscheinlich wenige Leistungen, die sich bereits in Umsetzung oder kurz davor befinden, von einem Schriftformabbau profitiert haben.

Auch insgesamt bewertet der NKR den Erfolg des Normenscreenings als „mäßig“ (NKR 2019b: S. 12). Er plädiert seit 2018 für eine pauschale Abschaffung aller papiergebundenen Schriftformerfordernisse und Nachweispflichten, mit Ausnahmen für begründete Einzelfälle, und andere Stimmen schließen sich dieser Forderung an (vgl. NKR 2018: S. 2; NKR 2019a: S. 9; Beyer 2021: S. 7). Die vorgeschlagene Beweislastumkehr („Die Schriftform ist abgeschafft, es sei denn ...“), die ein erneutes Normenscreening hätte ersetzen können, wurde von der Bundesregierung abgelehnt (NKR 2019b: S. 12; vgl. NKR 2020: S. 15). Ein solches Vorgehen hätte die OZG-Umsetzung möglicherweise beschleunigen können. Je mehr Schriftformerfordernisse wegfallen, desto häufiger kann auf aufwändige Prüfungen der Verfahren auf Notwendigkeit der einzelnen Schriftformfunktionen verzichtet werden (siehe Abschn. 5.2). Auch die Möglichkeit, mehr Leistungen ohne Schriftformerfordernis mit einem niedrigeren Vertrauensniveau umzusetzen zu können und diese damit – vor dem Hintergrund der weiterhin niedrigen eID-Nutzungszahlen[25] – mehr Ver-

[22] Beschlussvorlage VII-DS-01122; § 8 Abs. 1, 12 Abs. 2 Satzung der Stadt Leipzig über die Durchführung, Zulassung und Gebührenerhebung auf Wochen- und Spezialmärkten.

[23] Beschlussvorlage VII-DS-01074-NF-01; § 3 Abs. 1, 7 Abs. 5 Satzung der Stadt Leipzig über Erlaubnisse und Gebühren für Sondernutzungen an öffentlichen Straßen, Wegen und Plätzen; § 3 Abs. 4 ermöglicht die Erteilung eines elektronischen Bescheides.

[24] Beschlussvorlage VII-DS-06203; § 7 Abs. 1 Satzung zum Schutz und zur Pflege des Baumbestandes der Stadt Leipzig.

[25] Siehe Fußnote 40.

waltungskunden leichter zugänglich zu machen, wäre möglicherweise förderlich gewesen (siehe Abschn. 5.6.3).

Auch auf Landesebene sind die Auswirkungen auf die OZG-Umsetzung kleiner als es wegen der großen Anzahl der geänderten Rechtsvorschriften vielleicht zunächst anmutet.

Ein Beispiel aus dem Saarland: Nach einem aufwändigen Normenscreening von ca. 2.000 Einzelvorschriften, in das – anders als in vielen anderen Bundesländern – auch alle Rechtsverordnungen des Landesrechts einbezogen wurden, sind über 1.000 Schriftformerfordernisse bzw. Erfordernisse des persönlichen Erscheinens (also über die Hälfte) als verzichtbar identifiziert worden (Flätgen 2022).

Der geringen Akzeptanz der vorhandenen Schriftformsurrogate bei Bürgern und Unternehmen sollte abgeholfen werden (vgl. LT-Drs. SL 16/1806: S. 162, 287). Ziel des Normenscreenings war es daher, sofern möglich ein einfaches elektronisches Verfahren (E-Mail) als ausreichend zu etablieren (vgl. Flätgen 2022; LT-Drs. SL 16/1806: S. 162, 287).

Von den geänderten Vorschriften sind zwar auch einige mit Potenzial für Relevanz bei der OZG-Umsetzung in den kommunalen Verwaltungen (wie § 3 Abs. 4 SGastG, die Anzeige des vorübergehenden Betriebs eines Gaststättengewebes), jedoch betreffen ein Großteil der Änderungen verwaltungsinterne Prozesse (Flätgen 2022). Auch Potenzial für die verwaltungskundenfreundlichere, eID-freie Bereitstellung von OG-Leistungen wurde scheinbar nicht genutzt. So teilte Flätgen auf Nachfrage mit, dass die Rechtsbereinigung keine direkten Auswirkungen auf die OZG-Umsetzung im Saarland hatte und der Fokus auf der Ermöglichung von E-Mail-Kommunikation lag.

Zieht man in Betracht, dass Normenscreenings zum Schriftformersatz auf kommunaler Ebene bislang erst selten stattgefunden haben (siehe Abschn. 3.5.3), so ergibt sich die Vermutung, dass es im Zuge der kommunalen OZG-Umsetzung noch häufig nötig sein wird, Verwaltungsleistungen, die einer Schriftformerfordernis unterliegen, mit einem Schriftformersatz gem. § 3a VwVfG zu digitalisieren.

4 Vertrauensniveau

4.1 Konzept des Vertrauensniveaus in der eIDAS-VO

Die eIDAS-Verordnung schaffte im Jahr 2014 den Rahmen für sichere elektronische Interaktion und Vertrauen in elektronische Transaktionen im europäischen Binnenmarkt. Als EU-Verordnung entfaltet sie gem. Art. 288 S. 2 AEUV in allen EU-Mitgliedstaaten unmittelbare Wirkung. Sie trifft zahlreiche Bestimmungen zur elektronischen Identifizierung und zu Vertrauensdiensten, darunter auch Vorgaben zu Sicherheitsniveaus elektronischer Identifizierungssysteme. Mehrere eIDAS-Durchführungsverordnungen und -beschlüsse legen weitere Details fest.[26] Zusätzlich regelt das Vertrauensdienstegesetz Zuständigkeiten und präzisiert Vorgaben.

Nach der eIDAS-VO gibt das Sicherheitsniveau den Grad des Vertrauens in die behauptete Identität einer Person an (vgl. eIDAS-VO, Erwägungsgrund 16; EU-Kommission 2020). Es soll „Gewissheit schaffen, dass es sich bei der Person, die eine bestimmte Identität beansprucht, tatsächlich um die Person handelt, der diese Identität zugewiesen wurde“ (eIDAS-VO, Erwägungsgrund 16).

Art. 8 Abs. 2 eIDAS-VO legt die drei Sicherheitsniveaus „niedrig“, „substanziell“ und „hoch“ fest und definiert sie als sich auf solche elektronische Identifizierungsmittel beziehend, die ein „begrenztes“, „substanzielles“ bzw. „höheres Maß an Vertrauen in die beanspruchte oder behauptete Identität einer Person“ vermitteln. Maßstab für die Einordnung sind die „technischen Spezifikationen, Normen und Verfahren einschließlich technischer Überprüfungen“, die der „Verhinderung des Identitätsmissbrauchs oder der Identitätsveränderung“ dienen. Je höher das Vertrauensniveau ist, desto widerstandsfähiger ist das elektronische Identifizierungsmittel gegen Angriffe (vgl. Schönen 2020: S. 25).

Obwohl die Bezeichnung „assurance level“ (oder „level of assurance“) aus der englischen Version der eIDAS-VO mit „Sicherheitsniveau“ ins Deutsche übersetzt wurde, ist nichts anderes als „Vertrauensniveau“ gemeint (vgl. TR-03107-1: S. 8, 58; BMI 2021d: S. 103).

Es ist anzumerken, dass das Vertrauensniveau aus der eIDAS-VO nur die Identifizierung von Personen betrifft (vgl. eIDAS-VO, Erwägungsgrund 16; TR-03107-1: S. 9).

4.2 Konzept des Vertrauensniveaus in der TR-03107

Die Technische Richtlinie TR-03107 mit dem Titel „Elektronische Identitäten und Vertrauensdienste im E-Government“ ist die „nationale Ausprägung der eIDAS-Regulierung“ (Schönen 2020: S. 25). Das BSI konkretisiert in ihr die technischen Anforderungen an Identifizierungsmittel (vgl. BMI 2021d: S. 103). TR-03107 besteht aus zwei Teilen: Teil 1 („Vertrauensniveaus und Mechanismen“) definiert Vertrauensniveaus für Verfahren zu

[26] Durchführungsbeschluss (EU) 2015/296 vom 24.02.2015 zur Festlegung von Verfahrensmodalitäten für die Zusammenarbeit zwischen den Mitgliedstaaten auf dem Gebiet der elektronischen Identifizierung gemäß Artikel 12 Absatz 7 der eIDAS Verordnung; Durchführungsverordnung (EU) 2015/1501 vom 08.09.2015 über den Interoperabilitätsrahmen gemäß Artikel 12 Absatz 8 der eIDAS Verordnung; Durchführungsverordnung (EU) 2015/1502 vom 08.09.2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der eIDAS Verordnung; Durchführungsbeschluss (EU) 2015/1984 vom 03.11.2015 zur Festlegung der Umstände, Formate und Verfahren der Notifizierung gemäß Artikel 9 Absatz 5 der eIDAS Verordnung.

elektronischen Identitäten und Vertrauensdiensten und kategorisiert beispielhaft entsprechende Mechanismen; Teil 2 („Schriftformersatz mit elektronischem Identitätsnachweis“) macht Vorgaben für den Schriftformersatz mit elektronischem Identitätsnachweis gem. § 3a VwVfG (vgl. TR-03107-1: S. 7). Beide Teile wurden 2014 veröffentlicht; Teil 1 wurde zuletzt 2019 aktualisiert (vgl. TR-03107-1: S. 1; TR-03107-2: S. 1).

Die Definition der Vertrauensniveaus in der TR-03107 geht über die der eIDAS-VO hinaus. Neben Prozessen zur Identifizierung von Personen werden hier auch solche für Organisationseinheiten und Ressourcen betrachtet (vgl. TR-03107-1: S. 8). Der größere Unterschied besteht aber darin, dass auch die Prozesse „Abgabe einer Willenserklärung/Transaktionsauthentisierung, zum Beispiel als Zustimmung zu bestimmten Verwaltungsdienstleistungen/Geschäftsvorgängen oder Dokumenteninhalten“ und „Elektronische Übermittlung von Dokumenten und Identitätsdaten“ berücksichtigt werden (vgl. TR-03107-1: S. 8). Mit dieser Erweiterung nimmt die TR-03107 einen umfassenderen Blickwinkel ein (siehe auch Absch.4.4).

Anders als in der eIDAS-VO, die die Vertrauensniveaus als Abstufung der Vertrauenswürdigkeit einer behaupteten Identität versteht, definiert TR-03107-1 sie über die Schadensauswirkungen bei einer Kompromittierung (vgl. TR-03107-1: S. 8). Das Niveau „normal“ wird dabei begrenzten und überschaubaren Auswirkungen zugeordnet, Niveau „substanziell“ substanziellen Auswirkungen und das Niveau „hoch“ potenziell beträchtlichen Auswirkungen (vgl. TR-03107-1: S. 8). Zusätzlich zu diesen drei Niveaus, die „niedrig“, „substanziell“ und „hoch“ aus der eIDAS-VO entsprechen, werden die Niveaus „untergeordnet“ und „hoch +“ eingeführt (vgl. TR-03107-1: S. 8; siehe auch Tab. 3 auf S. 33). Dabei wird das Niveau „untergeordnet“ Geschäftsprozessen zugeordnet, bei denen eine Kompromittierung vernachlässigbare Schadensauswirkungen verursacht (vgl. TR-03107-1: S. 8). Das Niveau „hoch +“ wird verwendet, wenn aufgrund von Formvorschriften zusätzliche Anforderungen bestehen (vgl. TR-03107-1: S. 8).

Das BSI bezeichnet diese Abweichung als „im Wesentlichen historisch gewachsen“ und führt Überschneidungen auf ähnliche Überzeugungen auf Bundes- und EU-Ebene zurück (Felix Bleckmann, Referat DI 12, BSI, persönliche Kommunikation, 23.03.2022). Die Entwicklung der beiden Dokumente hätte parallel stattgefunden, und „Punkte aus der eIDAS-VO [wären in die TR-03107] übernommen [worden]“ (Felix Bleckmann, Referat DI 12, BSI, persönliche Kommunikation, 23.03.2022).

4.3 Weitere Standards und technische Umsetzung

Neben der eIDAS-VO und der TR-03107-1 gibt es noch weitere Standards, die Vertrauensniveaus definieren. Zu nennen sind hier ISO/IEC 29115:2013 und – für den US-amerikanischen Kontext – NIST SP 800-63-3. Dabei geht letztere mit ihren Bestandteilen Identity Proofing, Digital Authentication und Federated Identity Management, ebenso wie TR-03107-1, über die elektronische Identifizierung von Personen hinaus.

Aufgrund der eingeschränkten Vergleichbarkeit können die verschiedenen Vertrauensniveaus nicht eindeutig zugeordnet werden. Eine Annäherung für die TR-03107-1, ISO/IEC 29115:2013 und die eIDAS-VO zeigt die TR-03107-1 (vgl. TR-03107-1: S. 58).

Gemeinsam haben diese Standards, dass ihr Fokus auf den technischen Vorausset-

zungen liegt, die für ein bestimmtes Vertrauensniveau benötigt werden. Es werden Anforderungen formuliert und verschiedene Mechanismen klassifiziert. Für die TR-03107-1 gibt Abb. 2 eine Übersicht.

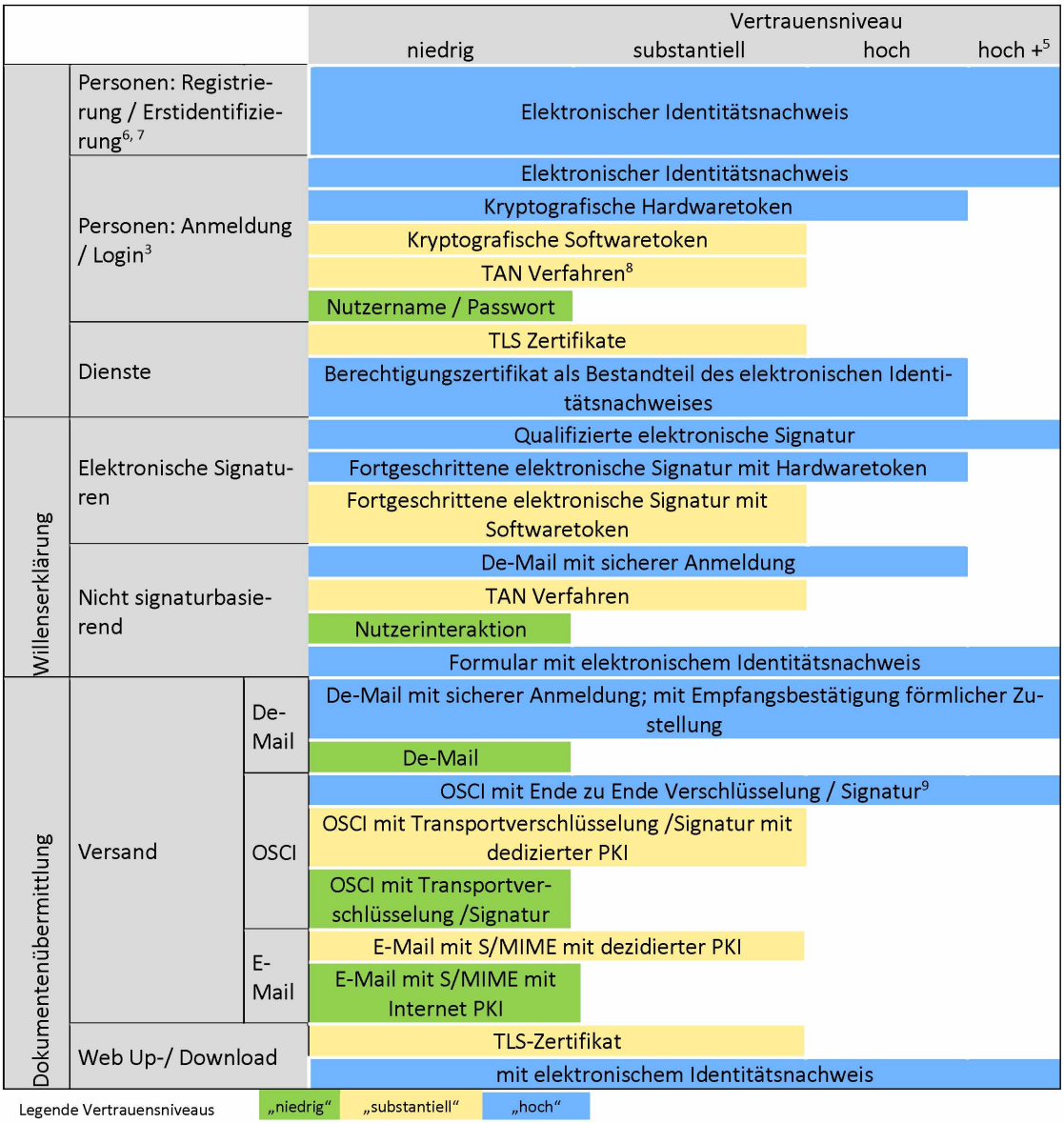


Tabelle 2: Übersicht zu den Anforderungen der verschiedenen Vertrauensniveaus an die eingesetzten Mechanismen (aus IT-Planungsrat 2020: S. 14; basiert auf TR-03107-1)[27]

Da sich diese Arbeit mit der Festlegung des Vertrauensniveau im Sinne einer „Bedarfsfeststellung“ beschäftigt, die aus Sicht der jeweiligen Verwaltungsleistung zunächst prüft, welches Vertrauensniveau benötigt wird, werden die Details zur technischen Umsetzung eines einmal festgelegten Vertrauensniveau nicht weiter beleuchtet.

[27] Auf die Erläuterungen zu den Fußnoten in der Tabelle wurde hier aus Platzgründen verzichtet. Die fehlende zusammenfassende Überschrift für die ersten drei Zeilen sollte höchstwahrscheinlich „Identifizierung“ lauten.

4.4 Vertrauensniveau und Schutzbedarf

„Der Schutzbedarf von verarbeiteten Daten darf NICHT mit dem Vertrauensniveau der Daten gleichgesetzt werden!“ warnt Richter-Schuppan (2021) im OZG-Newsletter der SAKD. Während dies grundlegend korrekt ist, darf nicht der Eindruck erweckt werden, es bestünde kein Zusammenhang zwischen Schutzbedarf und Vertrauensniveau.

Bei Anwendung der IT-Grundschutz-Methodik des BSI wird im Rahmen einer Schutzbedarfsfeststellung untersucht, wie viel Schutz der betrachtete Informationsverbund[28] und die ihm zugehörigen Zielobjekte bezüglich Vertraulichkeit, Integrität und Verfügbarkeit benötigen (vgl. BSI 200-2: S. 104). Es wird danach gefragt, welche Schäden bei Verletzung dieser drei Schutzziele entstehen könnten, und was deren Ausmaß wäre (vgl. BSI 200-2: S. 104).

Die Schutzbedarfsfeststellung für einen Informationsverbund gliedert sich in mehrere Schritte: Definition der Schutzbedarfskategorien, gefolgt von Schutzbedarfsfeststellungen jeweils für Geschäftsprozesse und Anwendungen, für IT-Systeme, IoT- und ICS-Geräte, für Gebäude, Räume, Werkhallen usw. sowie für Kommunikationsverbindungen (vgl. BSI 200-2: S. 104). Dabei unterstützt eine Liste typischer Schadensszenarien die Bewertung. Den Abschluss bilden die Schlussfolgerungen aus den Ergebnissen der Schutzbedarfsfeststellung, d. h. den bewerteten Zielobjekten wurde eine Schutzbedarfskategorie (meist zwischen „normal“ und „sehr hoch“) zugeordnet, die angibt, wie hoch die potenziellen Schadensauswirkungen bei einer Kompromittierung sind. An der Festlegung des Schutzbedarfs orientieren sich dann die zu erfüllenden Sicherheitsanforderungen (vgl. BSI 200-2: S. 104).

Die TR-03107-1 empfiehlt „die Feststellung des notwendigen Vertrauensniveaus auf Basis einer Schutzbedarfsfeststellung nach [BSI 200-2] unter zusätzlicher Berücksichtigung rechtlicher Vorgaben durchzuführen“ (TR-03107-1: S. 13). Gemeint sein muss dabei die Feststellung des Schutzbedarfs für Geschäftsprozesse und Anwendungen, genauer für die Prozesse Identifizierung, Willenserklärung und Daten-/Dokumentenübermittlung für eine OZG-Leistung. Vor dem Hintergrund der zwischenzeitlich eingetretenen rechtlichen Verpflichtung, die TR-03107-1 einzuhalten (siehe Abschn. 5.1), kann die Bedeutung der Schutzbedarfsfestlegung für die Vertrauensniveaubestimmung nicht geleugnet werden (siehe auch Abschn. 5.4.2).

Richter-Schuppan (2021) führt weiter aus, dass das Vertrauensniveau – anders als der Schutzbedarf „hingegen ausschließlich im Kontext der elektronischen Identifizierung und für die Bewertung von Verfahren zur Identitätsprüfung natürlicher und juristischer Personen verwendet [wird]“. Durch Abgleich mit den in Abschn. 4.2 dargestellten Informationen zur TR-03107 lässt sich leicht feststellen, dass dies nicht korrekt ist.

Die TR-03107-1, die ein weiteres Konzept des Vertrauensniveau als die eIDAS-VO vertritt, definiert ein Vertrauensniveau eben nicht darüber, „wie stark der Quelle der Daten vertraut werden kann“ (Richter-Schuppan 2021), sondern – ebenso wie bei der Schutz-

[28] „Ein Informationsverbund umfasst die Gesamtheit von infrastrukturellen, organi satorischen, personellen und technischen Komponenten, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen“ (BSI 200-2: S. 62).

bedarfsfeststellung – über das Ausmaß des potenziellen Schadens bei einer Kompromittierung (TR-03107-1: S. 8).

In Tab. 3 werden die verschiedenen Abstufungen der Sicherheitsniveaus, Vertrauensniveaus und Schutzbedarfskategorien gegenübergestellt. Dabei ist zu beachten, dass die Schutzbedarfskategorie „sehr hoch“ keine Entsprechung bei den Sicherheits- bzw. Vertrauensniveaus findet, da es „mit Mechanismen, die IT-Systeme des Endanwenders nutzen, im Allgemeinen nicht erreichbar [ist]“ (TR-03107-1: S. 12). Das Vertrauensniveau „hoch +“ wiederum ist nicht als Sicherheitsniveau oder Schutzbedarfskategorie abzubilden, da es sich auf die besonderen Anforderungen bezieht, die ein Schriftformerfordernis an die Umsetzung des Vertrauensniveaus stellt (vgl. TR-03107-1: S. 4).

Sicherheitsniveaus der eIDAS-VO	Vertrauensniveaus der TR-03107-1 bzw. aus IT-Planungsrat (2020)	Schutzbedarfskategorien des BSI 200-2
–	untergeordnet	ggf. unkritisch[29]
niedrig	normal	normal
substanziell	substanziell	normal bis hoch
hoch	hoch	hoch
–	hoch +	–
–	–	sehr hoch

Tabelle 3: Vergleich von Sicherheitsniveaus, Vertrauensniveaus und Schutzbedarfskategorien (vgl. TR-03107-1: S. 12; IT-Planungsrat 2020: S. 3 f.; BSI 200-2: S. 72 ff., 105 ff.)

Die Frage nach dem Grund für die Überschneidungen und Abweichungen zwischen Sicherheitsniveaus eIDAS-VO und Vertrauensniveaus i. S. d. der TR-03107 wurde in Abschn. 4.2 schon kurz angesprochen. Hier soll sie vor dem Hintergrund des Zusammenhang mit der Schutzbedarfsfeststellung erneut aufgegriffen werden.

Eine Erklärung dafür, warum für die über die Identifizierung hinausgehenden Prozesse nicht auf die zum Zeitpunkt der Verfassung der TR-03107 bereits in BSI 100-2 (inzwischen BSI 200-2) definierten Schutzbedarfskategorien (ggf. erweitert durch eine Stufe zwischen „normal“ und „hoch“, siehe Tab. 3) abgestellt wurde, die dann separat von der Bestimmung des Vertrauensniveaus bei einer Schutzbedarfsfeststellung zu betrachten und bewerten gewesen wären, wurde auf entsprechende Nachfrage nicht gegeben (Felix Bleckmann, Referat DI 12, BSI, persönliche Kommunikation, 23.03.2022).

Vor dem Hintergrund, dass für die Vertrauensniveaubestimmung dieselbe Liste an Schadenskategorien zugrundegelegt wird (vgl. TR-03107-1: S. 14; siehe Tab. 4 auf S. 41), die auch bei der Schutzbedarfsfeststellung (hier unter der Bezeichnung Schadensszenarien) zum Einsatz kommt (vgl. BSI 200-2: S. 105), erscheint die Trennung bzw. Dopplung unnötig (siehe auch Abschn. 5.3 und 5.4.2). Anderseits ist aber zu bemerken, dass die Verfahren ansonsten nicht unbedingt vergleichbar sind: Für die Vertrauensniveaube-

[29] Die Schutzbedarfskategorie „unkritisch“ gehört nicht zu den von BSI 200-2 definierten, die IT-Grundschutz-Methodik enthält aber die Möglichkeit, zusätzliche Schutzbedarfskategorien einzuführen (vgl. BSI 200-2: S. 104).

wertung wird eine Risikobetrachtung empfohlen (vgl. IT-Planungsrat 2020: S. 11), während das bei einer Schutzbedarfsfeststellung nicht notwendigerweise der Fall ist (vgl. BSI 200-2, S. 104 ff.; BSI 200-3: S. 9 ff.). Auch werden bei der Vertrauensniveaubewertung einzelne Prozessschritte statt ganzer Geschäftsprozesse betrachtet. Somit könnte eine Schutzbedarfsfeststellung eventuell nicht die gleichen bzw. nicht gleich genaue Ergebnisse wie eine Vertrauensniveaubestimmung erreichen. Inwieweit eine andere Abgrenzung der Konzepte und Verfahren sinnvoll gewesen wäre, bleibt unklar.

Dass diese Frage in der vorliegenden Arbeit nicht abschließend geklärt werden kann, hat für die weiteren Arbeitsergebnisse keine Auswirkungen, da die TR-03107-1 unabhängig von der Begründung ihrer Genese anzuwenden ist (siehe Abschn. 5.1).

5 Vertrauensniveaubestimmung

5.1 Verpflichtende Vorgaben für die Festlegung von Vertrauensniveaus

In der Literatur herrscht Einigkeit darüber, dass „die Identifizierungsmittel des Nutzerkontos die Vertrauensniveaus der eIDAS-Verordnung erfüllen müssen“ (Schnattinger 2019: S. 17; Denkhaus/Richter/Bostelmann 2019: § 8 EGovG Rn. 3; vgl. BT-Drs. 18/11135: S. 94; Herrmann/Stöber 2017: S. 1405). Daraus ergibt sich zunächst aber nur die allgemeine Verpflichtung, drei Vertrauensniveaus anzubieten, die die Abstufungen des Vertrauens in die behauptete Identität einer Person wiedergeben (siehe auch Abschn. 4.1).

Im Zusammenhang mit der Erwähnung der Notwendigkeit, im Rahmen der OZG-Umsetzung Vertrauensniveaus festzulegen, wird darüberhinaus meist auch auf die technische Richtlinie TR-03107-1 verwiesen – jedoch ohne darauf einzugehen, ob und inwieweit bzw. wobei und durch wen eine rechtliche Verpflichtung zu deren Einhaltung besteht (vgl. z. B. NEGZ 2019: S. 11 ff.; Schnattinger 2019: S. 17; Denkhaus/Richter/Bostelmann 2019: § 8 OZG Rn. 3; IT-Planungsrat 2020: S. 10 ff.; BMI 2021d: S. 103). Auch die Abweichungen zur eIDAS-VO bleiben unerwähnt (siehe Abschn. 4.2). Dies gilt auch im Kontext der OZG-Umsetzung im Freistaat Sachsen (vgl. z. B. Kretschmer 2021: S. 150).

Prüft man die tatsächliche Rechtslage, ist zunächst festzustellen, dass technische Richtlinien des BSI nur Empfehlungscharakter haben, solange nichts anderes vorgegeben ist (BSI 2021). Zwar wird die TR-03107 in einer Publikation des BSI als „nationale Ausprägung der eIDAS-Regulierung“ bezeichnet (Schönen 2020: S. 25; siehe auch Abschn. 4.2), eine entsprechende rechtliche Regelung fand sich im einschlägigen Europa- oder Bundesrecht aber bis vor Kurzem nicht (siehe unten).

Auch aus dem sächsischen Landesrecht ergibt sich keine direkte Verpflichtung, sich an die TR-03107 zu halten.[30]

Eine solche Verpflichtung könnte gemäß § 13 SächsEGovG für die Träger der Selbstverwaltung bestehen, wenn der IT-Planungsrat sie als verbindlich vorgeben würde. Und auch § 4 SächsISichG Abs. 2 S. 3 verpflichtet zur Einhaltung der vom IT-Planungsrates beschlossenen Standards. Ein entsprechender Beschluss wurde jedoch vom IT-Planungsrat bislang nicht getroffen (vgl. IT-Planungsrat 2022).

Das SächsISichG verpflichtet zwar staatliche Stellen, das IT-Grundschutz-Kompendium und die BSI-Standards zu berücksichtigen (§ 4 SächsISichG Abs. 1 S. 4). Für nichtstaatliche Stellen werden diese allerdings nur zur Anwendung empfohlen (§ 4 SächsISichG Abs. 2 S. 2) – im Unterschied etwa zu verbindlichen Vorgaben des IT-Planungsrates, die auch für nicht-staatliche Stellen im Anwendungsbereich unmittelbar verbindlich würden (S. 3). Die technischen Richtlinien des BSI finden dabei ebenfalls keine ausdrückliche Erwähnung.

Durch § 4 SächsISichG Abs. 2 S. 3 Alt. 2 werden nicht-staatliche Stellen allerdings zur Einhaltung der nach § 5 OZG festgelegten Informationssicherheitsstandards verpflichtet. § 5 OZG regelt die IT-Sicherheit im Portalverbund, und ermächtigt das BMI, durch

[30] Anders in Nordrhein-Westfalen: Dort sah man mit dem EGovG NRW eine Einhaltung der Standards aus TR-03107 von Anfang an vor (LT-Drs. NRW 16/10379: S. 47 ff.).

Rechtsverordnung entsprechende Standards festzulegen. Bis vor Kurzem gab es eine solche Rechtsverordnung nicht.

Mit Inkrafttreten der ITSiV-PV am 20. Januar 2022 hat sich dies geändert: Die ITSiV-PV des BMI legt diejenigen Standards fest, die zur Aufrechterhaltung der IT-Sicherheit im Portalverbund und bei den zur Anbindung an den Portalverbund genutzten IT-Komponenten notwendig sind. Diese Standards sind, wie oben erwähnt, nach § 4 SächsISichG Abs. 2 S. 3 Alt. 2 auch durch Kommunen bei der OZG-Umsetzung einzuhalten. Gemäß § 2 Abs. 2 ITSiV-PV gehört auch die TR-03107-1 zu diesen Standards (nicht aber TR-03107-2).

Die TR-03107-1 ist damit also auch für sächsische Kommunen verbindlich vorgegeben – besonders relevant ist dies bei der Basiskomponente Servicekonto, über die Identifizierung und Authentifizierung erfolgen, und die auch ein Nutzerkonto im Portalverbund nach § 3 Abs. 2 OZG darstellt (vgl. § 1 Abs. 11 S. 2 SächsEGovGDVO).

5.2 Vertrauensniveaufestlegung für Verwaltungsleistungen mit Schriftformerfordernis

Da die Vertrauensniveaufestlegung bei Verwaltungsleistungen mit Schriftformerfordernis deutlich anders abläuft als bei Leistungen ohne ein solches Erfordernis, wird das Verfahren hier kurz separat erläutert.

Grundsätzlich können solche Leistung gem. § 3a Abs. 2 Nr. 1 VwVfG OZG-konform umgesetzt werden (siehe Abschn. 3.3). Dazu ist die Authentisierung mit eID nötig.

Darüber hinaus muss durch Auslegung der Rechtsnorm und fachliche Bewertung des Geschäftsprozesses ermittelt werden, welche Schriftformfunktionen von der jeweiligen Leistung verlangt werden (vgl. BT-Drs. 18/9177: S. 6; Denkhaus/Richter/Bostelmann 2019: § 8 OZG Rn. 4; TR-03107-2: S. 6; siehe auch Abschn. 3.2). Daher wird für solche Leistungen fas Vertrauensniveau „hoch +“ vergeben (vgl. TR-03107-1: S. 8). Bei der Bewertung und Auswahl der Mechanismen kann die TR-03107-2 helfen, welche aber nicht verpflichtend zu beachten ist (siehe Abschn. 5.1).

5.3 Vorgehensweise bei der Vertrauensniveaubestimmung

Der Fokus der TR-03107-1 liegt auf der Bewertung von Mechanismen, d. h. sie legt fest, mit welchen technischen Lösungen ein bestimmtes Vertrauensniveau umzusetzen ist und wie man einen neuen Mechanismus bezüglich seines Vertrauensniveaus bewertet. Das Verfahren zur Bestimmung des Vertrauensniveaus einer Verwaltungsleistung wird nur kurz angerissen. Genauere Anweisungen finden sich in der Handreichung des IT-Planungsrates mit den Empfehlungen zur Vertrauensniveaufestlegung (IT-Planungsrat 2020).

Diese Empfehlungen, die auf der TR-03107-1 basieren, sind zwar nur Empfehlungen, eine Beachtung erscheint vor dem Hintergrund der zwischenzeitlich eingetretenen Verbindlichkeit der Richtlinie aber ratsam. Auch wurde die Verwendung der Empfehlungen des IT-Planungsrates von Anfang an überall empfohlen (vgl. z. B. BT-Drs. 18/10183: S. 65).

Bei Veröffentlichung dieser Empfehlungen in der Version 4.00 enthielt das Dokument als Anlage ein „Excel-Tool“, mit dem „Behörden bei der Einstufung von Vertrauensniveaus

unterstützt [werden sollten]“ und mit dem sie „ihre Erkenntnisse dokumentieren [können sollten]“ (IT-Planungsrat 2020: S. 12). Inzwischen ist dieses Excel-Tool, ebenso wie die Handreichung selbst, nicht mehr verfügbar.[31]

Da sich die Anleitung zur Vertrauensniveaubestimmung aus der Handreichung in manchen Teilen scheinbar auf dieses nicht mehr zur Verfügung stehende Excel-Tool bezieht – dessen Platz inzwischen das Praxistool Vertrauensniveau mit ähnlichem Verfahren eingenommen hat – werden in diesem Abschnitt nur kurz die Grundlagen der in der Handreichung empfohlenen Vorgehensweise erläutert. Auf weitere Details der Vertrauensniveaubestimmung mit dem Praxistool Vertrauensniveau geht Abschn. 5.4.2 ein; kritische Anmerkungen dazu finden sich in Abschn. 5.5.

Für die Vertrauensniveaubewertung empfiehlt die Handreichung ein zweischrittiges Vorgehen (IT-Planungsrat 2020: S. 9 f.). Zunächst soll ein vorläufiges Vertrauensniveau ermittelt werden, was danach im Abgleich mit den Erfahrungen aus der Verwaltungspraxis angepasst werden kann.

Dabei soll jeder Teilprozess einzeln betrachtet werden. Die nach der TR-03107-1 zu bewertenden Prozesse (Identifizierung von Personen, Identifizierung von Dienstanbietern, Abgabe einer Willenserklärung, Dokumentenübermittlung und Übermittlung von Identitätsdaten; vgl. TR-03107-1: S. 13), wurden in der Handreichung zu drei Prozessen (Identifizierung, Willenserklärung und Daten- bzw. Dokumentenübermittlung[32]) zusammengefasst (vgl. IT-Planungsrat 2020: S. 9 f.).

Für jeden Teilprozess wird „auf Basis der einzelnen Gefährdungen und potentiellen Schäden [...] sowie der abstrakten Eintrittswahrscheinlichkeit“ das jeweilige Vertrauensniveau ermittelt. Unterstützen soll dabei eine Tabelle mit potenziellen Gefährdungen und Vertrauensniveaubewertungen in Abhängigkeit von der Schadenshöhe (siehe Tab. 4).

Nach dieser vorläufigen Bewertung im ersten Schritt werden im zweiten Schritt „konkrete Erfahrungen der Verwaltungspraxis der jeweiligen Behörde“ berücksichtigt (IT-Planungsrat 2020: S. 10). Die abstrakt ermittelten Vertrauensniveaus werden mit praktischen Erfahrungen abgeglichen, und bei Abweichungen in der Bewertung kann das Vertrauensniveau auf- oder abgewertet werden – aber höchstens um eine Stufe. Eine Anleitung dazu gibt Tab. 5.

Die Erläuterungen zur Vorgehensweise enthalten keine Hinweise zur Bestimmung des Gesamtergebnisses der Vertrauensniveaubewertung. Ob eine solche Gesamtbewertung überhaupt das Ziel ist, ist unklar. An anderer Stelle wird empfohlen, bei der gemeinsamen Betrachtung mehrerer Teilprozesse das Maximum der für die einzelnen Prozessschritte ermittelten Vertrauensniveaus als Ergebnis anzunehmen (vgl. IT-Planungsrat 2020: S. 8), sodass davon ausgegangen werden kann, dass dieser Grundsatz auch auf das Gesamtergebnis anwendbar ist.

[31] Während es noch möglich war, das die Handreichung an anderer Stelle im Internet abzurufen, war das Excel-Tool nirgends mehr verfügbar.

[32] Die Handreichung spricht nur von Dokumentenübermittlung, die aber anscheinend die Datenübermittlung einschließt (vgl. IT-Planungsrat 2020: S. 7).

Gefährdung	Potentieller Schaden bedingt Vertrauensniveau		
	Normal	**Substantiell**	**Hoch**
Verstoß gegen Gesetze/Vorschriften	Verstoß mit geringfügigen Konsequenzen	Verstoß mit substantiellen Konsequenzen	Verstoß mit erheblichen Konsequenzen Besondere Formvorschriften (*hoch +*) bei Gefahr eines Verstoßes mit schwerwiegenden Konsequenzen
Unrichtige Identifizierung oder Zuordnung zu einer Identität	Geringfügige Konsequenzen	Substantielle Konsequenzen	Erhebliche Konsequenzen Besondere Formvorschriften (*hoch +*) bei Gefahr von schwerwiegenden Konsequenzen
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Verarbeitung personenbezogener Daten, die den Betroffenen in seiner gesellschaftlichen Stellung oder seinen wirtschaftlichen Verhältnissen beeinträchtigen können.	Verarbeitung personenbezogener Daten, die den Betroffenen in seiner gesellschaftlichen Stellung oder seinen wirtschaftlichen Verhältnissen substantiell beeinträchtigen können.	Verarbeitung personenbezogener Daten, die den Betroffenen in seiner gesellschaftlichen Stellung oder seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen können.
Beeinträchtigung körperlicher/persönlicher Unversehrtheit	Beeinträchtigung erscheint nicht möglich	Beeinträchtigung kann nicht vollständig ausgeschlossen werden	Beeinträchtigung kann nicht ausgeschlossen werden
Beeinträchtigung der Aufgabenerfüllung	Beeinträchtigung wird von den Betroffenen als tolerabel eingeschätzt	Beeinträchtigung wird von einzelnen Betroffenen als tolerabel eingeschätzt	Beeinträchtigung wird als nicht tolerabel eingeschätzt
Negative Innen- oder Außenwirkung	Geringe/nur interne Ansehens- oder Vertrauensbeeinträchtigung zu erwarten	Substantielle Ansehens- oder Vertrauensbeeinträchtigung zu erwarten	Breite Ansehens- oder Vertrauensbeeinträchtigung zu erwarten
Finanzielle Auswirkungen	Finanzieller Schaden tolerabel	Substantieller finanzieller Schaden möglich	Beachtliche finanzielle Verluste, jedoch nicht existenzbedrohend
Zu beachten: Die Aggregation von Gefährdungen kann zur Erhöhung des notwendigen Vertrauensniveaus führen. Zum Beispiel kann die Verarbeitung personenbezogener Daten mit Schutzbedarf *substantiell* zu einem notwendigen Vertrauensniveau *hoch* führen, wenn viele Personen von einer Beeinträchtigung betroffen sind. Sind mehrere Gefährdungen relevant, so ist für die Gesamtbewertung das Maximum der einzeln ermittelten notwendigen Vertrauensniveaus anzunehmen.			

Tabelle 4: Zuordnung von potenziellen Schäden zu den verschiedenen Vertrauensniveaus anhand möglicher Gefährdungen/Schadenskategorien (aus TR-03107-1: S. 14; IT-Planungsrat 2020: S. 10)

		Vertrauensniveau		
		niedrig	**substantiell**	**hoch**
Eintrittswahrscheinlichkeit	**unwahrscheinlicher**	niedrig	niedrig	substantiell
	Normal	niedrig	substantiell	hoch
	wahrscheinlicher	substantiell	hoch	hoch

Tabelle 5: Möglichkeiten der Auf- und Abwertung des Vertrauensniveaus (aus IT-Planungsrat 2020: S. 10)[33]

5.4 Praxistool Vertrauensniveau

5.4.1 Hintergrund und Übersicht

Statt des inzwischen nicht mehr verfügbaren Excel-Tool (siehe Abschn. 5.3) bietet das BMI unter https://vn-check.ozg-umsetzung.de/ ein interaktives Online-Tool an, das bei der Vertrauensniveaubewertung unterstützt. Das sog. Praxistool Vertrauensniveau führt die Nutzer durch eine Reihe von Fragen und gibt abschließend eine Einschätzung zum passenden Vertrauensniveau.

Da die Handreichung mit den Empfehlungen für die Zuordnung von Vertrauensniveaus – wie bereits erwähnt – aktuell nicht zur Verfügung steht, bleibt nur der Rückgriff auf das Praxistool. Im OZG-Leitfaden des BMI wird es als Arbeitshilfe beworben (vgl. BMI 2020), auch auch im Kontext der sächsischen OZG-Umsetzung wird es zur Anwendung empfohlen (vgl. Kretschmer 2021: S. 150).

Das Praxistool ist für „Fachexperten der zuständigen Behörden“ vorgesehen und soll dazu dienen, für Antragsprozesse „im Rahmen der Digitalisierungslabore bzw. der Entwicklung eines Prototyps“ das erforderliche Vertrauensniveau zu ermitteln (BMI 2021e). Es wurde durch die Firma]init[AG für digitale Kommunikation realisiert.

5.4.2 Verfahren

Das Vertrauensniveau eines Online-Antragsverfahrens wird im Praxistool Vertrauensniveau über die Beantwortung von Fragen in zwei Abschnitten bestimmt. Eine Übersicht zum Verfahren gibt Abb. 9. Dabei zeigt der obere Teil der Abbildung die Prozessschritte die ein Nutzer beim Antragsprozess durchläuft, für die der Schutzbedarf festgestellt wird,

[33] In Tab. 5 scheint sich die Spaltenüberschrift „Vertrauensniveau“ auf das im ersten Schritt basierend auf der abstrakten Eintrittswahrscheinlichkeit ermittelte Vertrauensniveau zu beziehen und die Zeilenüberschrift „Eintrittswahrscheinlichkeit“ auf die konkrete Eintrittswahrscheinlichkeit von aus der Praxis bekannten Gefährdungen.

und der untere Teil die dahinterstehenden Prozesse eines typischen Verwaltungsprozesses, die bei der Vertrauensniveaubestimmung betrachtet werden.

Diese Zweiteilung gleicht der Vorgehensweise, die in der Handreichung des IT-Planungsrates empfohlen wird. Statt des „abstrakten Vertrauensniveaus“ wird im Praxistool jedoch zunächst der Schutzbedarf festgestellt und danach anhand konkreter Schadensfällen das Vertrauensniveau.

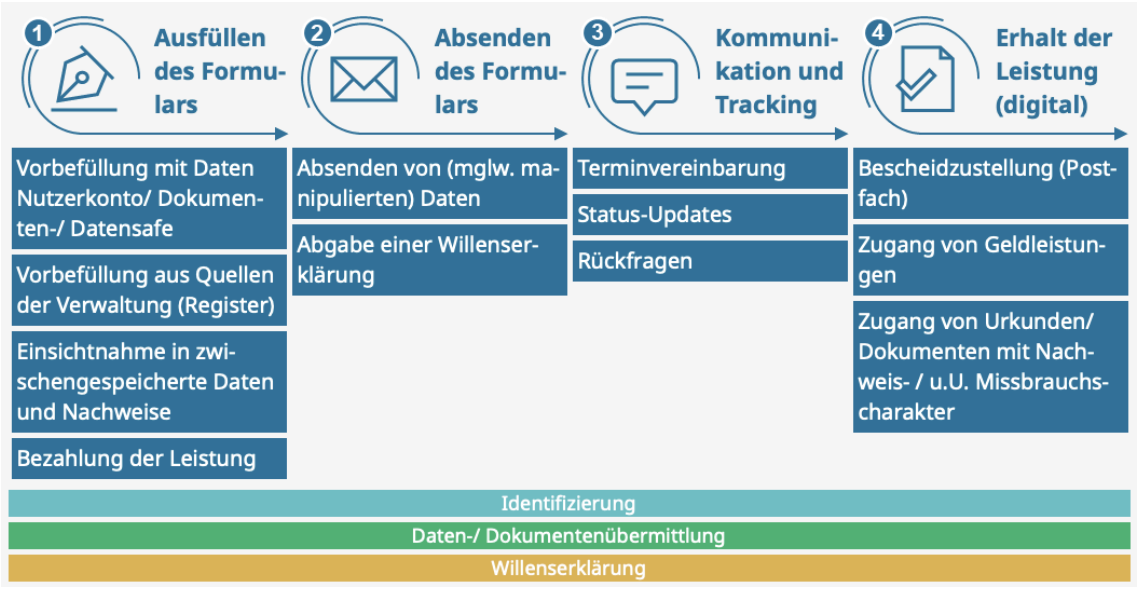


Abbildung 9: Übersicht Praxistool Vertrauensniveau (BMI 2021e)

5.4.2.1 Fragenabschnitt zum Schutzbedarf

Das Praxistool bewertet im ersten Fragenabschnitt den Schutzbedarf für vier Prozessschritte „entlang der Nutzerreise eines Antragsprozesses“ (BMI 2021e): Ausfüllen des Formulars, Absenden des Formulars, Kommunikation und Tracking sowie Erhalt der Leistung (digital). Dabei wird der Nutzer nach und nach durch eine Reihe von Fragen mit jeweils zwei vordefinierten Antwortmöglichkeiten geführt. Zusätzlich besteht die Möglichkeit, Notizen zu machen.

Mit Ausnahme des ersten Prozessschrittes, für den die Fragen die erfassten Daten und die Möglichkeit deren Zwischenspeicherung betreffen, beziehen sich die Fragen auf potenzielle Schäden bei den Prozessschritten und deren Eintrittswahrscheinlichkeiten. Eine vollständige Übersicht über die Fragen und Antwortmöglichkeiten geben Anh. 1 und 3.

Sind für einen Prozessschritt alle Fragen beantwortet, zeigt das Praxistool sofort eine Bewertung des Schutzbedarfs und das entsprechende Vertrauensniveau für diesen Prozessschritt an.

5.4.2.2 Fragenabschnitt zum Vertrauensniveau

Im zweiten Fragenabschnitt wird das Vertrauensniveau für die Prozesse Identifizierung, Willenserklärung und Daten-/Dokumentenübermittlung ermittelt. Dabei soll der Nutzer Schadensfälle mit Gefährdung/Schadenskategorie, Schadenshöhe und Eintrittswahrscheinlichkeit dokumentieren. Bei jedem der drei betrachteten Prozesse muss der Nutzer für

mindestens eine Gefährdung/Schadenskategorie die entsprechenden Angaben machen sowie eine kurze Beschreibung eines möglichen Schadensfalls geben.

Die Liste der Gefährdungen entspricht derjenige aus TR-03107-1 (siehe Tab. 4); für Schadenshöhe und Eintrittswahrscheinlichkeit kann jeweils zwischen drei Niveaus gewählt werden. Eine vollständige Liste der Fragen und Antwortmöglichkeiten zeigen die Tabelle in Anh. 2 und 4.

Die im ersten Fragenabschnitt ermittelten Schutzbedarfe bzw. die entsprechenden Vertrauensniveaus sollen dafür die Grundlage bilden und werden beim relevanten Prozess angezeigt. Welcher der relevante Prozess ist, also der Schutzbedarf welches Prozessschritts sich auf das Vertrauensniveau welches Prozesses auswirkt, ist für den Nutzer dabei nicht direkt erkennbar. Abbildung 10 zeigt die durch Überprüfung der Zusammenhänge mittels Exhaustionsmethode festgestellte Zuordnung. Im Fragenabschnitt zum Vertrauensniveau wird das im Fragenabschnitt zum Schutzbedarf höchste ermittelte Vertrauensniveau angezeigt. Für die Prozesse, die mit dem Schutzbedarf mehrerer Prozessschritte verknüpft sind, macht es dabei keinen Unterschied, ob nur einer oder mehrere Prozessschritte mit einem höheren Schutzbedarf bewertet wurden, d. h. es gilt zwar das Maximalprinzip, ein Kumulationseffekt wurde aber nicht implementiert.[34]

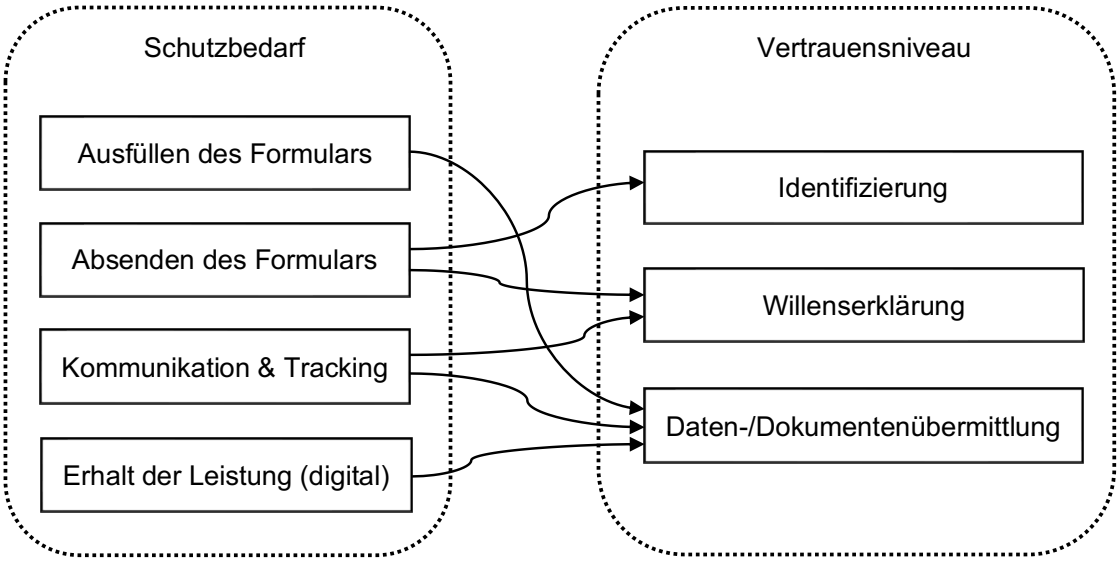


Abbildung 10: Zuordnung zwischen Schutzbedarf der Schritte und Vertrauensniveau der Prozesse im Praxistool Vertrauensniveau (eigene Darstellung)

Die im Fragenabschnitt zum Schutzbedarf vorgenommenen Bewertungen haben dabei aber selbst keinen Einfluss auf die Bestimmung des Vertrauensniveaus – diese stützt sich allein auf die im zweiten Fragenabschnitt gemachten Angaben. Auf der Informationsseite, die vor Beginn der Nutzung des Praxistools das gesamte Verfahren erläutert, heißt es dazu, dass hier für jeden Prozessschritt im Detail geprüft werden soll, „welche typischen Risiken für ihr [sic!] Verwaltungsverfahren relevanter oder weniger relevant sind“, wodurch „die Belastbarkeit des Bewertungsergebnisses erhöht werden [kann]“ (BMI 2021e).

[34] Die Begriffe „Maximalprinzip“ und „Kumulationseffekt“ beziehen sich auf die aus der Schutzbedarfsfeststellung nach IT-Grundschutz-Methodik bekannten Konzepte der Vererbung (vgl. BSI 200-2: S. 108 ff.; BSI 2022b).

Anders als im ersten Fragenabschnitt wird nach Beantwortung aller Fragen zu einem Prozessschritt nicht sofort das ermittelte Vertrauensniveau angezeigt. Die Bewertung lässt sich erst der Ergebnisübersicht entnehmen (siehe Abschn. 5.4.2.3).

5.4.2.3 Ergebnisse

Ist die Bewertung nach Beantwortung aller Fragen abgeschlossen, zeigt das Praxistool am Ende eine Übersicht der Ergebnisse an. Dabei wird für jeden Prozessschritt der festgestellte Schutzbedarf und für jeden Prozess das ermittelte Vertrauensniveau ausgegeben. Ein Gesamtergebnis für das Vertrauensniveau wird nicht gebildet, jedoch wird der Nutzer darauf hingewiesen, dass man sich am Prozessschritt mit dem höchsten Vertrauensniveau orientieren sollte.

Eine Tabelle (entnommen aus IT-Planungsrat 2020: Tab. 4) informiert den Nutzer darüber, welche Vertrauensdienste/-mechanismen für welche Vertrauensniveaus geeignet sind. Schließlich gibt es die Möglichkeit, die Ergebnisse als PDF zu speichern.

5.5 Kritikpunkte

Abgesehen von der Handreichung mit den Empfehlungen des IT-Planungsrats (IT-Planungsrat 2020) ist das Praxistool die einzige verfügbare Hilfestellung für die Festlegung des Vertrauensniveaus. Da sich die Handreichung – wie bereits in Kap. 1 erwähnt – seit Monaten in Überarbeitung befindet und nicht zur Verfügung steht, ist das Praxistool derzeit faktisch die einzige Informationsquelle für Fachexperten bei der (kommunalen) OZG-Umsetzung. Umso schwerer wiegen daher Unzulänglichkeiten im Praxistool. Einige solcher Defizite werden deshalb in den folgenden Abschnitte beleuchtet. Auch ausgewählte Probleme in der Handreichung des IT-Planungsrates, die von denen des Praxistools abweichen, werden kurz betrachtet (siehe Abschn. 5.5.4).

Zunächst wird der Blick jedoch auf eine Frage gerichtet, das direkt aus der TR-03107-1 hervorgeht (siehe Abschn. 5.5.1).

5.5.1 Gefährdungen/Schadenskategorien in der TR-03107-1

Tabelle 1 aus TR-03107-1, die auch in der Handreichung des IT-Planungsrates wiedergegeben wird (siehe Tab. 4 auf S. 41) enthält die Gefährdungen/Schadenskategorien, die bei der Vertrauensniveaufestlegung einschlägig sind. Sie basiert auf den Schadensszenarien der IT-Grundschutz-Methodik des BSI (vgl. BSI 100-2: S. 49; inzwischen BSI 200-2: S. 105) und entsprecht ihnen bis auf zwei kleine Abweichungen.[35] Abgesehen von diesen eher geringfügigen Änderungen wurde aber auch eine zusätzliche Zeile mit der Gefährdung „Unrichtige Identifizierung oder Zuordnung zu einer Identität“ hinzugefügt. Dies erscheint als Gefährdung/Schadenskategorie jedoch unpassend gewählt: Bei dieser neuen Schadenskategorie handelt es sich weniger um eine Kategorie von Schäden als vielmehr um einen Grund für den potenziellen Eintritt von Schäden anderer Schadenskategorien.

[35] In der TR-03107-1 heißt die zuerst aufgezählte Gefährdung „Verstoß gegen Gesetze/Vorschriften“; in BSI 100-2 bzw. BSI 200-2 hingegen nennt man das Schadensszenario „Verstoß gegen Gesetze/Vorschriften/ Verträge“. In der TR-03107-1 wird eine Gefährdung mit „Beeinträchtigung körperlicher/persönlicher Unversehrtheit“ bezeichnet; in BSI 100-2 bzw. BSI 200-2 heißt das entsprechende Schadensszenario „Beeinträchtigung der persönlichen Unversehrtheit“.

So könnten alle Schadensfälle, die auf einer unrichtigen Identifizierung bzw. unrichtigen Zuordnung zu einer Identität beruhen, anhand ihrer jeweiligen Auswirkungen einer oder mehrerer anderen Gefährdungen zuordnet werden, was „Unrichtige Identifizierung oder Zuordnung zu einer Identität“ als separate Schadenskategorie überflüssig macht.

Darüber hinaus ist fraglich, inwieweit diese neue Gefährdung eine Relevanz für alle zu bewertenden Prozessschritte entfaltet. Für den Teilprozess der Identifizierung liegt die Bedeutung auf der Hand: Eine unrichtige Identifizierung ist das, was ausgeschlossen werden soll, und stellt damit die übergreifende Zusammenfassung aller hierbei möglichen Schadenskategorien dar. Für die Teilprozesse Willenserklärung und Daten- bzw. Dokumentenübermittlung sind jedoch keine Anwendungsfälle für diese Gefährdung ersichtlich. Für den Teilprozess Willenserklärung könnte eine denkbare Gefährdung „Beeinträchtige Dokumentenübermittlung“ eine analoge Funktion übernehmen – diese existiert aber nicht. Ebensowenig gibt es eine entsprechende Gefährdung für den Teilprozess Daten- bzw. Dokumentenübermittlung, da auch sie beide überflüssig wären.

Weitere Ausführung zur Bedeutung der Gefährdung/Schadenskategorie „Unrichtige Identifizierung oder Zuordnung zu einer Identität“ werden in der Handreichung des IT-Planungsrates nicht gegeben. Auch Anwendungsbeispiele fehlen, weshalb der konkrete Nutzen und die dafür beabsichtigte praktische Anwendung unklar bleiben. Auf die Frage nach einer Begründung für die Einführung dieser Gefährdung und einer Abgrenzung zu den anderen Gefährdungen antwortete das BSI, dass „eine ‚Unrichtige Identifizierung oder Zuordnung der Identität‘ [...] als eine Gefährdung betrachtet werden [kann], die gleich mehrere Gefährdungen gleichzeitig abdeckt (so führt ein solcher Fall höchstwahrscheinlich gleichzeitig zu finanziellen Auswirkungen, negativen Innen- und Außenwirkungen etc.) und so eine Kombination in den Fokus rückt“ (Felix Bleckmann, Referat DI 12, BSI, persönliche Kommunikation, 23.03.2022). Damit wird implizit die Kritik bestätigt, dass es sich im Grunde um eine Metakategorie ohne überzeugende eigene Daseinsberechtigung handelt. Auf die Bitte um praktische Beispiele wurde nicht eingegangen (vgl. Felix Bleckmann, Referat DI12, BSI, persönliche Kommunikation, 23.03.2022).

In der Praxis der Vertrauensniveaubewertung ist es sogar denkbar, dass die Schadenskategorie „Unrichtige Identifizierung oder Zuordnung zu einer Identität“ mehr schadet als nützt: Werden Schadensfälle nur unter dieser kombinierten Kategorie dokumentiert, so verlieren sie im Vergleich zu einer auf die anderen Gefährdungen verteilten Dokumentation an Gewicht. Lässt man sich bei der Gesamtbewertung durch die Anzahl der dokumentierten Gefährdungen leiten, könnte sie verzerrt werden.

5.5.2 Informationen zur Beziehung zwischen Schutzbedarf und Vertrauensniveau im Praxistool

Wie in Abschn. 5.4.2 erläutert, besteht der Fragenteil des Praxistools Vertrauensniveau aus zwei Abschnitten.

Der Zusammenhang zwischen diesen beiden Abschnitten, die Schutzbedarf und Vertrauensniveau einzeln behandeln, wird weder aus den einleitenden Erklärungen noch während der Benutzung des Praxistools klar. Erschwerend kommt hinzu, dass die Begriffe „Schutzbedarf“ und „Vertrauensniveau“ nicht konsequent verwendet werden: In den

einleitenden Erläuterungen des Praxistools heißt es, dass die Bewertung des Vertrauensniveaus im ersten Fragenabschnitt stattfinde, und im zweiten Fragenabschnitt „plausibilisiert“ – d. h. mit der Dokumentation konkreter Schadensfällen unterlegt – werde, während beim Ausfüllen des Praxistools nach Bewertung des Schutzbedarfs im ersten und Bewertung des Vertrauensniveaus im zweiten Fragenabschnitt getrennt wird.

Damit wird die Empfehlung der TR-03107-1 „die Feststellung des notwendigen Vertrauensniveaus auf Basis einer Schutzbedarfsfeststellung nach [BSI 200-2] unter zusätzlicher Berücksichtigung rechtlicher Vorgaben durchzuführen“ (TR-03107-1: S. 13) zwar umgesetzt, aber dem Nutzer nicht erläutert.

Weitere Erklärungen zum Verhältnis der beiden Konzepte und der Bedeutung des Schutzbedarfs für die Vertrauensniveaubewertung sucht man bei der Nutzung des Praxistools vergeblich. Zwar werden der Standard BSI 200-2 und seine Schutzbedarfskategorien kurz als Grundlagen des Praxistools erwähnt. Weder aus dem Namen des Praxistools noch den einleitenden Erklärungen lässt sich jedoch entnehmen, dass eine Schutzbedarfsfeststellung im Rahmen der Vertrauensniveaubestimmung überhaupt relevant ist. Der Nutzer erfährt dies erst bei Beantwortung der ersten Fragen.

Gerade weil sich das Praxistool ausdrücklich auch an Nutzer ohne Vorkenntnisse zum Vertrauensniveau und ohne Erfahrung im Bereich Datenschutz und Informationssicherheit richtet, ist dieser Mangel an Erläuterungen potenziell problematisch (siehe Abschn. 5.5.7).

5.5.3 Verfahren im Praxistool

Der Nutzer des Praxistools wird im ersten Fragenabschnitt dazu aufgefordert Bewertungen zum Schutzbedarf der einzelnen Prozessschritte eines Online-Antragsverfahren abzugeben. Um die gestellten Fragen zu beantworten müssen potenzielle Schäden bezüglich ihrer Höhe und Eintrittswahrscheinlichkeit bewertet werden. Im zweiten Fragenabschnitt werden anschließend mit höherem Detaillierungsgrad Fragen gestellt, die sich im Wesentlichen nicht von denen des ersten Fragenabschnitts unterscheiden (vgl. Anh. 1–4). Ohne, dass sich der Nutzer die Fragen des zweiten Fragenabschnitts bereits selbst gestellt hat und die Antworten darauf kennt, ist es nicht möglich, die Fragen des ersten Fragenabschnitts korrekt zu beantworten.

Natürlich ist es möglich, eine Bewertung im ersten Fragenabschnitt anzupassen, falls sich ein Nutzer bei der Bearbeitung des zweiten Fragenabschnitts einer neuer Gefährdung bewusst wird und zu einer anderen Bewertung kommt. Der Aufwand, den eine solche Änderung mit sich bringt, ist ebenso unnötig, wie der Aufwand, dieselben Gefährdungen, Schadenshöhen und Risiken doppelt zu identifizieren und bewerten.

Die einleitenden Erläuterungen zum Praxistool räumen diese Doppelung sogar ein – mit dem Hinweis, dass die Bewertung aus dem ersten Fragenabschnitt im zweiten Fragenabschnitt „plausibilisier[t]“ wird. Die Sinnhaftigkeit dieses Vorgehen ist trotzdem fragwürdig.

5.5.4 Verfahren in der Handreichung des IT-Planungsrates

Die Teilung in zwei Fragenabschnitte im Praxistool beruht möglicherweise auf der zweischrittigen Vertrauensniveaubewertung aus der Handreichung des IT-Planungsrates. Das dort empfohlene Verfahren ist gleichermaßen umständlich, da es auch eine zweimalige Durchführung der Bewertung vorsieht. Hierbei ist noch problematisch, dass im ersten Schritt das Vertrauensniveau anhand der „abstrakte Eintrittswahrscheinlichkeiten“ (IT-Planungsrat 2020: S. 9) möglicher Gefährdungen bewertet werden soll, ohne das erklärt wird, worum es sich bei einer solchen abstrakten Eintrittswahrscheinlichkeit handelt und wie man sie feststellt. Die Erläuterungen zur Vorgehensweise bei der Auf- bzw. Abwertung des vorher bestimmten Vertrauensniveaus kontrastieren konkrete Eintrittswahrscheinlichkeiten scheinbar damit, Eintrittswahrscheinlichkeiten überhaupt nicht zu berücksichtigen, und zur Bewertung nur die Schadenshöhe heranzuziehen (vgl. IT-Planungsrat 2020: S. 11). Was genau gemeint ist, bleibt aber unklar.

Im zweiten Schritt der Vertrauensniveaubewertung wird dann ausschließlich auf die bereits vorhandenen Erfahrungen aus der Verwaltung abgestellt; noch nicht konkret erlebte, aber vorstellbare Schadensfälle bleiben ohne Beachtung.[36] Da zum Zeitpunkt der Vertrauensniveaubestimmung im Rahmen der Digitalisierung einer Verwaltungsleistung noch keine Erfahrungen zum Onlinebetrieb eben dieser Leistung vorliegen können, ist zu bezweifeln, inwieweit bei diesem Vorgehen die relevanten Schadensfälle betrachtet werden.

5.5.5 Fragenauswahl im Praxistool

Eine weitere Unzulänglichkeit im Praxistool, die weniger problematisch, aber trotzdem erwähnenswert ist, betrifft die Auswahl der gestellten Fragen. Bei den letzten beiden Prozessschritten werden jeweils in einer einzelnen Fragen die potenziellen Gefährdungen für den Antragsteller und die verarbeitende Stelle abgefragt. Für den Prozessschritt „Absenden des Formulars“ ist dies nicht der Fall: Hier gibt es nur eine allgemeine Frage zu möglichen Schäden, wobei die vorgegebenen Antworten deutlich machen, dass eigentlich nur auf Schäden für den Antragsteller abgestellt wird. Ein Grund für eine solche Einschränkung der Betrachtung ist nicht ersichtlich, da sich aus einer falschen Identifizierung auch Schäden für die verarbeitende Stelle ergeben können.

5.5.6 Bewertung und Ergebnisse im Praxistool

Wie bereits erwähnt (siehe Abschn. 5.4.2.1), kann der Nutzer im ersten Fragenabschnitt des Praxistools seine Antworten aus jeweils nur zwei Alternativen wählen. In den meisten Fällen wird dafür das Spektrum der möglichen Antworten auf zwei gegenüberliegende, teilweise praxisferne Extreme reduziert. Beispielsweise kann man sich bezüglich des Anreizes für einen Dritten, einen Prozess zu manipulieren, nur zwischen einer „sehr geringen

[36] Möglicherweise sind es diese noch nicht konkret aufgetretenen Schadensfälle die die Grundlage für die abstrakte Vertrauensniveaubewertung aus dem ersten Schritt bilden, doch aufgrund fehlender Informationen bleibt dies nur eine Mutmaßung.

Eintrittswahrscheinlichkeit“ und einem Prozess, der „scheinbar prädestiniert für Identitätsmissbrauch“ ist, entscheiden (BMI 2021e). Weitere Abstufungen würden den Prozess der Ergebnisermittlung natürlich verkomplizieren, aber aller Wahrscheinlichkeit nach auch die Genauigkeit des Ergebnisses erhöhen.

Im zweiten Fragenabschnitt werden die auf Basis der Schutzbedarfe ermittelten Vertrauensniveaus angezeigt. Da hierbei keine Unterscheidung zwischen den Vertrauensniveaus „substanziell“ und „hoch“ möglich ist, kann die Belastbarkeit dieser vom Schutzbedarf in Vertrauensniveaus übertragenen Bewertungen angezweifelt werden. Die Vertrauensniveaus „substanziell“ und „hoch“ korrespondieren beide mit dem Schutzbedarf „hoch“ (vgl. Tab. 3 auf S. 36), und da die Bewertung des Vertrauensniveaus, das in diesem Fragenabschnitt ausgegeben wird, ausschließlich auf dem ermittelten Schutzbedarf beruht, kann – gänzlich ungeachtet jedweder individueller Antworten in diesem Teil – in keinem Fall ein Ergebnis über „mindestens substanziell“ erreicht werden.

Zwar wird das Vertrauensniveau unabhängig vom Schutzbedarf ermittelt, jedoch wird der Nutzer aufgefordert, seine Dokumentation von Schadenskategorie, Schadenshöhe und Eintrittswahrscheinlichkeit auf das Vertrauensniveau zu stützen, was aus der Schutzbedarfsfeststellung abgeleitet wurde. So heißt es bei der Bewertung eines Prozesses beispielsweise: „Bitte bewerten Sie für Ihr bisher ermitteltes Vertrauensniveau „NIEDRIG“ mindestens einen möglichen Schadensfall mit Schadenskategorie, Schadenshöhe und Eintrittswahrscheinlichkeit (gemäß TR-03107-1) und dokumentieren Sie Ihre fachlichen Gründe aus Ihrer Verwaltungspraxis.“ Es liegt also nahe, dass sich die Nutzer bei seiner Einschätzung an dem bereits vorgegebenen Ergebnis, was zudem fett und in Großbuchstaben prominent angezeigt wird, orientiert.

Besonders problematisch kann dies bei den Prozessen Willenserklärung und Daten-/Dokumentenübermittlung werden: Die Vertrauensniveaubewertung dieser beiden Prozesse beruht auf der Schutzbedarfsfeststellung mehrerer Prozessschritte (vgl. Abb. 10). Dabei werden aber mehrere Schutzbedarfsfeststellungen von „hoch“ nicht zu einem Vertrauensniveau von „hoch“ kumuliert, sondern weiter als „mindestens substanziell“ geführt. Wird der Nutzer bei der Vertrauensniveaubewertung von dem schon vorgegeben Ergebnis beeinflusst, kann das zu einer Fehlbewertung führen. Besonders da es nicht direkt ersichtlich ist, in welchem Zusammenhang die Bewertungen aus dem ersten und dem zweiten Fragenabschnitt stehen, bleibt es fraglich, ob der durchschnittliche Nutzer die Zusammenhänge überblickt und die entsprechenden Anpassungen der Bewertung vornimmt.

Auch werden die Eingaben, die zur Untermauerung der Schutzbedarfsfeststellung aus dem ersten Fragenabschnitt gemacht werden, nicht auf ihre Plausibilität überprüft. Die Möglichkeit, hier zu einer abweichenden Bewertung zu kommen, ist zunächst zu begrüßen, da dadurch eine tatsächliche Prüfung der Ergebnisse der Schutzbedarfsfeststellung ermöglicht wird. Dass es jedoch ohne Probleme möglich ist, auch bei einem Schutzbedarf „hoch“ bzw. Vertrauensniveau „mindestens substanziell“ für alle Prozessschritte aus dem ersten Fragenabschnitt eine Vertrauensniveaubewertung von „niedrig“ im zweiten Fragenabschnitt vorzunehmen, erscheint problematisch. In solch einem Fall muss es in mindestens einem der Fragenteile zu einer Fehlbewertung gekommen sein.

Das Praxistool gibt, wie oben erläutert (siehe Abschn. 5.4.2.3), nach Abschluss des Fragenteils eine Übersicht der Ergebnisse aus, und es wird auch darauf hingewiesen, dass es sich anbietet, sich bei der Gesamtbewertung am höchsten ermittelten Vertrauensniveau zu orientieren. Was unklar bleibt, ist, wieso auf der – durch die Vielzahl der Bewertungen recht unübersichtlichen – Ergebnisseite, nicht das maximale Vertrauensniveau als Gesamtergebnis vorschlagen wird.

5.5.7 Empfehlung zu Zuständigkeiten im Praxistool

Obwohl die Handreichung des IT-Planungsrats ausdrücklich empfiehlt, die Beauftragten für IT-Sicherheit und für Datenschutz bei der Vertrauensniveaubestimmung zu beteiligen (IT-Planungsrat 2020: S. 5 f.), richtet sich das Praxistool nur „an Fachexperten der zuständigen Behörden“, denen damit die eigenständige Erarbeitung einer Empfehlung ermöglicht werden soll (BMI 2021e). Ausdrücklich werden „Hintergrundkenntnisse zum Datenschutz, zum Vertrauensniveau und zur Informationssicherheit“ zur Nutzung zwar als wünschenswert, jedoch nicht als erforderlich angesehen (BMI 2021e).

Diese Herangehensweise, in der die Fachverantwortlichen möglicherweise ohne jegliche weitere Kenntnisse eine Bewertung des erforderlichen Vertrauensniveaus erarbeiten, widerspricht nicht nur den Empfehlungen des IT-Planungsrats, sondern erscheint auch weder praktikabel noch zielführend. Eine Identifikation der Gefährdungen mag ausschließlich basierend auf Wissen aus der Verwaltungspraxis noch möglich sein, aber bei der Bewertung dieser Gefährdungen hinsichtlich Schadenshöhe und Eintrittswahrscheinlichkeit scheinen Kenntnisse im Bereich Informationssicherheit und Datenschutz unabdingbar. Auch ein Überblick über die Einordnung der zu bewertenden Leistung in den Rahmen der Informationssicherheit und des Datenschutzes in der gesamten Organisation ist für eine realistische Risikobewertung nötig.

Es besteht damit die Möglichkeit, dass Nutzer ohne entsprechende Erfahrung Gefährdungen verkennen bzw. Risiken zu niedrig einschätzen, was zur Umsetzung von OZG-Leistungen auf einem zu niedrigen Vertrauensniveau führen kann. Mit einer unzureichend abgesicherten Online-Leistung stünde die betroffene Behörde damit für Gefährdungen offen. Ebenfalls ist es möglich, dass Risiken von Fachexperten, die mit den speziellen Anforderungen an die Digitalisierung von Leistungen noch nicht weiter vertraut sind, als zu hoch eingeschätzt werden (vgl. Bericht aus der praktischen Erfahrung von Cornelia Pflüger, Projektleitung Serviceportal Amt 24, Hauptamt, Stadt Leipzig, persönliche Kommunikation, 15.02.2022). Werden die Zugangsvoraussetzung zu einer Online-Verwaltungsleistung damit in der Folge als zu hoch angesetzt, ist sie möglicherweise weniger attraktiv für die Nutzer (siehe auch Abschn. 5.6.3). Die abweichende Empfehlung bezüglich der Zuständigkeit bei der Vertrauensniveaubewertung ist daher kritisch zu sehen.

5.5.8 Fehlende Aktualisierung und Verbesserung des Praxistool

Seit Mitte März 2022 ist das Praxistool Vertrauensniveau ausschließlich in der Version „Stand, [sic!] 17.06.2021“ verfügbar. Vorher gelangte der Nutzer regulär zur Version „Stand, [sic!] 22.04.2020, 8:00 Uhr“ – bei direktem Aufruf der Startseite war aber auch

eine Auswahl der neueren Version möglich. Wieso erst im Jahr 2022 endgültig von einer Version von 2020 auf eine von 2021 gewechselt wurde, ist unklar, vor allem, da die neue Version keine signifikanten Änderungen beinhaltet. Weder die kleinen Darstellungsfehler, die Dopplung einer Frage noch die vorhandenen Rechtschreibfehler wurden in der neuen Version behoben.[37]

Eine inhaltliche Änderung in der neuen Version besteht in der Verschiebung und leichten Abänderung der Frage zur Schriftformerfordernis aus dem Fragenabschnitt zum Schutzbedarf beim Absenden des Formulars in den Fragenabschnitt zum Vertrauensniveaus der Willenserklärung. Methodisch ergibt diese Platzierung mehr Sinn, und es wird dadurch auch eine bessere Passung von Einleitungstext, der in einem Hinweis die Relevanz dieser Frage für die Abgabe der Willenserklärung erläutert, und Fragenplatzierung im Praxistool selbst erreicht. Eine andere Änderung in der neuen Version betrifft eine leichte Erweiterung der Darstellung der Ergebnisse: die Fragen und Antworten zum Schutzbedarf erscheinen nun nach der Aktivierung von Toggle-Buttons in Ausklappmenüs (siehe Anh. 5 und 6). Ansonsten wurden nur leichte sprachliche Anpassungen vorgenommen.[38]

5.5.9 Abschließende Betrachtungen

Vor dem Hintergrund, dass die Handreichung des IT-Planungsrates aktuell überarbeitet wird, ist jede Kritik an ihrem Inhalt mit der Veröffentlichung der neuen Version vielleicht sowieso hinfällig. Vor allem, da die Handreichung auch nicht mehr zur Anwendung empfohlen wird (vgl. Inga Greiner-Bild, Referat DV 3 – Bundesportal; Portalverbund; Geschäfts- und Koordinierungsstelle 115, BMI, persönliche Kommunikation, 06.01.2022), kann man davon ausgehen, kann man davon ausgehen, dass die neue Version signifikanten Änderungen wird.

Der Großteil der hier angebrachten Kritikpunkte bezieht sich jedoch auf die TR-03107-1 und das Praxistool Vertrauensniveau, die verbindlich zu beachten sind bzw. das weiterhin aktiv beworben wird, und haben damit Bestand.

Obwohl die Probleme des Praxistool für die Vertrauensniveaubewertung in der Praxis signifikanter sind, kann auch die überflüssige Schadenskategorie (siehe Abschn. 5.5.1) negative Auswirkungen haben.

Ob im Zuge der Überarbeitung der Empfehlungen des IT-Planungsrates zur Vertrauensniveaubestimmung eine grundlegende Änderung des Praxistools geplant ist, bleibt unklar. Auf Anfrage wurde nur die Auskunft gegeben wurde, dass eine Aktualisierung zur inhaltlichen Anpassung an die aktualisierten Empfehlungen bzw. die „technischen BSI-Richtlinien“ geplant sei (Daniel Obst,]init[AG, persönliche Kommunikation, 02.03.2022). Nutzungsdaten zum Praxistool, abgesehen von der Gesamtzahl der Aufrufe, würden nicht erhoben; auch werde kein Feedback zur Nutzung von der Zielgruppe eingeholt und ausgewertet (vgl. Daniel Obst,]init[AG, persönliche Kommunikation, 02.03.2022).

[37] Im Abschnitt mit den Fragen zum Erhalt der Leistung erscheint beispielsweise der Container mit der zusätzlichen Frage zur Eintrittswahrscheinlichkeit weiterhin nicht unter der vorherigen Frage am Ende der Liste, sondern oben über allen anderen Fragen.

[38] Beispielsweise wurde „Welche Gefährdungen/Schadenskategorien könnten in der Verwaltungspraxis bzw. bei der Digitalisierung relevant werden?“ geändert in „Wählen Sie bitte die Gefährdungen/Schadenskategorien, die für Sie aus Ihre Verwaltungspraxis bzw. bei der Digitalisierung relevant werden.“

Insgesamt drängt sich damit der Eindruck auf, dass nicht zielgerichtet und sorgfältig an der Verbesserung des Praxistools gearbeitet wird. Vor dem Hintergrund, dass durchaus Optimierungspotenzial besteht und das Praxistool auch aktuell die einzige verfügbare Ressource zur Vertrauensniveaubestimmmung darstellt, ist das nicht nur bedauerlich, sondern potenziell auch problematisch.

5.6 Empfehlungen für die Festlegung von Vertrauensniveaus

Die Empfehlungen des IT-Planungsrates zur Vertrauensniveaufestlegung (IT-Planungsrat 2020), die auf der TR-03107-1 basieren, bleiben zwar Empfehlungen, eine Beachtung erscheint vor dem Hintergrund der zwischenzeitlich eingetretenen Verbindlichkeit der Richtlinie aber ratsam; auch wurde die Verwendung Empfehlungen des IT-Planungsrates von Anfang an überall empfohlen (vgl. BT-Drs. 18/10183: S. 65).

Die über die Empfehlungen des IT-Planungsrats hinaus existierenden Quellen mit Empfehlungen zur Vertrauensniveaubestimmung sind weder zahlreich noch inhaltlich ausführlich. Im Folgenden sind die aus der Literatur zu gewinnenden Erkenntnisse zusammengetragen und mit Informationen zu deren praktischer Umsetzung unterlegt.

5.6.1 Technikunabhängige Festlegung

Zunächst ist zu beachten, dass nur das Vertrauensniveau, nicht aber der Vertrauensmechanismus festgelegt werden sollten (vgl. IT-Planungsrat 2020: S. 4; siehe Abschn. 4.3). Damit wird sichergestellt, dass die technische Umsetzung ständig dem Stand der Technik entsprechen kann (vgl. IT-Planungsrat 2020: S. 4).

Auch wenn die Information über die Festlegung von anderen nachgenutzt werden soll, ist Technikunabhängigkeit von Bedeutung. Wird der Vertrauensmechanismus festgelegt, besteht das Risiko, dass die Vorgabe in anderen Nutzerkonten nicht umgesetzt werden kann (IT-Planungsrat 2020: S. 4).

5.6.2 Einheitlichkeit für vergleichbare Leistungen

Es bestehen keine gesetzlichen Regelungen, die Vertrauensniveaus für Verwaltungsleistungen einheitlich festlegen (Herrmann/Stöber 2017: S. 1405). Stattdessen wird das Vertrauensniveau in jeder Behörde einzeln vom Fachverantwortlichen für die jeweilige Online-Leistungen festgelegt (IT-Planungsrat 2020: S. 3, 5). Da die Festlegung auf einer Abwägung verschiedener Faktoren beruht, kann es hierbei natürlich leicht zu Abweichungen kommen (siehe unten). Alle Quellen, die sich zu diesem Thema äußern, empfehlen bzw. fordern jedoch eine bundesweit einheitliche Festlegung der Vertrauensniveaus; Abweichungen bei vergleichbaren Verwaltungsleistungen werden als „hinderlich“ eingestuft (AG „Attraktivität des E-Government“ 2015: S. 5, 13; vgl. Fromm/Welzel/Nentwig/Mike Weber u. a. 2015: S. 58; Herrmann/Stöber 2017: S. 1405; IT-Planungsrat 2020: S. 5). Zur Erreichung dieses Ziels erklärte der IT-Planungsrat bereits im Jahr 2020, weiterführende Empfehlungen zu entwickeln (IT-Planungsrat 2020: S. 3, 5). Entsprechende Ergebnisse sind jedoch bisher nicht veröffentlicht worden.

Schon im Jahr 2015 wurden konkrete Vorschläge für eine einheitliche Festlegung der Vertrauensniveaus gemacht: im Rahmen des FIM-Projekts oder im LeiKa sollten einmal ermittelte Vertrauensniveaus hinterlegt und damit anderen Verwendern zur Verfügung gestellt werden (vgl. AG „Attraktivität des E-Government“ 2015: S. 24; Fromm/Welzel/Nentwig/Mike Weber u. a. 2015: S. 58). Als Ziel wurde genannt, bis 2018 für alle Verwaltungsleistungen eine Empfehlungen für das passende Vertrauensniveau zu erarbeiten, abzustimmen und im LeiKa zu dokumentieren (vgl. AG „Attraktivität des E-Government“ 2015: S. 24). Von einer einheitlichen Festlegung versprach man sich erhöhte Rechtssicherheit und Erleichterungen bei der Bereitstellung von Online-Verwaltungsleistungen, auch wenn man sich der eventuellen Nachteile dieses Vorgehens durch langwierige Abstimmungsprozesse bewusst war (vgl. Fromm/Welzel/Nentwig/Mike Weber u. a. 2015: S. 58).

Eine Recherche im FIM-Portal (FITKO 2022c) ergibt, dass aktuell unter den über 8.000 Leistungen des LeiKa nur 18 mit einer Angabe zum Vertrauensniveau im Steckbrief hinterlegt sind. Dabei handelt es sich ausschließlich um Typ-1- und Typ-2/3-Leistungen, weshalb die vorhandenen Informationen für die kommunale Ebene nur von geringer Bedeutung sind (siehe Anh. 7 für eine Übersicht). Die aktuelle Situation macht deutlich, dass den Empfehlungen aus AG „Attraktivität des E-Government“ (2015) und Fromm/Welzel/Nentwig/Mike Weber u. a. (2015) nicht gefolgt wurde.

Dass es ungeachtet der Bestrebungen zur Einheitlichkeit bei der Vertrauensniveaubewertung zu Abweichungen kommen kann, wurde bereits erwähnt. Dieser Umstand ergibt sich notwendigerweise aus den zahlreichen Abwägungen, die bei der Entscheidung in individueller Zuständigkeit von den Fachverantwortlichen getätigt werden müssen (siehe auch Abschn.5.3 und 5.4.2). Zur Vermeidung von Divergenzen wird eine Abstimmung mit den Fachkollegen in den Ländern empfohlen (vgl. IT-Planungsrat 2020: S. 5). Zusätzlich wurde im Jahr 2020 die Möglichkeit der Verschiebung der Festlegungszuständigkeit angekündigt (vgl. IT-Planungsrat 2020: S. 5). Bisher wurde keine weitere Pläne in diese Richtung veröffentlicht und sie erscheinen vor dem Hintergrund der kommunalen Selbstverwaltungsgarantie auch nicht für alle Leistungstypen umsetzbar.

Ein Blick in die Praxis zeigt, dass es teilweise zu stark abweichenden Vertrauensniveaubewertungen kommt. Breiter angelegte Untersuchungen zu den kommunal festgelegten Vertrauensniveaus scheint es aktuell (noch) nicht zu geben, eine Kurzstudie des NEGZ stellt aber beispielhaft die unterschiedlichen Umsetzungen zweier Leistungen gegenüber. Für eine Urkundenbestellung beim Standesamt reicht in Düsseldorf ein Antrag ohne Registrierung aus, während man sich in Schleswig-Holstein und Köln mit eID authentisieren muss (NEGZ 2019: S. 13).[39] Auch für die zweite untersuchte Leistung kommen ganz unterschiedliche Möglichkeiten zum Einsatz: Eine einfache Melderegisterauskunft ist in Köln ohne Registrierung möglich, während man in Schleswig-Holstein ein Servicekonto mit Benutzername und E-Mail benötigt und in Hamburg gar eine Authentisierung mit eID nötig ist (NEGZ 2019: S. 13).

Unklar ist, woraus sich diese Unterschiede ergeben. Die Studie gibt hierüber für die untersuchten Fälle keine Auskunft; auch inwieweit es sich tatsächlich um vergleichbare Verwaltungsleistungen handelt, bleibt unklar.

[39] Eine Überprüfung der Ergebnisse der Studie ergab, dass sich drei Jahre später nichts an der Situation geändert hat.

Für solche abweichenden Vertrauensniveaubewertung für auf den ersten Blick vergleichbare Leistungen lassen sich leicht weitere Beispiele finden: In der Stadt Leipzig muss man sich für die Beantragung eines Besucherparkausweises mit eID authentisieren (vgl. Stadt Leipzig 2022b), während in Bremen eine Anmeldung mit Benutzername und Passwort ausreicht (vgl. Bremen 2022). Bei beiden beantragten Leistungen handelt es sich um eine Parkerlaubnis für Gäste der Bewohner von Bewohnerparkbereichen in einer Großstadt mit knapp 600.000 Einwohnern, was zunächst eine Vergleichbarkeit suggeriert.

Wie die Vergleichbarkeit von Verwaltungsleistungen tatsächlich definiert oder beurteilt werden soll, wird bei den bisher publizierten Überlegungen zur einheitlichen Festlegung von Vertrauensniveaus nicht thematisiert. Gerade im Bereich der Typ-5-Leistungen ist damit zu rechnen, dass es zahlreiche ähnliche Leistungen gibt, die aber aufgrund von lokalen Besonderheiten möglicherweise nicht vollständig gleichartig bzw. vergleichbar sind.

In der Stadt Leipzig werden zum Beispiel Besuchern, die ihren Hauptwohnsitz im Umland haben, keine Besucherparkausweise erteilt, was zu erweiterten Nachweispflichten führt (vgl. Stadt Leipzig 2022b); in Bremen ist nicht der Fall (vgl. Bremen 2022). Ob damit eine Vergleichbarkeit dieser Leistungen ausgeschlossen ist, hängt von den noch zu definierenden Vergleichskriterien ab.

Wird die angestrebte Einheitlichkeit bei der Vertrauensniveaufestlegung wie oben beschrieben durch die Nachnutzung einmal festgelegter Vertrauensniveaus umgesetzt, so müsste für jede Verwaltungsleistung zunächst anhand dieser Vergleichskriterien geprüft werden, ob sich unter den bereits mit einer Vertrauensniveauzuordnung versehenen Verwaltungsleistungen eine gleichartige befindet. Ist dies der Fall, kann die Vertrauensniveaubewertung übernommen werden. Ist dies nicht der Fall – was bei der Vielfalt der Ausprägungen der Leistungen und der bei der Vertrauensniveaubewertung zu betrachtenden Umstände wahrscheinlich ist – muss doch eine eigene Vertrauensniveaufestlegung durchgeführt werden.

Vielversprechender im Sinne der Zielerreichung scheint es, striktere Vorgaben zu machen, wie es bereits vom IT-Planungsrat angekündigt wurde (siehe oben). Verbindlichere, insbesondere detailliertere, Vorgaben würden bei konsequenter Anwendung ebenfalls zu einer einheitlicheren Vertrauensniveaufestlegung führen, wenngleich es angesichts der Vielfalt der Verwaltungsleistung schwierig werden dürfte, alle Fälle zu erfassen.

5.6.3 Auswahl des niedrigstmöglichen Vertrauensniveaus

In seinem Bericht zur Attraktivität des E-Government, der mehrere Umfragen und Studien zu dem Thema zusammenfasst, nannte der IT-Planungsrat schon 2015 den niederschwelligen Zugang zu als eines der Erfolgskriterien für funktionierendes, von den Bürgern akzeptiertes E-Government (vgl. AG „Attraktivität des E-Government“ 2015: S. 4, 13, 18). Zur Akzeptanzsteigerung sollte daher für eine Verwaltungsleistung das niedrigste Vertrauensniveau ausgewählt werden, was die notwendigen Anforderungen noch erfüllt (vgl. AG „Attraktivität des E-Government“ 2015: S. 13).

Obwohl diese Einschätzung inzwischen bereits einige Jahre alt ist und die gestiegenen Nutzungszahlen der eID[40] einen Fortschritt bei der Akzeptanz dieser Technologie vermuten lassen, gibt es keinen Anlass, anzunehmen, dass das zugrundeliegende Prinzip keine Gültigkeit mehr hat.

Das NEGZ empfiehlt ebenfalls eine „nutzerorientiert[e] und realistisch[e]“ Festlegung des Vertrauensniveaus (NEGZ 2019: S. 5). Auch in der Handreichung des IT-Planungsrats wird die Ansicht geäußert, dass ein zu hoch bewertetes Vertrauensniveau negative Auswirkungen auf die Nutzung des Online-Dienstes haben könnte (vgl. IT-Planungsrat 2020: S. 8).

Ein Beispiel aus der Praxis: In Bremen, wo im Jahr 2021 116 Verwaltungsleistungen online angeboten wurden, wurde „nur eine davon von [...] zwei Dritteln der Bürgerinnen und Bürger wirklich digital genutzt“ – nämlich das Bewohnerparken, was auf dem niedrigsten Vertrauensniveau umgesetzt ist (Schüür-Langkau 2021: S. 24).

Der Deutsche Industrie- und Handelskammertag forderte im Jahr 2019 gar die grundsätzliche Vermeidung des Vertrauensniveaus „hoch“ für unternehmensbezogene Anwendungen und bewertete das Vertrauensniveau „substanziell“ als „in der Regel ausreichend“ (Sobania 2019: S. 10). Ein Begründung für diese Einschätzung wird nicht gegeben – für das Unternehmenskonto werden aber bisher nur ELSTER-Zertifikate zur Identifizierung und Authentifizierung angeboten, was die Nutzung eines Vertrauensniveau über „substanziell“ in der Praxis sowieso weiterhin unmöglich macht (vgl. BMI 2021b; BMI 2021h: S. 9).

Insgesamt ist festzuhalten, dass außer der Sicherheit auch noch die Faktoren der praktischen Umsetzbarkeit und der Nutzerfreundlichkeit beachtet werden sollten. Nicht nur wegen Bedenken bezüglich der Akzeptanz des einzusetzenden Identifizierungs- und Authentifizierungsverfahrens, sondern auch bei Nichtverfügbarkeit eines implementierten Vertrauensmechanismus auf einem bestimmten Vertrauensniveau sollte man daher die Möglichkeit prüfen, auf ein niedrigeres Vertrauensniveau zurückzugreifen.

[40] Das OZG-Dashboard weist zwar fast kontinuierlich steigende Zahlen für erfolgreiche eID-Transaktionen aus; mit dem Rekordwert von rund 400.000 Transaktionen im Januar 2022 kann aber noch nicht von einem flächendeckenden Einsatz die Rede sein (vgl. BMI 2022a).

6 Empfehlungen für die Festlegung von Vertrauensniveaus für OZG-Leistungen der Stadt Leipzig

Die eIDAS-VO und die TR-03107-1 bilden als verbindliche Vorgaben die Grundlage der Vertrauensniveaubestimmung (siehe Abschn. 5.1). Basierend auf den Erkenntnissen aus der Literatur und der Analyse des Praxistools Vertrauensniveau sowie den kritischen Überlegungen dazu werden im Folgenden weitere Empfehlungen für die Vertrauensniveaubestimmung für online auf Amt24 umzusetzende Verwaltungsleistungen der Stadt Leipzig gegeben.

Zur Erleichterung der Vertrauensniveaubestimmung wurde zudem eine Arbeitshilfe erarbeitet. Dabei handelt es sich um ein modular aufgebautes, erweiterbares Excel-Dokument, das mit Hinweisen und interaktiven Funktionen bei der Dokumentation im Rahmen der Vertrauensniveaubestimmung unterstützt. Die Details lassen sich der Arbeitshilfe selbst entnehmen (siehe Anh. 8).

Die nachfolgenden Empfehlungen sowie der Inhalt und Aufbau der Arbeitshilfe resultieren teilweise auch aus den praktischen Erfahrungen mit der Vertrauensniveaubestimmung. Beispiele dazu finden sich in Kap. 7 bzw. in den Anh. 9–11.

6.1 Festlegung tolerierbarer Schadenshöhen

Zunächst sollten die für eine möglichst genaue Vertrauensniveaubestimmung nötigen Grundlagen geschaffen werden. Im Detail bedeutet dies, dass für jede Schadenshöhe eine (grobe) Festlegung der maximal tolerierbaren Schäden nötig ist. Analog zu den Bewertungen des Schutzbedarfs in BSI (2022a) sollten Schadensbeträge (und ggf. Ausfallzeiten) festgelegt werden, die mit den Bewertungen „niedrig“, „substanziell“ und „hoch“ korrespondieren. Dazu ist eine vergleichende Gesamtsicht auf die Institution nötig, die auf der Ebene desjenigen Fachamts, in dem die konkrete Vertrauensniveaubewertung stattfindet, in der Regel fehlt. Daher sollten diese Informationen zentral zur Verfügung gestellt werden.

6.2 Bewertungsverfahren

6.2.1 Vereinfachte Vorgehensweise

Aufgrund der in den Abschn. 5.5.3 und 5.5.4 geäußerten Kritik wird ein vereinfachtes Verfahren zur Vertrauensniveaubestimmung vorgeschlagen. Für die praktische Durchführung wird die Nutzung der Arbeitshilfe in Anh. 8 empfohlen.

Zu Beginn wird das Vorliegen eines Schriftformerfordernis geprüft. Danach erfolgt die Bewertung wie in TR-03107-1 anhand der drei Prozesse Identifizierung, Willenserklärung und Daten-/Dokumentenübermittlung.

Vor jeder Teilprüfung ist es nötig, sich die Details des zu bewertenden Prozessschrittes bewusst zu machen. Dazu dienen einige Fragen, die zu den relevanten Überlegungen anregen. Auch die maximal tolerierbaren Schäden für die drei Abstufungen der Schadenshöhe sollten bekannt sein (siehe Abschn. 6.1). Danach werden für die entsprechenden

Gefährdungen mögliche Schadensfälle, Schadenshöhen und Eintrittswahrscheinlichkeiten dokumentiert.

Von der automatischen Bildung eines Gesamtergebnisses wird in der Arbeitshilfe absichtlich abgesehen, da es sich um eine komplexe Abwägung handelt, die mit den simplen Skalen, die die bestehenden Vorgaben bereitstellen, nur unzureichend abgebildet werden kann. Die Vorgaben müssten erheblich (und damit wahrscheinlich prohibitiv) viel detaillierter sein, um eine aussagekräftige automatische Bewertung zu ermöglichen.

Statt die Gesamtbewertung mit einem ungenau errechneten Ergebnis zu beeinflussen, sollte der Bewertende daher basierend auf den dokumentierten Gefährdungen und seinen Einschätzungen dazu selbst zu einer Bewertung gelangen (siehe auch Abschn. 6.3.3 und Beispiele dazu in Anh. 9–11).

6.2.2 Auswahl der Gefährdungen

Für die Arbeitshilfe in Anh. 8 wurden die Gefährdungen/Schadenskategorien von den Schadensszenarien der aktuellen Version der IT-Grundschutz-Methodik (vgl. BSI 200-2: S. 105) übernommen.

Die Gefährdung „Unrichtige Identifizierung oder Zuordnung zu einer Identität“ wurde aufgrund der verpflichtenden Anwendung der TR-03107-1 (siehe Abschn. 5.1) in die Arbeitshilfe in Anh. 8 hier der vollständogen Wiedergabe halber zwar aufgenommen, wird aber wegen der in Abschn. 5.5.1 geäußerten Bedenken nicht zur Benutzung empfohlen. Für die praktische Arbeit bietet es sich an, diese Schadenskategorie beim Ausfüllen unbeachtet zu lassen oder aus der Arbeitshilfe zu löschen.

6.2.3 Umfassende Betrachtung und ausführliche Dokumentation

Bei der Vertrauensniveaubewertung sollten alle denkbaren Schadensfälle dokumentiert werden, selbst wenn die Verwaltungspraxis zunächst eine sehr geringe Eintrittswahrscheinlichkeit nahelegt. So stellt man sicher, dass die iterative Erarbeitung des Vertrauensniveaus effektiv durchgeführt werden kann (siehe Abschn. 6.2.4).

Für die identifizierten Gefährdungen sollten alle Schadensfälle möglichst genau beschrieben werden. Die Einschätzungen für Schadenshöhe und Eintrittswahrscheinlichkeit sollten nachvollziehbar begründet werden. Diese ausführliche Dokumentation ist für die akkurate Vertrauensniveaubestimmung nützlich und wirkt unreflektierten Bewertungen entgegen.

Eine umfassende Betrachtung aller Gefährdungen mit ausführlicher Dokumentation ist in der Folge auch für die regelmäßige erneute Kontrolle der Vertrauensniveaubewertung nützlich: Anhand bereits dokumentierter Schadensfälle kann leichter geprüft werden, ob sich Schadenshöhe oder Eintrittswahrscheinlichkeit inzwischen geändert haben und daher eine Anpassung des im Gesamtergebnis ermittelten Vertrauensniveaus nötig wird (siehe Abschn. 6.3.1).

6.2.4 Iterativer Prozess

In Anlehnung an das Vorgehen bei der Schutzbedarfsfeststellung (vgl. BSI 200-2: S. 109 f.) wird die Vertrauensniveaubestimmung in einem iterativen Prozess empfohlen. Bei der ersten Erarbeitung einer Bewertung des Vertrauensniveaus einer Verwaltungsleistung sollten alle zusammengetragenen Informationen und Bewertungen nach Abschluss erneut betrachtet und geprüft werden. Durch die neuen Erkenntnisse, die während der Bearbeitung höchstwahrscheinlich gewonnen wurden, können eventuell Anpassungen nötig werden. Dadurch wird die Genauigkeit der Vertrauensniveaubestimmung erhöht. Werden nacheinander die Vertrauensniveaus mehrerer Verwaltungsleistung bestimmt, so ist dieser Prozess ebenfalls anzuwenden.

6.2.5 Stellenwert der Nutzerperspektive

Online angebotene Verwaltungsleistungen, die zwar formal die Vorgaben des OZG erfüllen, aber die Perspektive der Nutzer außer Acht lassen, verfehlen den Zweck des OZG und der Bestrebungen des Verwaltungsdigitalisierung insgesamt.

Es wird daher empfohlen, bei der Vertrauensniveaubewertung, die Nutzerperspektive im Blick zu behalten. Sofern es im Hinblick auf die dokumentierten Gefährdungen möglich ist, sollte geprüft werden, ob die Wahl des Vertrauensniveaus wegen der höheren Akzeptanz der Nutzer für Mechanismen auf niedrigeren Vertrauensniveaus angepasst werden kann.

Erreicht man bei der Gesamtbewertung beispielsweise knapp ein Vertrauensniveau von „substanziell“, so könnte geprüft werden, dieses auf „normal“ abzustufen, um mit der Verwaltungsleistung mehr Nutzer zu erreichen. Die Vorteile dieser Abwertung sind dabei sorgfältig gegen die Risiken abzuwägen.[41]

6.2.6 Zukünftige Erweiterungen

Die Prozessschritte Kommunikation und Tracking sowie Erhalt der Leistung (digital) werden aktuell in Amt24 (noch) nicht genutzt (vgl. Cornelia Pflüger, Projektleitung Serviceportal Amt 24, Hauptamt, Stadt Leipzig, persönliche Kommunikation, 22.02.2022; siehe auch Abschn. 2.5). Sie wurden daher bei den Empfehlungen zur Vertrauensniveaubewertung bisher noch nicht berücksichtigt und auch nicht in die Arbeitshilfe in Anh. 8 aufgenommen. Sobald sich das zukünftig ändert, ist die Arbeitshilfe entsprechend zu überarbeiten.

6.3 Durchführung

6.3.1 Zyklische Überprüfung

Bei der Bewertung des Erfüllungsaufwands der Verwaltung bei der Digitalisierung von Verwaltungsleistungen ging die Bundesregierung 2016 noch davon aus, dass es sich bei

[41] Auch vor dem Hintergrund der praktischen Umsetzbarkeit ist eine solche Prüfung aktuell angezeigt: Solange noch keine Möglichkeit vorhanden ist, sich auf substanziellem Vertrauensniveau zu authentisieren, sollte dafür ebenfalls geprüft werden, ob eine Herunterstufung sinnvoll ist.

der Bestimmung des Vertrauensniveaus um eine einmalige Aufgabe handelt (vgl. BT-Drs. 18/10183, S. 73). Eine zyklische Neubewertung in Anlehnung an das Verfahren der Managementsysteme für Informationssicherheit (BSI 200-1: S. 17 ff.) erscheint jedoch geeigneter.

Die Festlegung des Vertrauensniveau kann nicht statisch sein, da sich sowohl rechtliche und technische als auch tatsächliche Rahmenbedingungen kontinuierlich weiterentwickeln. Verschieben sich die Umstände, die die möglichen Schädensfälle, Schadenshöhen und Eintrittswahrscheinlichkeiten bedingen, können Anpassungen nötig werden. Auch jeder tatsächlich eingetretene Schadensfall kann eine Neubewertung erforderlich machen.

Vorgeschlagen wird deshalb eine jährliche Überprüfung, sofern sich nicht aus der praktischen Erfahrung ein anderer Turnus als passender abzeichnet.

6.3.2 Einbettung in vorhandene Strukturen

In der Praxis sollte erprobt werden, ob sich eine Vertrauensniveaubewertung im Zusammenhang mit den bereits etablierten Workshops zur Schutzbedarfsfeststellung anbietet (vgl. Cornelia Pflüger, Projektleitung Serviceportal Amt 24, Hauptamt, Stadt Leipzig, persönliche Kommunikation, 08.03.2022). Ob es günstig ist, diesen schon bestehenden Rahmen zu nutzen, oder ob die jeweilige Veranstaltung dadurch überladen wird, kann ohne praktische Überprüfung nicht beurteilt werden. In jedem Fall ist es nützlich, wenn bei der Vertrauensniveaubestimmung die Ergebnisse der Schutzbedarfsfeststellung bereits vorliegen.

6.3.3 Verantwortlicher und Beteiligte

Wie in der Handreichung des IT-Planungsrates vorgeschlagen sollte ein Experte aus der Fachlichkeit (z. B. Sachgebietsleiter) die Vertrauensniveaubewertung vornehmen. Wie bei der Schutzbedarfsfestellung ist *eine* geeignete Person ausreichend; die Beteiligung einer größeren Gruppe ist nicht nötig (vgl. BSI 200-2: S. 110).

Ebenfalls wie in der Handreichung des IT-Planungsrates vorgeschlagen sollten aber die Beauftragten für Informationssicherheit und Datenschutz beteiligt werden. Gerade bei der Bildung der Gesamtbewertung könnten sie bei Bedarf beratend zur Seite stehen.

6.3.4 Zusammenarbeit

Mit dem Ziel, die Vertrauensniveaubewertung zu verbessern, wird empfohlen, einen Austausch mit anderen Kommunen anzustreben. Anders als in der Handreichung des IT-Planungsrates nahegelegt (vgl. IT-Planungsrat 2020: S. 5), muss dabei nicht eine Abstimmung zur einheitlichen Vergabe von Vertrauensniveaus für gleichartige Verwaltungsleistungen im Vordergrund stehen. Auch Informationen zum Vorgehen, zu konkreten Erfahrungen bei der Vertrauensniveaubewertung und zu eingetretenen Schadensfällen könnten Inhalte des Dialogs im Sinne eines Best-Practice-Austauschs sein. Besonders da die Informationslage zum Thema Vertrauensniveau aus den allgemeinen Vorgaben eher dürftig ist, kann ein solcher Austausch gewinnbringend sein.

7 Beispiele für die Vertrauensniveaubestimmung von OZG-Leistungen der Stadt Leipzig

Die Verwendung der für diese Arbeit erstellten Arbeitshilfe zur Vertrauensniveaubewertung wird an drei Beispielen illustriert. Im Folgenden sollen in aller Kürze die betrachteten Leistungen vorgestellt werden.

7.1 Baumfällung

Möchte ein Verwaltungskunde einen Baum oder ein anderes Gehölz fällen oder stark zurückschneiden und ist dieser Baum oder dieses Gehölz von BNatSchG oder SächsNatSchG oder der Baumschutzsatzung der Stadt Leipzig geschützt, so muss ein entsprechender Antrag gestellt werden. Weitere Details können der Leistungsseite auf Amt24 entnommen werden (Stadt Leipzig 2022d).

Die Vertrauensniveaubewertung fand ohne Konsultation eines Verantwortlichen aus der Fachlichkeit statt. Die Einschätzungen beruhen auf den für die Antragstellung zu übermittelnden Daten. Die Dokumentation der Vertrauensniveaubestimmung und das resultierende Ergebnis befindet sich in Anh. 9.

7.2 Havariemeldung (Aufgrabung)

Grundsätzlich bedürfen Aufgrabungen im öffentlichen Raum einer Genehmigung; muss jedoch aufgrund einer Havarie an einer im Boden verlegten Strom-, Gas-, Wasser-, Abwasser- oder Telekommunikationsleitung zeitnah eine Aufgrabung vorgenommen werden, reicht eine sog. Havariemeldung aus, mit der die nachträglich zu genehmigende Aufgrabung angemeldet wird (vgl. Kathrin Herz-Meinschenk, Sachgebietsleiterin Stadttechnische Koordinierung, Verkehrs- und Tiefbauamt, Stadt Leipzig, persönliche Kommunikation, 22.02.2022).

Die Havariemeldung wird durch die Versorgungsunternehmen bzw. Betreiber der o. g. Netze oder von ihnen beauftragten Bauunternehmen abgegeben (vgl. Kathrin Herz-Meinschenk, Sachgebietsleiterin Stadttechnische Koordinierung, Verkehrs- und Tiefbauamt, Stadt Leipzig, persönliche Kommunikation, 22.02.2022). Die rechtlichen Grundlagen finden sich in § 8 FStrG, §§ 18, 23 SächsStrG und § 127 TKG. Weiterhin existieren Konzessionsverträge mit den Versorgungsunternehmen, die wiederum Rahmenverträge mit Bauunternehmen haben (vgl. Kathrin Herz-Meinschenk, Sachgebietsleiterin Stadttechnische Koordinierung, Verkehrs- und Tiefbauamt, Stadt Leipzig, persönliche Kommunikation, 22.02.2022).

Für die Vertrauensniveaubestimmung für diese Leistung wurde eine Verantwortliche aus der Fachlichkeit konsultiert. Die Dokumentation und das ermittelte Vertrauensniveau finden sich in Anh. 10.

7.3 Urkundenbestellung

Vom Standesamt der Stadt Leipzig können folgende Personenstandsurkunden angefordert werden: Geburtsurkunden, beglaubigte Abschriften aus dem Geburtenbuch/Geburtenregister, Sterbeurkunden, Eheurkunden und Lebenspartnerschaftsurkunden (Stadt Leipzig 2022e). Aufgrund der Ähnlichkeit der Leistungen wurde eine gemeinsame Vertrauensniveaubestimmung durchgeführt.

Urkunden werden gem. § 62 Abs. 1 PStG nur an Berechtigte erteilt. Sofern eine Gebühr anfällt, erfolgt die Bezahlung per Nachnahme. Weitere Details können der Leistungsseite auf Amt24 entnommen werden (Stadt Leipzig 2022c).

Die Vertrauensniveaubestimmung für diese Leistungen basiert auf Auskünften aus der Fachlichkeit (siehe Anh. 11).

8 Fazit und Ausblick

Ausgangspunkt dieser Arbeit war die Frage nach der Bestimmung eines angemessenen Vertrauensniveaus für Verwaltungsleistungen, die von der Stadt Leipzig selbst OZG-konform umzusetzen sind. Der Umstand, dass diese Frage kurz vor Ablauf der vom OZG vorgegebenen Umsetzungsfrist noch unbeantwortet war, zeigt einerseits, wie weit entfernt die Erreichung der OZG-Ziele noch liegt, und illustriert andererseits das Schattendasein, dass das Thema Vertrauensniveaubestimmung bisher geführt hat.

Die Frage zu stellen und zu beantworten ist jedoch unumgänglich: Die Vertrauensniveaubestimmung ist fester Bestandteil jeder OZG-konformen Digitalisierung einer Verwaltungsleistung.

Mit der im Rahmen dieser Arbeit erstellten Arbeitshilfe und den Empfehlungen zu Verfahren und Durchführung der Vertrauensniveaubestimmung ist der Stadt Leipzig hoffentlich eine nützliche Unterstützung zur Erfüllung dieser Aufgabe an die Hand gegeben. Eine gründliche „Felderprobung“ durch Verantwortliche aus der Fachlichkeit unter Beteiligung der Beauftragten für Informationssicherheit und Datenschutz steht noch aus, sie war im Rahmen der knapp bemessenen Durchführungszeit dieser Arbeit leider noch nicht im wünschenswerten Umfang möglich. Daraus entstehende Anpassungen, die sich aus den praktischen Erfahrungen und dem Fachwissen der beteiligten Experten ergeben, sind also nach Abschluss dieser Arbeit noch einzuarbeiten.

Sobald die aktualisierte Fassung der Handreichung des IT-Planungsrates veröffentlicht ist, muss zudem geprüft werden, inwieweit dadurch Änderungen am vorgeschlagenen Vorgehen notwendig werden. Wird das Praxistool Vertrauensniveau grundlegend überarbeitet, empfiehlt es sich, dieses ebenfalls erneut zu überprüfen.

Auch eine weiterführende Beleuchtung der theoretischen Hintergründen bietet sich an, denn ggf. lassen sich daraus auch für die praktische Umsetzung nützliche Erkenntnisse ableiten. Einige Zusammenhänge zwischen Sicherheitsniveaus, Vertrauensniveaus und Schutzbedarfskategorien sowie deren Festlegung wurden in dieser Arbeit bereits identifiziert und diskutiert. Die Komplexität der Materie überstieg dabei jedoch die anfänglichen Erwartungen deutlich, weshalb einige Fragen in diesem Rahmen offen bleiben mussten.

Wie sich die aktuellen Entwicklungen bezüglich des Rechtsrahmens der Verwaltungsdigitalisierung auf das Thema Verwaltungsdigitalisierung auswirken wird, ist noch nicht abschätzbar. Beispielsweise verlangen die sog. Dresdner Forderungen die Rückgabe der digitalisierbaren Pflichtaufgaben an die jeweilige Gesetzgebungsebene (vgl. Adelskamp u. a. 2021: S. 18). Sollte dies umgesetzt werden, würde damit auch die Bedeutung der Vertrauensniveaubestimmung auf kommunaler Ebene schwinden.

Auch eher gesellschaftlich-technologische Verschiebungen könnten die Zukunft dieses Themas beeinflussen. Ein Beispiel: Die Notwendigkeit der Berücksichtigung der Nutzerperspektive bei der Vertrauensniveaubestimmung beruht zum Teil auf der mangelnden Akzeptanz und Nutzung der eID-Funktion. Diesem Umstand versuchen verschiedene Initiativen, wie der Verein buergerservice.org (buergerservice.org e. V. 2022), entgegenzuwirken; aktuell gibt es auch auch in der Stadt Leipzig solche Bestrebungen (Stadt Leipzig 2022a). International sind eID-Lösung teilweise ubiquitär – meist in Verbindung mit einer Nutzung durch Private (wie z. B. Banken), was die Nutzungsintensität und damit die Ak-

zeptanz fördert (vgl. Martens 2010; Martini 2018: S. 20 ff.; Riedel 2019: S. 25 ff.; Felden u. a. 2020: S. 16 ff.).

Würde ein solcher Zustand auch in Deutschland erreicht, bestünde aus Nutzerperspektive kaum noch Druck, Verwaltungsleistungen auf niedrigeren Vertrauensniveaus anzubieten.

Ein weiteres Beispiel: Durch die Ausweitung der online angebotenen Verwaltungsleistungen angespornte Entwicklungen im Bereich der Cyberkriminalität könnte Veränderungen für die Sicherstellung der Informationssicherheit bei der Nutzung von Verwaltungsportalen nötig machen. Jedes neue denkbare Schadensszenario – und jeder tatsächlich eingetretene Schadensfall – beeinflusst die Vertrauensniveaubestimmung und verdeutlicht die Relevanz dieses Themas.

Ungeachtet eventueller Verschiebungen in die eine oder andere Richtung ändert sich das Grundprinzip nicht: Die Notwendigkeit für die Verwaltung, bei der Interaktion mit Verwaltungskunden zu wissen, wie viel Vertrauen sie der behaupteten Identität und den übermittelten Daten und Dokumenten schenken darf, wird bestehen bleiben. Denn ohne Umsetzung eines angemessenen Vertrauensniveau gilt weiterhin das altbekannte Sprichwort:

"On the Internet, nobody knows you're a dog."

— Peter Steiner, The New Yorker, 05.06.1993

Kernsätze

1. Die Bestimmung eines adäquaten Vertrauensniveaus ist eine essenzielle Voraussetzung für die rechtssichere und nutzerfreundliche Digitalisierung von Verwaltungsleistungen im Kontext des OZG.

2. Obwohl die Vertrauensniveaubestimmung für eine erfolgreiche OZG-Umsetzung von wesentlicher Bedeutung ist, ist die Informationsbasis, die den betroffenen Behörden dafür zu den theoretischen Hintergründen sowie zur praktischen Durchführung bislang zur Verfügung steht, überraschend unzureichend.

3. Auf die Vertrauensniveaubestimmung wirken sich Vorgaben von allen Rechtsetzungsebenen (EU: eIDAS-VO, Bund: EGovG, OZG, VwVfg, AO, SGB, ITSiV-PV; Land: SächsEGovG, SächsEGovGDVO, SächsVwVfZG; Kommune: z. B. Marktsatzung der Stadt Leipzig) sowie aus weiteren Normquellen (TR-03107-1) verbindlich aus.

4. Damit Hilfsmittel für Digitalisierungsvorhaben tatsächlichen Nutzen stiften können, müssen sie stets mindestens ebenso aktuell gehalten werden wie die rechtlichen und technischen Bedingungen des Rahmens, den sie ausfüllen helfen sollen.

5. Die Nutzung des Praxistools Vertrauensniveau des BMI kann in seiner aktuellen Version (Stand 2021) nur eingeschränkt empfohlen werden.

6. Für eine effektive und effiziente Vertrauensniveaubestimmung bei der OZG-Umsetzung in der Stadt Leipzig werden mit dieser Arbeit passgenaue Empfehlungen und eine praktische Arbeitshilfe vorgelegt, die die Arbeit der zuständigen Akteure in der Verwaltungsdigitalisierung nach aktuellem Stand bestmöglich unterstützen und für künftige Weiterentwicklungen offen sind.

7. Normenscreenings als Vorbereitung entsprechender Gesetzgebung zum Schriftformabbau sollten alle Rechtsvorschriften einbeziehen und sowohl die verwaltungsinterne als auch -externe Kommunikation im Blick haben, um die größtmöglichen Vorteile für die OZG-Umsetzung und Verwaltungsdigitalsierung zu erzielen, da erfolgreiche Digitalisierung von Verwaltungsleistungen nicht darin besteht, analoge Prozesse mit digitalen Mitteln nachzubilden, sondern die hergebrachten Prozesse zu hinterfragen und neu zu gestalten.

Anhangsverzeichnis

Anhang 1 Übersicht Praxistool Vertrauensniveau („Stand, 22.04.2020, 8:00 Uhr“): Fragen zum Schutzbedarf

Prozess(schritt)	Fragen	Mögliche Antworten
Ausfüllen des Formulars	Wie sensibel sind die erfassten Daten und Dokumente?	Keine Daten mit Personenbezug oder Daten, bei deren Offenlegung mit nur geringfügigen Auswirkungen für den Betroffenen zu rechnen ist.
		Es handelt sich um personenbezogene Daten, die in den Bereich der "besonderen Kategorien" schützenswerter Daten nach DSGVO fallen, z.B. Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, rassische und ethnische Herkunft, Personalaktendaten, Kontodaten, gesundheitliche Verhältnisse, strafbare Handlungen, Ordnungswidrigkeiten, religiöse oder politische Anschauungen, arbeitsrechtliche Verhältnisse, ferner Steuerdaten, Sozialdaten, psychologische Daten, Unterbringung in Anstalten, Adoptionen, Betreuungen, Wahlausschlüsse, Passversagungsgründe (moralische und soziale Existenz).
	Werden bei der Antragstellung: a.) Daten aus öffentlichen Registern oder Nutzerkonten abgefragt (z.B. um dem Antragsteller die Eingabe zu erleichtern) bzw. b.) sind vom Antragsteller Nachweise hochzuladen und werden diese Daten mit zwischengespeichert?	Ja
		Nein, es ist keine Zwischenspeicherung oder Austausch von Daten vorgesehen
Absenden des Formulars	Welche Schäden können entstehen, wenn es Dritten gelingt, sich mit falscher Identität zu authentisieren bzw. einen Antrag abzusenden?	Es können keine oder nur geringfügige Schäden für Betroffene entstehen, die Richtigstellung der Daten geht bis auf geringfügige Ausnahmen zu Lasten der verarbeitenden Stelle. Falls die verarbeitende Stelle den Fehler nicht selbst bemerkt, ist der Betroffene in der Lage, die Richtigstellung durch einfache Kommunikation mit der verarbeitenden Stelle durchzusetzen, wodurch ihm keine oder unerhebliche Mehrkosten/Zeitaufwand entstehen.
		Es können erhebliche Schäden für Betroffene entstehen.

Prozess(schritt)	Fragen	Mögliche Antworten
	Wie hoch ist der Anreiz für Dritte oder für organisierte Kriminalität, Daten zu manipulieren? Welche Angriffe, Vorfälle sind für diesen Prozess in der (analogen) Vergangenheit bekannt geworden? Würde der Angriff bemerkt und kompensiert werden?	Sehr geringer Anreiz, sehr geringe Eintrittswahrscheinlichkeit. Es gab bisher keine ähnlich gelagerten Fälle und selbst durch die Digitalisierung der Prozesse ist ein solches Szenario schwer vorstellbar. Es gibt eine unmittelbare Möglichkeit, den Vorfall durch den Kontext des Antrages zu erkennen und zu kompensieren.
		Bestehender Anreiz oder bestehende Angreifergruppe. Der Prozess ist scheinbar prädestiniert für Identitätsmissbrauch und kann nicht so umstrukturiert werden, dass die Vorfälle zweifelsfrei bemerkt würden. Manipulation/ Einsichtnahme/ Löschung würde nicht sofort bemerkt werden.
	Besteht für diesen Antrag eine Schriftformerfordernis, dann gelten die Vorgaben zum elektronischen Schriftformersatz gem. § 3a Verwaltungsverfahrensgesetz des Bundes bzw. vergleichbarer Regelungen in den Ländern (weiterer Ausführungen können der technischen Richtlinie TR-03107-2 entnommen werden)?	Ja
		Nein
Kommunikation und Status-Tracking	Welche Schäden könnten Antragstellern entstehen, wenn unbefugte Dritte im Namen der Antragstellers Status-Updates oder Kommunikation mit der Behörde einsehen, verändern oder löschen können (inkl. Terminvereinbarung)?	Keine oder geringfügige Schäden für Betroffene, die Richtigstellung der Daten geht bis auf geringfügige Ausnahmen zu Lasten der verarbeitenden Stelle. Falls die verarbeitende Stelle den Fehler nicht selbst bemerkt, ist der Betroffene in der Lage, die Richtigstellung durch einfache Kommunikation mit der verarbeitenden Stelle durchzusetzen, wodurch ihm keine oder unerhebliche Mehrkosten/Zeitaufwand entstehen. Es sind keine inhaltlichen Daten des Antrages sichtbar, diese können weder modifiziert noch gelöscht werden.

Prozess(schritt)	Fragen	Mögliche Antworten
		Erhebliche Schäden – Zeitlicher und/oder finanzieller Aufwand für die Richtigstellung des Sachverhaltes – Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden – Offenlegung oder Änderungs-/Löschungsmöglichkeit sensibler Daten (besonders schützenswerte personenbezogene Daten im Sinne der DSGVO), die Teil des Antrages sind
	Welche Schäden könnten für Sie als verarbeitende Stelle dadurch entstehen, dass unbefugte Dritte (Personen, die sich als Antragstellender ausgeben) Status-Updates oder Kommunikation mit der Behörde einsehen, verändern oder löschen können (inkl. Terminvereinbarung)?	Vertretbare Schäden – Finanzielle Schäden (z.B. Schadensersatzansprüche oder Geldstrafen durch Klagen der Betroffenen oder von Aktivisten wegen Verletzung von Gesetzen, Verträgen, Vorschriften) können ohne negative Auswirkungen aus dem laufenden Haushalt bestritten werden – Leichte Zeitverzögerung in der Bearbeitung, tolerierbare Beeinträchtigung der Aufgabenerfüllung – Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten – Es werden keine dienstrechtlichen Konsequenzen ausgelöst
		Existenzbedrohende und erhebliche Schäden – Mögliche Schäden (z.B. Schadensersatzansprüche oder Geldstrafen durch Klagen der Betroffenen oder von Aktivisten wegen Verletzung von Gesetzen, Verträgen, Vorschriften) können nur aus dem laufenden Haushalt bestritten werden, wenn andere Vorhaben eingeschränkt oder verschoben werden – Erhebliche, öffentlich sichtbare Beeinträchtigung der Aufgabenerfüllung – Es ist eine breite Ansehens- oder Vertrauensbeeinträchtigung gegenüber der Öffentlichkeit zu erwarten – Es werden dienstrechtliche Konsequenzen ausgelöst
	Wie hoch ist der Anreiz für einen Dritten, die Kommunikation (Statusanfragen, Rückfragen, Terminvereinbarungen) zu manipulieren, zu löschen? Welche Angriffe, Vorfälle sind für diesen Prozess in der (analogen) Vergangenheit bekannt	Sehr geringer Anreiz, sehr geringe Eintrittswahrscheinlichkeit. Es gab bisher keine ähnlich gelagerten Fälle und selbst durch die Elektronifizierung der Prozesse ist ein solches Szenario schwer vorstellbar. Es gibt eine unmittelbare Möglichkeit, den Vorfall durch

Prozess(schritt)	Fragen	Mögliche Antworten
	geworden? Würde der Angriff bemerkt und kompensiert werden?	Bestehender Anreiz, bestehende Angreifergruppe. Der Prozess ist scheinbar prädestiniert für Identitätsmissbrauch und kann nicht so umstrukturiert werden, dass die Vorfälle zweifelsfrei bemerkt würden. Manipulation/Einsichtnahme/Löschung würde nicht sofort bemerkt werden.
Erhalt der Leistung (digital)	Welche Schäden können Antragstellern entstehen, wenn unbefugte Dritte im Namen der Antragstellenden Möglichkeiten zur Kenntnisnahme/Änderung/Löschung des Bescheids der Behörde haben?	Keine oder geringfügige Schäden für Betroffene, die Richtigstellung der Daten geht bis auf geringfügige Ausnahmen zu Lasten der verarbeitenden Stelle. Falls die verarbeitende Stelle den Fehler nicht selbst bemerkt, ist der Betroffene in der Lage, die Richtigstellung durch einfache Kommunikation mit der verarbeitenden Stelle durchzusetzen, wodurch ihm keine oder unerhebliche Mehrkosten/Zeitaufwand entstehen. Es sind keine inhaltlichen Daten des Antrages sichtbar, diese können weder modifiziert noch gelöscht werden.
		Erhebliche Schäden – Zeitlicher und/oder finanzieller Aufwand für die Richtigstellung des Sachverhaltes – Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden – Offenlegung oder Änderungs-/Löschungsmöglichkeit sensibler Daten (besonders schützenswerte personenbezogene Daten im Sinne der DSGVO), die Teil des Antrages sind
	Welche Schäden könnten für Sie als verarbeitende Stelle dadurch entstehen, dass unbefugte Dritte (Personen, die sich als der Antragstellende ausgeben) Möglichkeiten zur Kenntnisnahme/Änderung/Löschung des Bescheids der Behörde haben?	Vertretbare Schäden – Finanzielle Schäden (z.B. Schadensersatzansprüche oder Geldstrafen durch Klagen der Betroffenen oder von Aktivisten wegen Verletzung von Gesetzen, Verträgen, Vorschriften) können ohne negative Auswirkungen aus dem laufenden Haushalt bestritten werden – Leichte Zeitverzögerung in der Bearbeitung, tolerierbare Beeinträchtigung der Aufgabenerfüllung – Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten – Es werden keine dienstrechtlichen Konsequenzen ausgelöst

Anhang 2 Übersicht Praxistool Vertrauensniveau („Stand, 22.04.2020, 8:00 Uhr“): Fragen zum Vertrauensniveau

Prozess(schritt)	Fragen	Mögliche Antworten
Identifizierung	Welche Gefährdungen/Schadenskategorien könnten in der Verwaltungspraxis bzw. bei der Digitalisierung relevant werden?	Verstoß gegen Gesetze/Vorschriften
		Unrichtige Identifizierung oder Zuordnung zu einer Identität
		Beeinträchtigung des informationellen Selbstbestimmungsrechts
		Beeinträchtigung körperlicher/persönlicher Unversehrtheit
		Beeinträchtigung der Aufgabenerfüllung
		Negative Innen- oder Außenwirkung
		Finanzielle Auswirkungen
	Bitte beschreiben Sie kurz und nachvollziehbar ein mögliches Schadenszenario aus Ihrer Verwaltungspraxis mit Blick auf die anschließende Bewertung mit Schadenshöhe und Eintrittswahrscheinlichkeit.	[Freitext]
	Wie hoch schätzen Sie den möglichen Schaden ein?	niedrig
		substanziell
		hoch
	Wie groß ist der Anreiz und damit auch die Wahrscheinlichkeit, dass ein Antragsteller versucht sich mit falscher Identität zu authentisieren?	unwahrscheinlich
		normal
		wahrscheinlich
Daten-/ Dokumentenübermittlung	Welche Gefährdungen/Schadenskategorien könnten in der Verwaltungspraxis bzw. bei der Digitalisierung relevant werden?	Verstoß gegen Gesetze/Vorschriften
		Unrichtige Identifizierung oder Zuordnung zu einer Identität
		Beeinträchtigung des informationellen Selbstbestimmungsrechts
		Beeinträchtigung körperlicher/persönlicher Unversehrtheit
		Beeinträchtigung der Aufgabenerfüllung
		Negative Innen- oder Außenwirkung
		Finanzielle Auswirkungen
	Bitte beschreiben Sie kurz und nachvollziehbar ein mögliches Schadenszenario aus Ihrer Verwaltungspraxis mit Blick auf die anschließende Bewertung mit Schadenshöhe und Eintrittswahrscheinlichkeit.	[Freitext]

Prozess(schritt)	Fragen	Mögliche Antworten
	Wie hoch schätzen Sie den möglichen Schaden ein?	niedrig
		substanziell
		hoch
	Wie groß ist der Anreiz und damit auch die Wahrscheinlichkeit, dass Dritte versuchen Daten abzufangen und diese gegebenenfalls zu verändern?	unwahrscheinlich
		normal
		wahrscheinlich
Willenserklärung	Welche Gefährdungen/Schadenskategorien könnten in der Verwaltungspraxis bzw. bei der Digitalisierung relevant werden?	Verstoß gegen Gesetze/Vorschriften
		Unrichtige Identifizierung oder Zuordnung zu einer Identität
		Beeinträchtigung des informationellen Selbstbestimmungsrechts
		Beeinträchtigung körperlicher/persönlicher Unversehrtheit
		Beeinträchtigung der Aufgabenerfüllung
		Negative Innen- oder Außenwirkung
		Finanzielle Auswirkungen
	Bitte beschreiben Sie kurz und nachvollziehbar ein mögliches Schadenszenario aus Ihrer Verwaltungspraxis mit Blick auf die anschließende Bewertung mit Schadenshöhe und Eintrittswahrscheinlichkeit.	[Freitext]
	Wie hoch schätzen Sie den möglichen Schaden ein?	niedrig
		substanziell
		hoch
	Wie groß ist der Anreiz und damit auch die Wahrscheinlichkeit, dass ein Antragsteller bestreitet eine Willenserklärung abgegeben zu haben?	unwahrscheinlich
		normal
		wahrscheinlich

Anhang 3 Übersicht Praxistool Vertrauensniveau („Stand, 17.06.2021“): Fragen zum Schutzbedarf

Prozess(schritt)	Fragen	Mögliche Antworten
Ausfüllen des Formulars	Wie sensibel sind die erfassten Daten und Dokumente?	Keine Daten mit Personenbezug oder Daten, bei deren Offenlegung mit nur geringfügigen Auswirkungen für den Betroffenen zu rechnen ist.
		Es handelt sich um personenbezogene Daten, die in den Bereich der "besonderen Kategorien" schützenswerter Daten nach DSGVO fallen, z.B. Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, rassische und ethnische Herkunft, Personalaktendaten, Kontodaten, gesundheitliche Verhältnisse, strafbare Handlungen, Ordnungswidrigkeiten, religiöse oder politische Anschauungen, arbeitsrechtliche Verhältnisse, ferner Steuerdaten, Sozialdaten, psychologische Daten, Unterbringung in Anstalten, Adoptionen, Betreuungen, Wahlausschlüsse, Passversagungsgründe (moralische und soziale Existenz).
	Werden bei der Antragstellung: a.) Daten aus öffentlichen Registern oder Nutzerkonten abgefragt (z.B. um dem Antragsteller die Eingabe zu erleichtern) bzw. b.) sind vom Antragsteller Nachweise hochzuladen und werden diese Daten mit zwischengespeichert?	Ja
		Nein, es ist keine Zwischenspeicherung oder Austausch von Daten vorgesehen
Absenden des Formulars	Welche Schäden können entstehen, wenn es Dritten gelingt, sich mit falscher Identität zu authentisieren bzw. einen Antrag abzusenden?	Es können keine oder nur geringfügige Schäden für Betroffene entstehen, die Richtigstellung der Daten geht bis auf geringfügige Ausnahmen zu Lasten der verarbeitenden Stelle. Falls die verarbeitende Stelle den Fehler nicht selbst bemerkt, ist der Betroffene in der Lage, die Richtigstellung durch einfache Kommunikation mit der verarbeitenden Stelle durchzusetzen, wodurch ihm keine oder unerhebliche Mehrkosten/Zeitaufwand entstehen.
		Es können erhebliche Schäden für Betroffene entstehen.

Prozess(schritt)	Fragen	Mögliche Antworten
	Wie hoch ist der Anreiz für Dritte oder für organisierte Kriminalität, Daten zu manipulieren? Welche Angriffe, Vorfälle sind für diesen Prozess in der (analogen) Vergangenheit bekannt geworden? Würde der Angriff bemerkt und kompensiert werden?	Sehr geringer Anreiz, sehr geringe Eintrittswahrscheinlichkeit. Es gab bisher keine ähnlich gelagerten Fälle und selbst durch die Digitalisierung der Prozesse ist ein solches Szenario schwer vorstellbar. Es gibt eine unmittelbare Möglichkeit, den Vorfall durch den Kontext des Antrages zu erkennen und zu kompensieren.
		Bestehender Anreiz oder bestehende Angreifergruppe. Der Prozess ist scheinbar prädestiniert für Identitätsmissbrauch und kann nicht so umstrukturiert werden, dass die Vorfälle zweifelsfrei bemerkt würden. Manipulation/ Einsichtnahme/ Löschung würde nicht sofort bemerkt werden.
Kommunikation und Status-Tracking	Welche Schäden könnten Antragstellern entstehen, wenn unbefugte Dritte im Namen der Antragstellers Status-Updates oder Kommunikation mit der Behörde einsehen, verändern oder löschen können (inkl. Terminvereinbarung)?	Keine oder geringfügige Schäden für Betroffene, die Richtigstellung der Daten geht bis auf geringfügige Ausnahmen zu Lasten der verarbeitenden Stelle. Falls die verarbeitende Stelle den Fehler nicht selbst bemerkt, ist der Betroffene in der Lage, die Richtigstellung durch einfache Kommunikation mit der verarbeitenden Stelle durchzusetzen, wodurch ihm keine oder unerhebliche Mehrkosten/Zeitaufwand entstehen. Es sind keine inhaltlichen Daten des Antrages sichtbar, diese können weder modifiziert noch gelöscht werden.
		Erhebliche Schäden – Zeitlicher und/oder finanzieller Aufwand für die Richtigstellung des Sachverhaltes – Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden – Offenlegung oder Änderungs-/Löschungsmöglichkeit sensibler Daten (besonders schützenswerte personenbezogene Daten im Sinne der DSGVO), die Teil des Antrages sind

Prozess(schritt)	Fragen	Mögliche Antworten
	Welche Schäden könnten für Sie als verarbeitende Stelle dadurch entstehen, dass unbefugte Dritte (Personen, die sich als Antragstellender ausgeben) Status-Updates oder Kommunikation mit der Behörde einsehen, verändern oder löschen können (inkl. Terminvereinbarung)?	Vertretbare Schäden – Finanzielle Schäden (z.B. Schadensersatzansprüche oder Geldstrafen durch Klagen der Betroffenen oder von Aktivisten wegen Verletzung von Gesetzen, Verträgen, Vorschriften) können ohne negative Auswirkungen aus dem laufenden Haushalt bestritten werden – Leichte Zeitverzögerung in der Bearbeitung, tolerierbare Beeinträchtigung der Aufgabenerfüllung – Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten – Es werden keine dienstrechtlichen Konsequenzen ausgelöst
		Existenzbedrohende und erhebliche Schäden – Mögliche Schäden (z.B. Schadensersatzansprüche oder Geldstrafen durch Klagen der Betroffenen oder von Aktivisten wegen Verletzung von Gesetzen, Verträgen, Vorschriften) können nur aus dem laufenden Haushalt bestritten werden, wenn andere Vorhaben eingeschränkt oder verschoben werden – Erhebliche, öffentlich sichtbare Beeinträchtigung der Aufgabenerfüllung – Es ist eine breite Ansehens- oder Vertrauensbeeinträchtigung gegenüber der Öffentlichkeit zu erwarten – Es werden dienstrechtliche Konsequenzen ausgelöst
	Wie hoch ist der Anreiz für einen Dritten, die Kommunikation (Statusanfragen, Rückfragen, Terminvereinbarungen) zu manipulieren, zu löschen? Welche Angriffe, Vorfälle sind für diesen Prozess in der (analogen) Vergangenheit bekannt geworden? Würde der Angriff bemerkt und kompensiert werden?	Sehr geringer Anreiz, sehr geringe Eintrittswahrscheinlichkeit. Es gab bisher keine ähnlich gelagerten Fälle und selbst durch die Elektronifizierung der Prozesse ist ein solches Szenario schwer vorstellbar. Es gibt eine unmittelbare Möglichkeit, den Vorfall durch den Kontext des Antrages zu erkennen und zu kompensieren.
		Bestehender Anreiz, bestehende Angreifergruppe. Der Prozess ist scheinbar prädestiniert für Identitätsmissbrauch und kann nicht so umstrukturiert werden, dass die Vorfälle zweifelsfrei bemerkt würden. Manipulation/Einsichtnahme/Löschung würde nicht sofort bemerkt werden.

Prozess(schritt)	Fragen	Mögliche Antworten
Erhalt der Leistung (digital)	Welche Schäden können Antragstellern entstehen, wenn unbefugte Dritte im Namen der Antragstellenden Möglichkeiten zur Kenntnisnahme/Änderung/Löschung des Bescheids der Behörde haben?	Keine oder geringfügige Schäden für Betroffene, die Richtigstellung der Daten geht bis auf geringfügige Ausnahmen zu Lasten der verarbeitenden Stelle. Falls die verarbeitende Stelle den Fehler nicht selbst bemerkt, ist der Betroffene in der Lage, die Richtigstellung durch einfache Kommunikation mit der verarbeitenden Stelle durchzusetzen, wodurch ihm keine oder unerhebliche Mehrkosten/Zeitaufwand entstehen. Es sind keine inhaltlichen Daten des Antrages sichtbar, diese können weder modifiziert noch gelöscht werden.
		Erhebliche Schäden – Zeitlicher und/oder finanzieller Aufwand für die Richtigstellung des Sachverhaltes – Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden – Offenlegung oder Änderungs-/Löschungsmöglichkeit sensibler Daten (besonders schützenswerte personenbezogene Daten im Sinne der DSGVO), die Teil des Antrages sind
	Welche Schäden könnten für Sie als verarbeitende Stelle dadurch entstehen, dass unbefugte Dritte (Personen, die sich als der Antragstellende ausgeben) Möglichkeiten zur Kenntnisnahme/Änderung/Löschung des Bescheids der Behörde haben?	Vertretbare Schäden – Finanzielle Schäden (z.B. Schadensersatzansprüche oder Geldstrafen durch Klagen der Betroffenen oder von Aktivisten wegen Verletzung von Gesetzen, Verträgen, Vorschriften) können ohne negative Auswirkungen aus dem laufenden Haushalt bestritten werden – Leichte Zeitverzögerung in der Bearbeitung, tolerierbare Beeinträchtigung der Aufgabenerfüllung – Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten – Es werden keine dienstrechtlichen Konsequenzen ausgelöst

Anhang 4 Übersicht Praxistool Vertrauensniveau („Stand, 17.06.2021“): Fragen zum Vertrauensniveau

Prozess(schritt)	Fragen	Mögliche Antworten
Identifizierung	Wählen Sie bitte die Gefährdungen/Schadenskategorien, die für Sie aus Ihre Verwaltungspraxis bzw. bei der Digitalisierung relevant werden.	Verstoß gegen Gesetze/Vorschriften
		Unrichtige Identifizierung oder Zuordnung zu einer Identität
		Beeinträchtigung des informationellen Selbstbestimmungsrechts
		Beeinträchtigung körperlicher/persönlicher Unversehrtheit
		Beeinträchtigung der Aufgabenerfüllung
		Negative Innen- oder Außenwirkung
		Finanzielle Auswirkungen
	Bitte beschreiben Sie kurz und nachvollziehbar ein mögliches Schadenszenario aus Ihrer Verwaltungspraxis mit Blick auf die anschließende Bewertung mit Schadenshöhe und Eintrittswahrscheinlichkeit.	[Freitext]
	Wie hoch schätzen Sie den möglichen Schaden ein?	niedrig
		substanziell
		hoch
	Wie groß ist der Anreiz und damit auch die Wahrscheinlichkeit, dass ein Antragsteller versucht sich mit falscher Identität zu authentisieren?	unwahrscheinlich
		normal
		wahrscheinlich
Willenserklärung	Wählen Sie bitte die Gefährdungen/Schadenskategorien, die für Sie aus Ihre Verwaltungspraxis bzw. bei der Digitalisierung relevant werden.	Verstoß gegen Gesetze/Vorschriften
		Unrichtige Identifizierung oder Zuordnung zu einer Identität
		Beeinträchtigung des informationellen Selbstbestimmungsrechts
		Beeinträchtigung körperlicher/persönlicher Unversehrtheit
		Beeinträchtigung der Aufgabenerfüllung
		Negative Innen- oder Außenwirkung
		Finanzielle Auswirkungen
	Bitte beschreiben Sie kurz und nachvollziehbar ein mögliches Schadenszenario aus Ihrer Verwaltungspraxis mit Blick auf die anschließende Bewertung mit Schadenshöhe und Eintrittswahrscheinlichkeit.	[Freitext]

Prozess(schritt)	Fragen	Mögliche Antworten
	Wie hoch schätzen Sie den möglichen Schaden ein?	niedrig
		substanziell
		hoch
	Wie groß ist der Anreiz und damit auch die Wahrscheinlichkeit, dass ein Antragsteller bestreitet eine Willenserklärung abgegeben zu haben?	unwahrscheinlich
		normal
		wahrscheinlich
Daten-/ Dokumentenübermittlung	Wählen Sie bitte die Gefährdungen/Schadenskategorien, die für Sie aus Ihre Verwaltungspraxis bzw. bei der Digitalisierung relevant werden.	Verstoß gegen Gesetze/Vorschriften
		Unrichtige Identifizierung oder Zuordnung zu einer Identität
		Beeinträchtigung des informationellen Selbstbestimmungsrechts
		Beeinträchtigung körperlicher/persönlicher Unversehrtheit
		Beeinträchtigung der Aufgabenerfüllung
		Negative Innen- oder Außenwirkung
		Finanzielle Auswirkungen
	Bitte beschreiben Sie kurz und nachvollziehbar ein mögliches Schadenszenario aus Ihrer Verwaltungspraxis mit Blick auf die anschließende Bewertung mit Schadenshöhe und Eintrittswahrscheinlichkeit.	[Freitext]
	Wie hoch schätzen Sie den möglichen Schaden ein?	niedrig
		substanziell
		hoch
	Wie groß ist der Anreiz und damit auch die Wahrscheinlichkeit, dass Dritte versuchen Daten abzufangen und diese gegebenenfalls zu verändern?	unwahrscheinlich
		normal
		wahrscheinlich
Schriftformerfordernis	Besteht für diesen Antrag eine Schriftformerfordernis, dann gelten die Vorgaben zum elektronischen Schriftformersatz gem. § 3a Verwaltungsverfahrensgesetz des Bundes bzw. vergleichbarer Regelungen in den Ländern (weiterer Ausführungen können der technischen Richtlinie TR-03107-2 entnommen werden)?	Ja
		Nein

Anhang 5 Beispiel Ergebnisdarstellung Version 2020: keine Ausgabe der Details

Ihr Ergebnis für den Prozessschritt "Ausfüllen des Formulars":

Für Ihren Online-Dienst wurde der Schutzbedarf **NORMAL** festgestellt.

Anhang 6 Beispiel Ergebnisdarstellung Version 2021: Toggle-Button (oben) und eingeblendete Details (unten)

Ihr Ergebnis für den Prozessschritt "Ausfüllen des Formulars":

Für Ihren Online-Dienst wurde der Schutzbedarf **NORMAL** festgestellt.

Frage und Antworten	Ihre Auswahl anzeigen

Ihr Ergebnis für den Prozessschritt "Ausfüllen des Formulars":

Für Ihren Online-Dienst wurde der Schutzbedarf **NORMAL** festgestellt.

Frage	Ihre Antwort
Wie sensibel sind die erfassten Daten und Dokumente?	Keine Daten mit Personenbezug oder Daten, bei deren Offenlegung mit nur geringfügigen Auswirkungen für den Betroffenen zu rechnen ist.
Werden bei der Antragstellung: a.)Daten aus öffentlichen Registern oder Nutzerkonten abgefragt (z.B. um dem Antragsteller die Eingabe zu erleichtern) bzw. b.) sind vom Antragsteller Nachweise hochzuladen und werden diese Daten mit zwischengespeichert?	Nein, es ist keine Zwischenspeicherung oder Austausch von Daten vorgesehen

Anhang 7 Übersicht zu FIM-Leistungen mit Informationen zum Vertrauensniveau

Schlüssel	Bezeichnung	Vertrauens-niveau	Typ
99050051001000	Erlaubnis zur gewerbsmäßigen Bekämpfung von Wirbeltieren als Schädlinge Erteilung	normal	2/3
99050066007000	Brütereien Zulassung	normal	2/3
99050132019000	Brütereien und Betriebe zur Erzeugung von Bruteiern Registrierung	normal	2/3
99110013061000	Tierschutzbeauftragte Bestellung	normal	2/3
99110010022000	Sachkundenachweis zum Töten von Wirbeltieren Bescheinigung	normal	2/3
99089051169002	Meldung des Verdachts auf Geldwäsche oder Terrorismusfinanzierung Anzeige über die Auslagerung interner Sicherungsmaßnahmen	normal	1
99090007006004	Zoo-Genehmigung für den Betrieb	normal	2/3
99110003001000	Erlaubnis zur Zucht, Haltung und zum Handel mit Tieren Erteilung	normal	2/3
99050032002001	Veranstaltung Festsetzung von Tierausstellung, Tiermarkt oder Tierbörse	normal	2/3
99102015111000	Kraftfahrzeugsteuer Erhebung	substanziell	1
99082004007000	Rechtsanwaltsgesellschaft Zulassung	hoch	2/3
99085003015000	Kinderreisepass Statusabfrage	hoch	2/3
99111023080000	Witwen- und Witwerrente für Hinterbliebene von gesetzlich Unfallversicherten Gewährung	hoch	1
99111012080000	Leistungen bei Pflegebedürftigkeit für gesetzlich Unfallversicherte Gewährung	hoch +	1
99085001012007	Reisepass Ausstellung zusätzlicher Pässe	hoch +	2/3
99085001012009	Reisepass Ausstellung neu wegen Namenänderung bei Scheidung oder Aufhebung einer Lebenspartnerschaft	hoch +	2/3
99085001036003	Reisepass Ersatz bei Passverlust im Ausland	hoch +	2/3
99085003011001	Kinderreisepass Änderung wegen Adressänderung	hoch +	2/3

Schriftformerfordernis

Hinweise:

- Die bloße Verpflichtung, ein Antragsformular mit Unterschriftfeld zu verwenden, stellt noch kein Schriftformerfordernis dar (vgl. § 13 EGovG).
- Liegt ein Schriftformerfordernis vor, wird das Vertrauensniveau als "hoch +" bewertet. Dann kommt ein Schriftformersatz gem. § 3a Abs. 2 Nr. 1 VwVfG in Frage (Identifikation mit eID, entspricht dem Vertrauensniveau "hoch"). Zusätzlich sollte durch Auslegung der Rechtnorm und fachliche Bewertung des Geschäftsprozesses ermittelt werden, welche Funktionen der Schriftform genau benötigt werden. Die technische Richtlinie des BSI TR-03107-2 gibt Auskunft zu Bewertung und technischer Umsetzung.

Frage	Antwort	Notizen
Besteht für diesen Antrag ein gesetzliches Schriftformerfordernis?	[Wählen Sie eine Antwort aus der Drop-down-Liste.]	
Falls ja, wo ist das Schriftformerfordernis verankert?		

Daten-/Dokumentenübermittlung

Übergreifende Frage:
Könnten bzw. würden Dritte Einfluss auf die Daten-/Dokumentenübermittlung nehmen? Könnten bzw. würden sie Daten oder Dokumente abfangen und diese ggf. verändern?

In Vorbereitung der Identifikation und Bewertung der Gefährdungen/Schadenskategorien zum Prozess Daten-/Dokumentenübermittlung machen Sie sich bitte zu folgenden Fragen Gedanken:

- Wie sensibel sind die erfassten Daten und Dokumente?
- Handelt es sich um Daten ohne Personenbezug oder Daten, bei deren Offenlegung mit nur geringfügigen Auswirkungen für den Betroffenen zu rechnen ist?
- Handelt es sich um personenbezogene Daten?
- Falls ja, werden diese in größerem Umfang erhoben?
- Handelt es sich um personenbezogene Daten besonderer Kategorie gem. Art. 9 Abs. 1 DSGVO (Daten zur rassische und ethnische Herkunft, zu politische Meinungen, religiösen oder weltanschaulichen Überzeugungen oder Gewerkschaftszugehörigkeit hervorgehen, genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung)?
- Handelt es sich um andere schützenswerte Daten (Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, Personalaktendaten, Kontodaten, Daten zu strafbaren Handlungen und Ordnungswidrigkeiten, Steuerdaten, Sozialdaten, Daten zu Wahlausschlüssen oder Passversagungsgründe)?

Thema	Fragen	Antwort	Notizen
Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Daten- bzw. Dokumenten-übermittlung sind aus der Verwaltungspraxis bereits bekannt? Welche könnten bei der Digitalisierung der Leistung relevant werden?	[Wählen Sie eine Gefährdung/Schadenskategorie aus der Drop-down-Liste.]	[Bitte erläutern Sie die Gefährdung näher, indem Sie mind. einen möglichen Schadensfall beschreiben.]
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?	[Wählen Sie die passende Schadenshöhe aus der Drop-down-Liste.]	[Bitte begründen Sie Ihre Einschätzung zur Schadenshöhe.]
Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für einen Angriff auf die Daten- bzw. Dokumentenübermittlung? Wie groß ist die Wahrscheinlichkeit dafür?	[Wählen Sie die passende Eintrittswahrscheinlichkeit aus der Drop-down-Liste.]	[Bitte begründen Sie Ihre Einschätzung zur Eintrittswahrscheinlichkeit.]

Identifizierung

Übergreifende Frage:
Könnten bzw. würden sich Dritte mit falscher Identität authentisieren?

In Vorbereitung der Identifikation und Bewertung der Gefährdungen/Schadenskategorien zum Prozess Identifizierung machen Sie sich bitte zu folgenden Fragen Gedanken:

- Sind entsprechende Fälle bereits aus der Verwaltungspraxis (analoge Antragstellung) bekannt?
- Würde eine Authentisierung mit falscher Identität bemerkt werden?
- Mit welchen Schäden ist für den Betroffenen zu rechnen, wenn es einem Dritten gelingt, sich mit dessen Identität zu authentisieren?
- Hat der Betroffene mit erheblichem Aufwand für eine Richtigstellung der falschen Authentisierung zu rechnen?

Thema	Fragen	Antwort	Notizen
Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Identifizierung sind aus der Verwaltungspraxis bereits bekannt? Welche könnten bei der Digitalisierung der Leistung relevant werden?	[Wählen Sie eine Gefährdung/Schadenskategorie aus der Drop-down-Liste.]	[Bitte erläutern Sie die Gefährdung näher, indem Sie mind. einen möglichen Schadensfall beschreiben.]
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?	[Wählen Sie die passende Schadenshöhe aus der Drop-down-Liste.]	[Bitte begründen Sie Ihre Einschätzung zur Schadenshöhe.]
Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für eine Authentisierung mit falscher Identität? Wie groß ist die Wahrscheinlichkeit einer Authentisierung mit falscher Identität?	[Wählen Sie die passende Eintrittswahrscheinlichkeit aus der Drop-down-Liste.]	[Bitte begründen Sie Ihre Einschätzung zur Eintrittswahrscheinlichkeit.]

Willenserklärung

Übergreifende Frage:
Könnte bzw. würde ein Antragsteller die Abgabe einer Willenserklärung bestreiten?

In Vorbereitung der Identifikation und Bewertung der Gefährdungen machen Sie sich bitte zu folgender Frage Gedanken:

Thema	Fragen	Antwort	Notizen
Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Willenserklärung sind aus der Verwaltungspraxis bereits bekannt? Welche könnten bei der Digitalisierung der Leistung relevant werden?	[Wählen Sie eine Gefährdung/Schadenskategorie aus der Drop-down-Liste.]	[Bitte erläutern Sie die Gefährdung näher, indem Sie mindestens einen möglichen Schadensfall beschreiben.]
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?	[Wählen Sie die passende Schadenshöhe aus der Drop-down-Liste.]	[Bitte begründen Sie Ihre Einschätzung zur Schadenshöhe.]
Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für das Abstreiten der Abgabe einer Willenserklärung? Wie groß ist die Wahrscheinlichkeit dafür?	[Wählen Sie die passende Eintrittswahrscheinlichkeit aus der Drop-down-Liste.]	[Bitte begründen Sie Ihre Einschätzung zur Eintrittswahrscheinlichkeit.]

Bildung des Gesamtergebnisses

Übergreifende Frage:
Welches Vertrauensniveau ist unter Abwägung aller Gefährdungen und ihrer Risiken (gebildet aus Schadenshöhe und Schadenswahrscheinlichkeit) angemessen?

Gesamtergebnis	Begründung
[Bitte wählen Sie das Gesamtergebnis aus der Liste aus.]	[Bitte begründen Sie Ihre Gesamtbewertung.]

Schriftformerfordernis

Hinweise:

- Die bloße Verpflichtung, ein Antragsformular mit Unterschriftfeld zu verwenden, stellt noch kein Schriftformerfordernis dar (vgl. § 13 EGovG).
- Liegt ein Schriftformerfordernis vor, wird das Vertrauensniveau als "hoch +" bewertet. Dann kommt ein Schriftformersatz gem. § 3a Abs. 2 Nr. 1 VwVfG in Frage (Identifikation mit eID, entspricht dem Vertrauensniveau "hoch"). Zusätzlich sollte durch Auslegung der Rechtnorm und fachliche Bewertung des Geschäftsprozesses ermittelt werden, welche Funktionen der Schriftform genau benötigt werden. Die technische Richtlinie des BSI TR-03107-2 gibt Auskunft zu Bewertung und technischer Umsetzung.

Frage	Antwort	Notizen
Besteht für diesen Antrag ein gesetzliches Schriftformerfordernis?	Nein	
Falls ja, wo ist das Schriftformerfordernis verankert?	–	–

Daten-/Dokumentenübermittlung

Übergreifende Frage:
Könnten bzw. würden Dritte Einfluss auf die Daten-/Dokumentenübermittlung nehmen? Könnten bzw. würden sie Daten oder Dokumente abfangen und diese ggf. verändern?

In Vorbereitung der Identifikation und Bewertung der Gefährdungen/Schadenskategorien zum Prozess Daten-/Dokumentenübermittlung machen Sie sich bitte zu folgenden Fragen Gedanken:

- Wie sensibel sind die erfassten Daten und Dokumente?
- Handelt es sich um Daten ohne Personenbezug oder Daten, bei deren Offenlegung mit nur geringfügigen Auswirkungen für den Betroffenen zu rechnen ist?
- Handelt es sich um personenbezogene Daten?
- Falls ja, werden diese in größerem Umfang erhoben?
- Handelt es sich um personenbezogene Daten besonderer Kategorie gem. Art. 9 Abs. 1 DSGVO (Daten zur rassische und ethnische Herkunft, zu politische Meinungen, religiösen oder weltanschaulichen Überzeugungen oder Gewerkschaftszugehörigkeit hervorgehen, genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung)?
- Handelt es sich um andere schützenswerte Daten (Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, Personalaktendaten, Kontodaten, Daten zu strafbaren Handlungen und Ordnungswidrigkeiten, Steuerdaten, Sozialdaten, Daten zu Wahlausschlüssen oder Passversagungsgründe)?

Thema	Fragen	Antwort	Notizen
Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Daten- bzw. Dokumentenübermittlung sind aus der Verwaltungspraxis bereits bekannt? Welche könnten bei der Digitalisierung der Leistung relevant werden?	Verstoß gegen Gesetze/Vorschriften/Verträge	Es könnten durch Dritte personenbezogene Daten des Antragsstellers (insb. Anschrift und Telefonnummer) abgefangen werden.
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?	niedrig	Da es sich nicht um sehr sensible Daten handelt, ist der Schaden des Verstoßes eher gering.
Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für einen Angriff auf die Daten- bzw. Dokumentenübermittlung? Wie groß ist die Wahrscheinlichkeit dafür?	niedrig	Die abgreifbaren Daten sind auch auf anderem – wahrscheinlich einfacherem – Weg beschaffbar. Daher ist der Anrreiz für einen Angriff gering.
Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Daten- bzw. Dokumenten-übermittlung sind aus der Verwaltungspraxis bereits bekannt? Welche könnten bei der Digitalisierung der Leistung relevant werden?	Beeinträchtigung des informationellen Selbstbestimmungsrechts	Es könnten durch Dritte personenbezogene Daten des Antragsstellers (insb. Anschrift und Telefonnummer) abgefangen werden.
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?	niedrig	Da es sich nicht um sehr sensible Daten handelt, ist der Schaden eher gering.
Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für einen Angriff auf die Daten- bzw. Dokumentenübermittlung? Wie groß ist die Wahrscheinlichkeit dafür?	niedrig	Die abgreifbaren Daten sind auch auf anderem – wahrscheinlich einfacherem – Weg beschaffbar. Daher ist der Anrreiz für einen Angriff gering.

Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Daten- bzw. Dokumentenübermittlung sind aus der Verwaltungspraxis bereits bekannt? Welche könnten bei der Digitalisierung der Leistung relevant werden?	Negative Innen- oder Außenwirkung	Es könnten durch Dritte personenbezogene Daten des Antragsstellers (insb. Anschrift und Telefonnummer) abgefangen werden. In der Folge könnte es aufgrund von negativer medialer Aufmerksamkeit zu einem Vertrauensverlust gegenüber der Statd Leipzig und/oder dem betroffenen Online-Dienst kommen.
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?	niedrig	Da es sich nicht um sehr sensible Daten handelt, ist der Schaden eher gering.
Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für einen Angriff auf die Daten- bzw. Dokumentenübermittlung? Wie groß ist die Wahrscheinlichkeit dafür?	niedrig	Die abgreifbaren Daten sind auch auf anderem – wahrscheinlich einfacherem – Weg beschaffbar. Daher ist der Anrreiz für einen Angriff gering.
Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Daten- bzw. Dokumentenübermittlung sind aus der Verwaltungspraxis bereits bekannt?	Finanzielle Auswirkungen	Nach Offenlegung/Abfang von Daten könnten Schadenersatzzahlungen oder Bußgelder fällig werden.
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?	niedrig	Da es sich nicht um sehr sensible Daten handelt, ist der Schaden eher gering.
Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für einen Angriff auf die Daten- bzw. Dokumentenübermittlung? Wie groß ist die Wahrscheinlichkeit dafür?	niedrig	Die abgreifbaren Daten sind auch auf anderem – wahrscheinlich einfacherem – Weg beschaffbar. Daher ist der Anrreiz für einen Angriff gering.

Identifizierung

Übergreifende Frage:
Könnten bzw. würden sich Dritte mit falscher Identität authentisieren?

In Vorbereitung der Identifikation und Bewertung der Gefährdungen/Schadenskategorien zum Prozess Identifizierung machen Sie sich bitte zu folgenden Fragen Gedanken:

- Sind entsprechende Fälle bereits aus der Verwaltungspraxis (analoge Antragstellung) bekannt?
- Würde eine Authentisierung mit falscher Identität bemerkt werden?
- Mit welchen Schäden ist für den Betroffenen zu rechnen, wenn es einem Dritten gelingt, sich mit dessen Identität zu authentisieren?
- Hat der Betroffene mit erheblichem Aufwand für eine Richtigstellung der falschen Authentisierung zu rechnen?

Thema	Fragen	Antwort	Notizen
Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Identifizierung sind aus der Verwaltungspraxis bereits bekannt? Welche könnten bei der Digitalisierung der Leistung relevant werden?	Beeinträchtigung der Aufgabenerfüllung	Ein Dritter könnte sich mit falscher Identität authentisieren und einen Antrag stellen. Die Kapazitäten, die durch die Bearbeitung der Bestellung gebunden sind, könnten anderswo fehlen. Besonders bei Urkundenbestellungen in größerem Umfang könnte dies problematisch werden.
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?	niedrig	Der Bearbeitungsaufwand pro Antrag ist eher gering. Es ist nicht mit einer signifikanten Beeinträchtigung der Aufgabenerfüllung zu rechnen.
Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für eine Authentisierung mit falscher Identität? Wie groß ist die Wahrscheinlichkeit einer Authentisierung mit falscher Identität?	niedrig	Der Umstand, dass der Antrag eine Liste des Baumbestandes und eine Begründung des Antrags enthält, sowie eine Lageskizze bzw. ein Lageplan beigefügt werden müssen, macht eine Antragstellung (vor allem in größerem Umfang), mit dem Ziel Kapazitäten bei der Stadt zu binden, unwahrscheinlich. Soll mit der Antragstellung unter falschem Namen nur der Stadt Leipzig geschadet werden, bieten sich zudem anderswo größere Angriffsflächen.

Willenserklärung

Übergreifende Frage:
Könnte bzw. würde ein Antragsteller die Abgabe einer Willenserklärung bestreiten?

In Vorbereitung der Identifikation und Bewertung der Gefährdungen machen Sie sich bitte zu folgender Frage Gedanken:

Thema	Fragen	Antwort	Notizen
Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Willenserklärung sind aus der Verwaltungspraxis bereits bekannt? Welche könnten bei der Digitalisierung der Leistung relevant werden?	Negative Innen- oder Außenwirkung	Der Antragsteller könnte die Abgabe der Willenserklärung abstreiten und sich weigern, die Kosten für eine notwendige Ersatzpflanzug zu zahlen. In Folge könnte es zu einem Rechtsstreit kommen, der negative Presse nach sich zieht. Dadurch könnte ein Imageschaden für die Stadt entstehen.
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?	niedrig	Durch die geringe Bedeutung des Sachverhalts ist nur mit einer geringen Schadenshöhe zu rechnen.
Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für das Abstreiten der Abgabe einer Willenserklärung? Wie groß ist die Wahrscheinlichkeit dafür?	niedrig	Da sich die Umstände (stattgefundene Baumfällung) wahrscheinlich sehr leicht nachprüfen lassen, besteht kaum Anreiz zur Abstreitung der Willenserklärung.
Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Willenserklärung sind aus der Verwaltungspraxis bereits bekannt? Welche könnten bei der Digitalisierung der Leistung relevant werden?	Finanzielle Auswirkungen	Der Antragsteller könnte die Abgabe der Willenserklärung abstreiten und sich weigern, die Kosten für eine notwendige Ersatzpflanzug zu zahlen.
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?	niedrig	Die Kosten übersteigen einen geringen Umfang voraussichtlich nicht.
Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für das Abstreiten der Abgabe einer Willenserklärung? Wie groß ist die Wahrscheinlichkeit dafür?	niedrig	Da sich die Umstände (stattgefundene Baumfällung) wahrscheinlich sehr leicht nachprüfen lassen, besteht kaum Anreiz zur Abstreitung der Willenserklärung.

Bildung des Gesamtergebnisses

Übergreifende Frage:
Welches Vertrauensniveau ist unter Abwägung aller Gefährdungen und ihrer Risiken (gebildet aus Schadenshöhe und Schadenswahrscheinlichkeit) angemessen?

Gesamtergebnis	Begründung
normal	Es besteht ein geringes Risiko für alle identifizierten Gefährdungen: Es wurde keine Gefährdung mit einer Schadenshöhe über niedrig und keine Eintrittswahrscheinlichkeit über niedrig

Anhang 10 Ausgefüllte Arbeitshilfe für die Verwaltungsleistung Havariemeldung

Schriftformerfordernis

Hinweise:

- Die bloße Verpflichtung, ein Antragsformular mit Unterschriftfeld zu verwenden, stellt noch kein Schriftformerfordernis dar (vgl. § 13 EGovG).
- Liegt ein Schriftformerfordernis vor, wird das Vertrauensniveau als "hoch +" bewertet. Dann kommt ein Schriftformersatz gem. § 3a Abs. 2 Nr. 1 VwVfG in Frage (Identifikation mit eID, entspricht dem Vertrauensniveau "hoch"). Zusätzlich sollte durch Auslegung der Rechtnorm und fachliche Bewertung des Geschäftsprozesses ermittelt werden, welche Funktionen der Schriftform genau benötigt werden. Die technische Richtlinie des BSI TR-03107-2 gibt Auskunft zu Bewertung und technischer Umsetzung.

Frage	Antwort	Notizen
Besteht für diesen Antrag ein gesetzliches Schriftformerfordernis?	Nein	Auch aus den weiteren Regelungen (Gestattungs- und Konzessionsverträge, Rahmenverträge) ergibt sich kein Schriftformerfordernis (vgl. Kathrin Herz-Meinschenk, Sachgebietsleiterin Stadttechnische Koordinierung, Verkehrs- und Tiefbauamt, Stadt Leipzig, persönliche Kommunikation, 22.02.2022).
Falls ja, wo ist das Schriftformerfordernis verankert?	–	

Daten-/Dokumentenübermittlung

Übergreifende Frage:
Könnten bzw. würden Dritte Einfluss auf die Daten-/Dokumentenübermittlung nehmen? Könnten bzw. würden sie Daten oder Dokumente abfangen und diese ggf. verändern?

In Vorbereitung der Identifikation und Bewertung der Gefährdungen/Schadenskategorien zum Prozess Daten-/Dokumentenübermittlung machen Sie sich bitte zu folgenden Fragen Gedanken:

- Wie sensibel sind die erfassten Daten und Dokumente?
- Handelt es sich um Daten ohne Personenbezug oder Daten, bei deren Offenlegung mit nur geringfügigen Auswirkungen für den Betroffenen zu rechnen ist?
- Handelt es sich um personenbezogene Daten?
- Falls ja, werden diese in größerem Umfang erhoben?
- Handelt es sich um personenbezogene Daten besonderer Kategorie gem. Art. 9 Abs. 1 DSGVO (Daten zur rassische und ethnische Herkunft, zu politische Meinungen, religiösen oder weltanschaulichen Überzeugungen oder Gewerkschaftszugehörigkeit hervorgehen, genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung)?
- Handelt es sich um andere schützenswerte Daten (Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, Personalaktendaten, Kontodaten, Daten zu strafbaren Handlungen und Ordnungswidrigkeiten, Steuerdaten, Sozialdaten, Daten zu Wahlausschlüssen oder Passversagungsgründe)?

Thema	Fragen	Antwort	Notizen
Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Daten- bzw. Dokumenten-übermittlung sind aus der Verwaltungspraxis bereits bekannt? Welche könnten bei der Digitalisierung der Leistung relevant werden?	Beeinträchtigung der Aufgabenerfüllung	Dritte könnten Informationen zu Havarien, insbesondere aber die Pläne abfangen. Diese enthalten sensible Informationen zu kritischer Infrastruktur, die potenziell zur gezielten Manipulation dieser Infrastruktur eingesetzt werden könnten. Realisiert sich diese Gefahr in einem Schaden, könnte dadurch die Aufgabenerfüllung der Stadt Leipzig beeinträchtigt werden (z. B. Ausfall der Wasserversorgung).
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?	substanziell	Je nach abgegriffener Information könnten potenziell große Schäden eintreten.
Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für einen Angriff auf die Daten- bzw. Dokumentenübermittlung? Wie groß ist die Wahrscheinlichkeit dafür?	niedrig	Aus der Praxis sind keine entsprechenden Fälle bekannt (vgl. Kathrin Herz-Meinschenk, Sachgebietsleiterin Stadttechnische Koordinierung, Verkehrs- und Tiefbauamt, Stadt Leipzig, persönliche Kommunikation, 22.02.2022). Die potenziell abgreifbaren Daten und Dokumente sind auch auf anderem Wege (Versorgungsunternehmen, Bauunternehmen) verfügbar Angriffe auf die kritische Infrastruktur, die Schäden in ähnlicher Höhe verursachen könnten, sind auch ohne diese Informationen möglich, weshalb ein Angriff auf die Dokumentenübermittlung, der auf den Erhalt dieser Informationen abzielt, unwahrscheinlich ist.

Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Daten- bzw. Dokumenten-übermittlung sind aus der Verwaltungspraxis bereits bekannt? Welche könnten bei der Digitalisierung der Leistung relevant werden?	Negative Innen- oder Außenwirkung	Dritte könnten Informationen zu Havarien, insbesondere aber die Pläne abfangen. Diese enthalten sensible Informationen zu kritischer Infrastruktur. Gelangen Informationen dazu an die Öffentlichkeit, könnte dies ein Imageschaden für den Online-Dienst und die Stadt Leipzig zur Folge haben.
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?	niedrig	Es ist kein größerer Schaden zu erwarten, solange es sich bei einem Vorfall um einen Einzellfall handelt.
Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für einen Angriff auf die Daten- bzw. Dokumentenübermittlung? Wie groß ist die Wahrscheinlichkeit dafür?	niedrig	Aus der Praxis sind keine entsprechenden Fälle bekannt (vgl. Kathrin Herz-Meinschenk, Sachgebietsleiterin Stadttechnische Koordinierung, Verkehrs- und Tiefbauamt, Stadt Leipzig, persönliche Kommunikation, 22.02.2022). Die potenziell abgreifbaren Daten und Dokumente sind auch auf anderem Wege (Versorgungsunternehmen, Bauunternehmen) verfügbar, weshalb die Schadenswahrscheinlichkeit als sehr gering eingeschätzt wird.
Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Daten- bzw. Dokumenten-übermittlung sind aus der Verwaltungspraxis bereits bekannt?	Beeinträchtigung der persönlichen Unversehrtheit	Dritte könnten Informationen zu Havarien, insbesondere aber die Pläne abfangen. Diese enthalten sensible Informationen zu kritischer Infrastruktur, die potenziell zur gezielten Manipulation dieser Infrastruktur eingesetzt werden könnten. Realisiert sich diese Gefahr in einem Schaden, könnte dadurch die persönliche Unversehrtheit von einer oder mehrerer Personen beeinträchtigt werden (z. B. körperlicher Schaden durch verunreinigtes Trinkwasser).
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?	hoch	Es sind sowohl niedrige und substanzielle als auch hohe Schäden denkbar.
Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für einen Angriff auf die Daten- bzw. Dokumentenübermittlung? Wie groß ist die Wahrscheinlichkeit dafür?	niedrig	Aus der Praxis sind keine entsprechenden Fälle bekannt (vgl. Kathrin Herz-Meinschenk, Sachgebietsleiterin Stadttechnische Koordinierung, Verkehrs- und Tiefbauamt, Stadt Leipzig, persönliche Kommunikation, 22.02.2022). Die potenziell abgreifbaren Daten und Dokumente sind auch auf anderem Wege (Versorgungsunternehmen, Bauunternehmen) verfügbar. Angriffe auf die kritische Infrastruktur, die Schäden in ähnlicher Höhe verursachen könnten, sind auch ohne diese Informationen möglich, weshalb ein Angriff auf die Dokumentenübermittlung, der auf den Erhalt dieser Informationen abzielt, unwahrscheinlich ist.

Identifizierung

Übergreifende Frage:
Könnten bzw. würden sich Dritte mit falscher Identität authentisieren?

In Vorbereitung der Identifikation und Bewertung der Gefährdungen/Schadenskategorien zum Prozess Identifizierung machen Sie sich bitte zu folgenden Fragen Gedanken:

- Sind entsprechende Fälle bereits aus der Verwaltungspraxis (analoge Antragstellung) bekannt?
- Würde eine Authentisierung mit falscher Identität bemerkt werden?
- Mit welchen Schäden ist für den Betroffenen zu rechnen, wenn es einem Dritten gelingt, sich mit dessen Identität zu authentisieren?
- Hat der Betroffene mit erheblichem Aufwand für eine Richtigstellung der falschen Authentisierung zu rechnen?

Thema	Fragen	Antwort	Notizen
Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Identifizierung sind aus der Verwaltungspraxis bereits bekannt? Welche könnten bei der Digitalisierung der Leistung relevant werden?	Negative Innen- oder Außenwirkung	Ein Dritter könnte sich mit falscher Identität authentisieren und eine Havariemeldung abgeben. Daraufhin kommt es für Betroffenen zu Aufwand für die Richtigstellung der falschen Authentisierung. Das könnte zu individuellem Vertrauensverlust in das Online-Verfahren führen, oder – bei begleitender negativer medialer Aufmerksamkeit – zu breiterem Ansehensverlust.
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?	niedrig	Es ist kein größerer Schaden zu erwarten, solange es sich bei einem Vorfall um einen Einzelfall handelt.
Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für eine Authentisierung mit falscher Identität? Wie groß ist die Wahrscheinlichkeit einer Authentisierung mit falscher Identität?	niedrig	Aus der Praxis sind keine entsprechenden Fälle bekannt (vgl. Kathrin Herz-Meinschenk, Sachgebietsleiterin Stadttechnische Koordinierung, Verkehrs- und Tiefbauamt, Stadt Leipzig, persönliche Kommunikation, 22.02.2022). Außerdem erschwert der Umstand, dass zur Havariemeldung ein Lageplan eingereicht werden muss, der nichtöffentliche Informationen enthält, die Antragstellung durch fremde Dritte (vgl. Kathrin Herz-Meinschenk, Sachgebietsleiterin Stadttechnische Koordinierung, Verkehrs- und Tiefbauamt, Stadt Leipzig, persönliche Kommunikation, 22.02.2022).
Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Identifizierung sind aus der Verwaltungspraxis bereits bekannt? Welche könnten bei der Digitalisierung der Leistung relevant werden?	Beeinträchtigung der Aufgabenerfüllung	Ein Dritter könnte sich mit falscher Identität authentisieren und eine Havariemeldung abgeben. Die Kapazitäten, die durch die Bearbeitung (Prüfung, Nachforschung, Korrektur) der Havarimeldung gebunden sind, könnten anderswo fehlen. Besonders bei Havariemeldungen in größerem Umfang könnte dies problematisch werden.
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?	niedrig	Die Bearbeitungsdauer der einzelnen Havariemeldungen ist eher gering (vgl. Kathrin Herz-Meinschenk, Sachgebietsleiterin Stadttechnische Koordinierung, Verkehrs- und Tiefbauamt, Stadt Leipzig, persönliche Kommunikation, 22.02.2022).
Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für eine Authentisierung mit falscher Identität? Wie groß ist die Wahrscheinlichkeit einer Authentisierung mit falscher Identität?	niedrig	Aus der Praxis sind keine entsprechenden Fälle bekannt (vgl. Kathrin Herz-Meinschenk, Sachgebietsleiterin Stadttechnische Koordinierung, Verkehrs- und Tiefbauamt, Stadt Leipzig, persönliche Kommunikation, 22.02.2022). Außerdem erschwert der Umstand, dass zur Havariemeldung ein Lageplan eingereicht werden muss, der nichtöffentliche Informationen enthält, die Antragstellung durch fremde Dritte (vgl. Kathrin Herz-Meinschenk, Sachgebietsleiterin Stadttechnische Koordinierung, Verkehrs- und Tiefbauamt, Stadt Leipzig, persönliche Kommunikation, 22.02.2022).

Willenserklärung

Übergreifende Frage:
Könnte bzw. würde ein Antragsteller die Abgabe einer Willenserklärung bestreiten?

In Vorbereitung der Identifikation und Bewertung der Gefährdungen machen Sie sich bitte zu folgender Frage Gedanken:

Thema	Fragen	Antwort	Notizen
Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Willenserklärung sind aus der Verwaltungspraxis bereits bekannt? Welche könnten bei der Digitalisierung der Leistung relevant werden?	Finanzielle Auswirkungen	Kommt es durch eine unsachgemäße Havariebeseitigung zu einem Schaden, könnten die Kosten für dessen Beseitigung nicht beim Antragsteller geltend gemacht werden, wenn dieser die Abgabe der Willenserklärung abstreitet. Folgt daraufhin ein Rechtsstreit, könnte dies mit weiteren Kosten verbunden sein.)
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?	substanziell	Die maximale Schadenshöhe ist schlecht einschätzbar. Ein Schaden, dessen Höhe ein substanzielles Niveau übersteigt ist jedoch schwerlicht vorstellbar.
Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für das Abstreiten der Abgabe einer Willenserklärung? Wie groß ist die Wahrscheinlichkeit dafür?	niedrig	Aus der Praxis sind keine entsprechenden Fälle bekannt (vgl. Kathrin Herz-Meinschenk, Sachgebietsleiterin Stadttechnische Koordinierung, Verkehrs- und Tiefbauamt, Stadt Leipzig, persönliche Kommunikation, 22.02.2022). Außerdem erschwert der Umstand, dass zur Havariemeldung ein Lageplan eingereicht werden muss, der nichtöffentliche Informationen enthält, die Antragstellung durch fremde Dritte (vgl. Kathrin Herz-Meinschenk, Sachgebietsleiterin Stadttechnische Koordinierung, Verkehrs- und Tiefbauamt, Stadt Leipzig, persönliche Kommunikation, 22.02.2022).
Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Willenserklärung sind aus der Verwaltungspraxis bereits bekannt? Welche könnten bei der Digitalisierung der Leistung relevant werden?	Negative Innen- oder Außenwirkung	Kommt es durch eine unsachgemäße Havariebeseitigung zu einem Schaden, könnten die Kosten für dessen Beseitigung nicht beim Antragsteller geltend gemacht werden, wenn dieser die Abgabe der Willenserklärung abstreitet. Folgt daraufhin ein Rechtsstreit, könnte die begleitende negative mediale Aufmerksamkeit zu einem Vertrauens- und Ansehensverlust für die Stadt Leipzig und den betroffenen Online-Dienst führen.
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?	niedrig	Da es sich um einen isolierten Einzellfall handelt, ist mit keinem größeren Schaden zu rechnen.
Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für das Abstreiten der Abgabe einer Willenserklärung? Wie groß ist die Wahrscheinlichkeit dafür?	niedrig	Aus der Praxis sind keine entsprechenden Fälle bekannt (vgl. Kathrin Herz-Meinschenk, Sachgebietsleiterin Stadttechnische Koordinierung, Verkehrs- und Tiefbauamt, Stadt Leipzig, persönliche Kommunikation, 22.02.2022). Außerdem erschwert der Umstand, dass zur Havariemeldung ein Lageplan eingereicht werden muss, der nichtöffentliche Informationen enthält, die Antragstellung durch fremde Dritte (vgl. Kathrin Herz-Meinschenk, Sachgebietsleiterin Stadttechnische Koordinierung, Verkehrs- und Tiefbauamt, Stadt Leipzig, persönliche Kommunikation, 22.02.2022).

Bildung des Gesamtergebnisses

Übergreifende Frage:
Welches Vertrauensniveau ist unter Abwägung aller Gefährdungen und ihrer Risiken (gebildet aus Schadenshöhe und Schadenswahrscheinlichkeit) angemessen?

Gesamtergebnis	Begründung
normal	Es wurde zwar für einen Schadensfall eine mögliche Schadenshöhe von "hoch" festgestellt, da es sich dabei aber um einen indirekten Schaden handelt, der mehr der Vollständigkeit halber und mit Blick auf zukünftige Überprüfungen dieser Bewerungt dokumentiert wurde, wird die Entrittswahrscheinlichkeit als besonders gering eingeschätzt. Die eine andere Gefährdung für die die mögliche Schadenshöhe als "substanziell" bewertet wurde, führt durch die Eintrittswahrscheinlichkeit von "niedrig" nicht zu einer Gesamtbewertung über "normal".

Anhang 11 Ausgefüllte Arbeitshilfe für die Verwaltungsleistung Urkundenbestellung

Schriftformerfordernis

Hinweise:

- Die bloße Verpflichtung, ein Antragsformular mit Unterschriftfeld zu verwenden, stellt noch kein Schriftformerfordernis dar (vgl. § 13 EGovG).
- Liegt ein Schriftformerfordernis vor, wird das Vertrauensniveau als "hoch +" bewertet. Dann kommt ein Schriftformersatz gem. § 3a Abs. 2 Nr. 1 VwVfG in Frage (Identifikation mit eID, entspricht dem Vertrauensniveau "hoch"). Zusätzlich sollte durch Auslegung der Rechtnorm und fachliche Bewertung des Geschäftsprozesses ermittelt werden, welche Funktionen der Schriftform genau benötigt werden. Die technische Richtlinie des BSI TR-03107-2 gibt Auskunft zu Bewertung und technischer Umsetzung.

Frage	Antwort	Notizen
Besteht für diesen Antrag ein gesetzliches Schriftformerfordernis?	Nein	Kein gesetzliches Schriftformerfordernis (vgl. § 62 PStG). Aus der Prüfpflicht der Benutzungsberechtigung ergibt sich aber die Notwendigkeit, schriftliche Unterlagen vorliegen zu haben (vgl. Odette Steiner, Sachgebietsleiterin Urkundenstelle und Sterbefallbeurkundungen, Standesamt, Stadt Leipzig, persönliche Kommunikation, 16.03.2022)
Falls ja, wo ist das Schriftformerfordernis verankert?	–	

Daten-/Dokumentenübermittlung

Übergreifende Frage:
Könnten bzw. würden Dritte Einfluss auf die Daten-/Dokumentenübermittlung nehmen? Könnten bzw. würden sie Daten oder Dokumente abfangen und diese ggf. verändern?

In Vorbereitung der Identifikation und Bewertung der Gefährdungen/Schadenskategorien zum Prozess Daten-/Dokumentenübermittlung machen Sie sich bitte zu folgenden Fragen Gedanken:

- Wie sensibel sind die erfassten Daten und Dokumente?
- Handelt es sich um Daten ohne Personenbezug oder Daten, bei deren Offenlegung mit nur geringfügigen Auswirkungen für den Betroffenen zu rechnen ist?
- Handelt es sich um personenbezogene Daten?
- Falls ja, werden diese in größerem Umfang erhoben?
- Handelt es sich um personenbezogene Daten besonderer Kategorie gem. Art. 9 Abs. 1 DSGVO (Daten zur rassische und ethnische Herkunft, zu politische Meinungen, religiösen oder weltanschaulichen Überzeugungen oder Gewerkschaftszugehörigkeit hervorgehen, genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung)?
- Handelt es sich um andere schützenswerte Daten (Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, Personalaktendaten, Kontodaten, Daten zu strafbaren Handlungen und Ordnungswidrigkeiten, Steuerdaten, Sozialdaten, Daten zu Wahlausschlüssen oder Passversagungsgründe)?

Thema	Fragen	Antwort	Notizen
Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Daten- bzw. Dokumentenübermittlung sind aus der Verwaltungspraxis bereits bekannt? Welche könnten bei der Digitalisierung der Leistung relevant werden?	Verstoß gegen Gesetze/Vorschriften/Verträge	Personenbezogene Daten könnten offengelegt oder abgefangen werden.
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?	niedrig	Da die übermittelten Daten nicht besonders sensibel sind, kein großer Schaden zu erwarten.
Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für einen Angriff auf die Daten- bzw. Dokumentenübermittlung? Wie groß ist die Wahrscheinlichkeit dafür?	niedrig	Die Daten sind auch anderweitig verfügbar. Die Daten sind nicht in größerem Umfang abgreifbar, daher ist der Anreiz eher niedrig.
Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Daten- bzw. Dokumentenübermittlung sind aus der Verwaltungspraxis bereits bekannt? Welche könnten bei der Digitalisierung der Leistung relevant werden?	Beeinträchtigung des informationellen Selbstbestimmungsrechts	Personenbezogene Daten könnten offengelegt oder abgefangen werden.
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?	niedrig	Da die übermittelten Daten nicht besonders sensibel sind, kein großer Schaden zu erwarten. Allerdings könnten zu einzelnen Personen sehr viele persönliche Daten abgegriffen werden. Daher ist die Gefahr des Identitätsdiebstahls zu bedenken (siehe unten).
Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für einen Angriff auf die Daten- bzw. Dokumentenübermittlung? Wie groß ist die Wahrscheinlichkeit dafür?	niedrig	Die Daten sind auch anderweitig verfügbar. Die Daten sind nicht in größerem Umfang abgreifbar, daher ist der Anreiz eher niedrig.

Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Daten- bzw. Dokumentenübermittlung sind aus der Verwaltungspraxis bereits bekannt? Welche könnten bei der Digitalisierung der Leistung relevant werden?	Negative Innen- oder Außenwirkung	Die Offenlegung bzw. Abfang von Daten könnte negative mediale Aufmerksamkeit verursachen, die zu einem Verlust an Ansehen und Vertrauen führt. Kommt es zu einem Identitätsdiebstahl, der auf abgefangene Daten zurückzuführen ist, und infolgedessen zu negativer Presse, könnte der Imageschade schwerer wiegen.
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?	substanziell	Die Schadenshöhe ist schwer abschätzbar, wahrscheinlich eher gering; im Falle eines Identitätsdiebstahls höchstens substanziell.
Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für einen Angriff auf die Daten- bzw. Dokumentenübermittlung? Wie groß ist die Wahrscheinlichkeit dafür?	niedrig	Die Daten sind auch anderweitig verfügbar. Die Daten sind nicht in größerem Umfang abgreifbar, daher ist der Anreiz eher niedrig.
Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Daten- bzw. Dokumenten-übermittlung sind aus der Verwaltungspraxis bereits bekannt?	Finanzielle Auswirkungen	Nach Offenlegung/Abfang von Daten könnten Schadenersatzzahlungen oder Bußgelder fällig werden.
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?	niedrig	Die Schadenshöhe ist schwer abschätzbar, höchstwahrscheinlich aber tolerabel.
Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für einen Angriff auf die Daten- bzw. Dokumentenübermittlung? Wie groß ist die Wahrscheinlichkeit dafür?	niedrig	Die Daten sind auch anderweitig verfügbar. Die Daten sind nicht in größerem Umfang abgreifbar, daher ist der Anreiz eher niedrig.

Identifizierung

Übergreifende Frage:
Könnten bzw. würden sich Dritte mit falscher Identität authentisieren?

In Vorbereitung der Identifikation und Bewertung der Gefährdungen/Schadenskategorien zum Prozess Identifizierung machen Sie sich bitte zu folgenden Fragen Gedanken:

- Sind entsprechende Fälle bereits aus der Verwaltungspraxis (analoge Antragstellung) bekannt?
- Würde eine Authentisierung mit falscher Identität bemerkt werden?
- Mit welchen Schäden ist für den Betroffenen zu rechnen, wenn es einem Dritten gelingt, sich mit dessen Identität zu authentisieren?
- Hat der Betroffene mit erheblichem Aufwand für eine Richtigstellung der falschen Authentisierung zu rechnen?

Thema	Fragen	Antwort	Notizen
Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Identifizierung sind aus der Verwaltungspraxis bereits bekannt? Welche könnten bei der Digitalisierung der Leistung relevant werden?	Verstoß gegen Gesetze/Vorschriften/Verträge	Bei Authentisierung mit falscher Identität könnte eine Urkunde an einen Nicht-Berechtigten erteiilt werden, was einen Verstioß gegen § 62 Abs. 1 PStG darstellt.
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?		Die Schadenshöhe lässt sich schwer abschätzen.
Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für eine Authentisierung mit falscher Identität? Wie groß ist die Wahrscheinlichkeit einer Authentisierung mit falscher Identität?	niedrig	Aus der Verwaltungspraxis sind keine entsprechenden Fälle bekannt. Durch die Versendung per Nachnahme müsste eine Dritter auch in fremdem Namen Post empfangen, um an die Urkunden zu gelangen. Außerdem erschwert der Umstand, dass zur Antragstellung weitere Informationen (mind. Geburts-/Sterbe-/Eheschließungs-/Begründungsdatum und -ort) und ggf. Nachweise (Beziehung zur betroffenen Person, berechtigtes Interesse) nötig sind, die Antragstellung durch fremde Dritte. Die Angaben und Nachweise werden im Rahmen der Sachbearbeitung geprüft (vgl. Odette Steiner, Sachgebietsleiterin Urkundenstelle und Sterbefallbeurkundungen, Standesamt, Stadt Leipzig, persönliche Kommunikation, 14.03.2022).
Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Identifizierung sind aus der Verwaltungspraxis bereits bekannt? Welche könnten bei der Digitalisierung der Leistung relevant werden?	Beeinträchtigung der Aufgabenerfüllung	Ein Dritter könnte sich mit falscher Identität authentisieren und Urkunden bestellen. Die Kapazitäten, die durch die Bearbeitung der Bestellung gebunden sind, könnten anderswo fehlen. Besonders bei Urkundenbestellungen in größerem Umfang könnte dies problematisch werden. Da allerdings laufend entsprechende Statistiken gepflegt werden, würde Auffälligkeiten bemerkt werden (vgl. Odette Steiner, Sachgebietsleiterin Urkundenstelle und Sterbefallbeurkundungen, Standesamt, Stadt Leipzig, persönliche Kommunikation, 14.03.2022).
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?	niedrig	Der Bearbeitungsaufwand einer einzelnen Bestellung ist eher gering: in den meisten Fällen ca. 10 min. beim Sachbearbeitenden und 15 min. beim Standesbeamten; bei Fällen mit höherem Suchaufwand dauert die Sachbearbeitung bis zu 45 min (vgl. Odette Steiner, Sachgebietsleiterin Urkundenstelle und Sterbefallbeurkundungen, Standesamt, Stadt Leipzig, persönliche Kommunikation, 14.03.2022). Der Umfang der gebundenen Kapazität ist daher gering; die Aufgabenerfüllung nur minimalst beeinträchtigt.

Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für eine Authentisierung mit falscher Identität? Wie groß ist die Wahrscheinlichkeit einer Authentisierung mit falscher Identität?	niedrig	Für den Dritten ergibt sich aus der Bestellung unter falschem Namen kein Vorteil, da er die Urkunden nicht erhält. Daher ist der Anreiz gering. Soll mit der Bestellung unter falschem Namen nur der Stadt Leipzig geschadet werden, bieten sich anderswo größere Angriffsflächen. Außerdem erschwert der Umstand, dass zur Antragstellung weitere Informationen (mind. Geburts-/Sterbe-/Eheschließungs-/Begründungsdatum und -ort) und ggf. Nachweise (Beziehung zur betroffenen Person, berechtigtes Interesse) nötig sind, die Antragstellung durch fremde Dritte. Die Angaben und Nachweise werden im Rahmen der Sachbearbeitung geprüft (vgl. Odette Steiner, Sachgebietsleiterin Urkundenstelle und Sterbefallbeurkundungen, Standesamt, Stadt Leipzig, persönliche Kommunikation, 14.03.2022).
Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Identifizierung sind aus der Verwaltungspraxis bereits bekannt? Welche könnten bei der Digitalisierung der Leistung relevant werden?	Negative Innen- oder Außenwirkung	Ein Dritter könnte sich mit falscher Identität authentisieren und Urkunden bestellen. Derjenige, auf dessen Namen die Urkunden bestellt wurde, erhält die Unterlagen und soll per Nachnahme zahlen. Dies könnte zu Verwunderung und Empörung führen und schließlich zu einem Vertrauensverlust in den Online-Dienst und die Stadt Leipzig.
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?	niedrig	Es ist kein Schade in größerem Umfang zu erwarten, da es sich, wenn überhaupt, um einzelne Vorfälle handelt.
Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für eine Authentisierung mit falscher Identität? Wie groß ist die Wahrscheinlichkeit einer Authentisierung mit falscher Identität?	niedrig	Für den Dritten ergibt sich aus der Bestellung unter falschem Namen kein Vorteil, da er die Urkunden nicht erhält. Daher ist der Anreiz gering. Soll mit der Bestellung unter falschem Namen nur der Stadt Leipzig geschadet werden, bieten sich anderswo größere Angriffsflächen. Außerdem erschwert der Umstand, dass zur Antragstellung weitere Informationen (mind. Geburts-/Sterbe-/Eheschließungs-/Begründungsdatum und -ort) und ggf. Nachweise (Beziehung zur betroffenen Person, berechtigtes Interesse) nötig sind, die Antragstellung durch fremde Dritte. Die Angaben und Nachweise werden im Rahmen der Sachbearbeitung geprüft (vgl. Odette Steiner, Sachgebietsleiterin Urkundenstelle und Sterbefallbeurkundungen, Standesamt, Stadt Leipzig, persönliche Kommunikation, 14.03.2022).

Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Identifizierung sind aus der Verwaltungspraxis bereits bekannt? Welche könnten bei der Digitalisierung der Leistung relevant werden?	Finanzielle Auswirkungen	Ein Dritter könnte sich mit falscher Identität authentisieren und Urkunden bestellen. Nimmt derjenige, auf dessen Namen die Urkunden bestellt wurden, sie nicht ab, entsteht ein finanzieller Schaden.
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?	niedrig	Bei Bestellungen im gewöhnlichen Rahmen fallen keine hohen Kosten an; bei ungewöhnlich großen Bestellungen wird vor Bearbeitung Rücksprache mit dem Antragsteller gehalten (vgl. Odette Steiner, Sachgebietsleiterin Urkundenstelle und Sterbefallbeurkundungen, Standesamt, Stadt Leipzig, persönliche Kommunikation, 14.03.2022).
Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für eine Authentisierung mit falscher Identität? Wie groß ist die Wahrscheinlichkeit einer Authentisierung mit falscher Identität?	niedrig	Aktuell wird ca. einmal im Monat eine Bestellung nicht angenommen (vgl. Odette Steiner, Sachgebietsleiterin Urkundenstelle und Sterbefallbeurkundungen, Standesamt, Stadt Leipzig, persönliche Kommunikation, 14.03.2022). Für den Dritten ergibt sich aus der Bestellung unter falschem Namen kein Vorteil, da er die Urkunden nicht erhält. Daher ist der Anreiz gering. Soll mit der Bestellung unter falschem Namen nur der Stadt Leipzig geschadet werden, bieten sich anderswo größere Angriffsflächen. Außerdem erschwert der Umstand, dass zur Antragstellung weitere Informationen (mind. Geburts-/Sterbe-/Eheschließungs-/Begründungsdatum und -ort) und ggf. Nachweise (Beziehung zur betroffenen Person, berechtigtes Interesse) nötig sind, die Antragstellung durch fremde Dritte. Die Angaben und Nachweise werden im Rahmen der Sachbearbeitung geprüft (vgl. Odette Steiner, Sachgebietsleiterin Urkundenstelle und Sterbefallbeurkundungen, Standesamt, Stadt Leipzig, persönliche Kommunikation, 14.03.2022).

Willenserklärung

Übergreifende Frage:
Könnte bzw. würde ein Antragsteller die Abgabe einer Willenserklärung bestreiten?

In Vorbereitung der Identifikation und Bewertung der Gefährdungen machen Sie sich bitte zu folgender Frage Gedanken:

Thema	Fragen	Antwort	Notizen
Gefährdung/Schadens-kategorie	Welche Gefährdungen/Schadenskategorien für den Prozess Willenserklärung sind aus der Verwaltungspraxis bereits bekannt? Welche könnten bei der Digitalisierung der Leistung relevant werden?	Finanzielle Auswirkungen	Der Antragsteller könnte Bestellung abstreiten, die Sendung nicht annehmen und die Gebühr nicht bezahlen.
Schadenshöhe	Wie hoch schätzen Sie den möglichen Schaden ein?	niedrig	Bei Bestellungen im gewöhnlichen Rahmen fallen keine hohen Kosten an; bei ungewöhnlich großen Bestellungen wird vor Bearbeitung Rücksprache mit dem Antragsteller gehalten (vgl. Odette Steiner, Sachgebietsleiterin Urkundenstelle und Sterbefallbeurkundungen, Standesamt, Stadt Leipzig, persönliche Kommunikation, 14.03.2022).
Wahrscheinlichkeit des Schadenseintritts	Wie groß ist der Anreiz für das Abstreiten der Abgabe einer Willenserklärung? Wie groß ist die Wahrscheinlichkeit dafür?	niedrig	Aktuell wird ca. einmal im Monat eine Bestellung nicht angenommen (vgl. Odette Steiner, Sachgebietsleiterin Urkundenstelle und Sterbefallbeurkundungen, Standesamt, Stadt Leipzig, persönliche Kommunikation, 14.03.2022). Für den Antragsteller ergibt sich aus dem Abstreiten der Abgabe der Willenserklärung kein Vorteil, da er bei Ablehnung der Sendung die Urkunden nicht erhält. Daher ist der Anreiz gering. Soll mit der Nicht-Zahlung der anfallenden Gebühr nur der Stadt Leipzig geschadet werden, bieten sich anderswo größere Angriffsflächen.

Bildung des Gesamtergebnisses

Übergreifende Frage:
Welches Vertrauensniveau ist unter Abwägung aller Gefährdungen und ihrer Risiken (gebildet aus Schadenshöhe und Schadenswahrscheinlichkeit) angemessen?

Gesamtergebnis	Begründung
normal	Die durchweg als "niedrig" eingeschätzten Eintrittswahrscheinlichkeiten erlauben eine Gesamtbewertung von "normal". Die umfassenden Prüfungen, die bei dieser Leistung im Rahmen der Sachbearbeitung durchgeführt werden, und die Übermittlung der Urkunden per Nachname verringern das Missbrauchsrisiko.

Literaturverzeichnis

Adelskamp, Peter / Bastians, Uda / Krins, Tanja / Möwes, Sabine / Aegerter, Christian / Glock, Wolfgang / Mutter, Bernd: *Kommunalverwaltung weiterdenken – Perspektiven über das OZG hinaus*. Vortrag beim Fachkongress des IT-Planungsrates 2021, verfügbar unter: https://www.it-planungsrat.de/fileadmin/it-planungsrat/der-it-planungsrat/fachkongress/fachkongress_2021/Tag_2_Kommunaleverwaltung_weiterdenken.pdf [Zugriff am 20.03.2022].

Arbeitsgruppe „Attraktivität des E-Government“ des IT-Planungsrats / Kompetenzzentrum Öffentliche IT: *Abschlussbericht AG Attraktivität des E-Government*. Berlin, IT-Planungsrat 2015.

Berger, Ariane: Onlinezugangsgesetz und Digitalisierungsprogramm – Auf die Kommunen kommt es an! *Kommunaljurist*. Nr. 12 (2018), S. 441–445.

Beyer, Rolf: Das Backend nicht vergessen – Öffentliche IT zwischen Kooperation und Wettbewerb, Standardisierung und Freiraum. *Vitako aktuell*. Nr. 3 (2021).

buergerservice.org e. V. (Hrsg.): *Bessere Digitalisierung durch Einsatz der Online-Ausweisfunktion*. 2021, verfügbar unter: https://www.buergerservice.org/lib.medien/aktuell/20200901BessereDigitalisierung.pdf [Zugriff am 14.02.2022].

buergerservice.org e. V. (Hrsg.): *Über uns – Wir betreiben Wissensvermittlung zum Online Ausweisen für ein besseres digitales Gemeinwohl*. 2022, verfügbar unter: https://www.buergerservice.org/ueber-uns/ [Zugriff am 27.03.2022].

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *Technische Richtlinien*. 2021, verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/technische-richtlinien_node.html [Zugriff am 11.03.2022].

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *Lerneinheit 4.2: Schutzbedarfskategorien*. Berlin 2022, verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_4_Schutzbedarfsfeststellung/Lektion_4_02/Lektion_4_02_node.html [Zugriff am 17.02.2022].

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *Online-Kurs IT-Grundschutz – Lerneinheit 4.3: Vorgehen und Vererbung*. 2022, verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_4_Schutzbedarfsfeststellung/Lektion_4_03/Lektion_4_03_node.html [Zugriff am 17.03.2022].

Bundesministerium des Innern (Hrsg.): *Bericht der Bundesregierung zur Verzichtbarkeit der Anordnungen der Schriftform und des persönlichen Erscheinens im Verwaltungsrecht des Bundes*. Berlin 2016.

Bundesministerium des Innern und für Heimat (Hrsg.): *OZG-Leitfaden – Leitfaden zum Digitalisierungsprogramm des IT-Planungsrates*. Berlin 2020, verfügbar unter: https://leitfaden.ozg-umsetzung.de [Zugriff am 07.02.2022].

Bundesministerium des Innern und für Heimat (Hrsg.): *Das EfA-Prinzip einfach erklärt – Folge 1: Einführung zu „Einer für Alle“*. 2021, verfügbar unter: https://www.onlinezugangsgesetz.de/SharedDocs/videos/Webs/OZG/DE/EFA-videos/efa-video-1.html [Zugriff am 08.02.2020].

Bundesministerium des Innern und für Heimat (Hrsg.): *Einheitliches Unternehmenskonto auf ELSTER-Basis geht an den Start*. 2021, verfügbar unter: https://www.onlinezugangsgesetz.de/SharedDocs/kurzmeldungen/Webs/OZG/DE/2021/06_unternehmenskonto-startet.html [Zugriff am 11.03.2022].

Bundesministerium des Innern und für Heimat (Hrsg.): *Glossar für die OZG-Informationsplattform (Stand 25.03.2021)*. Berlin 2021.

Bundesministerium des Innern und für Heimat (Hrsg.): *Integrationsleitfaden Bund (Version 1.6)*. Berlin 2021.

Bundesministerium des Innern und für Heimat (Hrsg.): *Praxistool Vertrauensniveau*. Berlin 2021, verfügbar unter: https://vn-check.ozg-umsetzung.de/index.php/96979 [Zugriff am 10.02.2022].

Bundesministerium des Innern und für Heimat (Hrsg.): *Was ist das Reifegradmodell?* 2021, verfügbar unter: https://www.onlinezugangsgesetz.de/Webs/OZG/DE/grundlagen/info-ozg/info-reifegradmodell/info-reifegradmodell-node.html [Zugriff am 25.02.2022].

Bundesministerium des Innern und für Heimat (Hrsg.): *Was sind OZG-Leistungen?* Berlin 2021, verfügbar unter: https://www.onlinezugangsgesetz.de/Webs/OZG/DE/grundlagen/info-ozg/info-leistungen/info-leistungen-node.html [Zugriff am 08.02.2020].

Bundesministerium des Innern und für Heimat (Hrsg.): *OZG-Dashboard*. 2022, verfügbar unter: https://www.onlinezugangsgesetz.de/Webs/OZG/DE/umsetzung/ozg-dashboard/ozg-dashboard-node.html [Zugriff am 25.02.2022].

Bundesministerium des Innern und für Heimat: *OZG-Informationsplattform*. 2022, verfügbar unter: https://informationsplattform.ozg-umsetzung.de [Zugriff am 26.02.2022].

Bundesministerium des Innern, für Bau und Heimat (Hrsg.): *Das Nutzerkonto Bund – Verwaltungen von Bund, Ländern und Kommunen*. Berlin 2021.

Bundesministerium des Innern, für Bau und Heimat (Hrsg.): *Wegweiser „Einer für Alle/Viele“ Juni 2021 (Version 2.0)*. 2021.

Bundesregierung (Hrsg.): *Digitale Verwaltung 2020 – Regierungsprogramm 18. Legislaturperiode*. Berlin, Bundesministerium des Innern 2014.

CDU Sachsen / Bündnis 90/Die Grünen Sachsen / SPD Sachsen (Hrsg.): *Gemeinsam für Sachsen – Koalitionsvertrag 2019 bis 2024 – Erreichtes bewahren. Neues ermöglichen. Menschen verbinden*. Dresden 2019.

Denkhaus, Wolfgang / Richter, Eike / Bostelmann, Lars (Hrsg.): *E-Government-Gesetz/Onlinezugangsgesetz – Mit E-Government-Gesetzen der Länder und den Bezügen zum Verwaltungsrecht – Kommentar*. München, Beck 2019.

Europäische Kommission (Hrsg.): *eGovernment Benchmark 2017 – Taking stock of user-centric design and delivery of digital public services in Europe*. Brüssel 2017.

Europäische Kommission (Hrsg.): *eIDAS Levels of Assurance (LoA)*. Brüssel 2020, verfügbar unter: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Levels+of+Assurance [Zugriff am 10.02.2020].

Felden, Frank / Zelt, Thilo / Bauer, Patrick / Siegert, Sabine / Einaste, Taavi / Müller, Mario / Lume, Hendrik / Hoffmann, Till: *Zehn Jahre elektronischer Personalausweis: Wie Deutschland ein erfolgreiches eID-Ökosystem aufbauen kann*. 2020.

Flätgen, Timo: *1.000 Formerfordernisse im Landesrecht gestrichen – Das Saarländische Digitalisierungsgesetz als konkreter Beitrag zum Bürokratieabbau*. Vortrag vom 10. März 2022 beim 10. Fachkongress des IT-Planungsrats. 2022. verfügbar unter: https://www.it-planungsrat.de/fileadmin/it-planungsrat/der-it-planungsrat/fachkongress/fachkongress_2022/S1_Tag2_Flaetgen_Saarlaendisches_Digitalisierungsgesetzungsgesetz-.pdf [Zugriff am 17.03.2022].

Föderale IT-Kooperation (Hrsg.): *Leistungstyp 2/3 läuft aus – Neue Version der Codeliste*. 2021, verfügbar unter: https://fimportal.de/details?tx_news_pi1%5Baction%5D=detail&tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Bnews%5D=29&cHash=6199168649b7a766e5fbb0f1cd06fb96 [Zugriff am 20.03.2022].

Föderale IT-Kooperation (Hrsg.): *FIM-Glossar*. 2022, verfügbar unter: https://fimportal.de/glossar [Zugriff am 20.03.2022].

Föderale IT-Kooperation (Hrsg.): *FIT-Store*. 2022, verfügbar unter: https://www.fitko.de/fit-store [Zugriff am 26.02.2022].

Föderale IT-Kooperation (Hrsg.): *Föderales Informationsmanagement*. 2022, verfügbar unter: https://fimportal.de/ [Zugriff am 06.03.2022].

Freie Hansestadt Bremen (Hrsg.): *Übermittlung von Besucherkarten / Wochenkarten*. 2022, verfügbar unter: https://onlinedienste.bremen.de/Onlinedienste/Service/Entry/AFMParkBes [Zugriff am 20.03.2022].

Freistaat Sachsen (Hrsg.): *Strategie für IT und E-Government des Freistaates Sachsen*. Dresden 2014.

Fromm, Jens / Welzel, Christian / Nentwig, Lutz / Weber, Mike: *E-Government in Deutschland: Vom Absteig zum Aufstieg*. Kompetenzzentrum Öffentliche IT, Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS und Nationaler Normenkontrollrat (Auftraggeber) 2015.

Fromm, Jens / Welzel, Christian / Nentwig, Lutz / Weber, Mike / Ziesing, Jan Henrik / Martin, Philipp / Gumz, Jan Dennis / Hecht, Stefanie / Kuper, Susanna / Bruns, Lina / Mahler, Michél / Bieker, Lisa: *Bürokratieabbau durch Digitalisierung: Kosten und Nutzen von E-Government für Bürger und Verwaltung – Gutachten für den Nationalen Normenkontrollrat – Dokumentation*. Berlin, Kompetenzzentrum Öffentliche IT, Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS und Nationaler Normenkontrollrat (Auftraggeber) 2015.

Generaldirektion Kommunikationsnetze, Inhalte und Technologien, Europäische Kommission (Hrsg.): *Data Visualisation Tool*. Brüssel 2020, verfügbar unter: https://digital-agenda-data.eu [Zugriff am 07.02.2022].

Gerlach, Judith: *Beyond OZG!* Vortrag vom 10. März 2022 beim 10. Fachkongress des IT-Planungsrats. 2022.

Herrmann, Marco / Stöber, Karlheinz: Das Onlinezugangsgesetz des Bundes – Wie der Gang zum Amt überflüssig werden soll. *Neue Zeitschrift für Verwaltungsrecht*. Nr. 19 Jg. 36 (2017), S. 1401–1407.

Hoepner, Petra / Welzel, Christian / Wulff, Marianne: *Identifizierung und Authentifizierung leicht gemacht – Die Nutzer ins Zentrum stellen*. Berichte des NEGZ, Nr. 6. Berlin, Nationales E-Government Kompetenzzentrum e. V. 2019.

Initiative D21 e. V. (Hrsg.): *eGovernment MONITOR 2016: Nutzung und Akzeptanz digitaler Verwaltungsangebote – Deutschland, Österreich und Schweiz im Vergleich*. Berlin 2016.

IT-Planungsrat (Hrsg.): *Beschlüsse und Empfehlungen des IT-Planungsrates*. 2022, verfügbar unter: https://www.it-planungsrat.de/beschluesse [Zugriff am 11.03.2022].

IT-Planungsrat (Hrsg.): *Empfehlungen für die Zuordnung von Vertrauensniveaus in der Kommunikation zwischen Verwaltung und Bürgerinnen und Bürgern bzw. der Wirtschaft – Handreichung (Stand: 24.02.2020, Version 4.00)*. Berlin 2020.

Kreis Unna (Hrsg.): *Digitaler Masterplan – Digitalisierungsstrategie der Kreisverwaltung Unna – Zeitraum 2019–2022*. Unna 2019.

Kretschmer, Jürgen: Informationssicherheit bei der Umsetzung des Online-Zugangs-Gesetz (OZG) durch sächsische Kommunen. *Sachsenlandkurier*. Nr. 3 Jg. 32 (2021).

Lucke, Jörn von: *Portale für die öffentliche Verwaltung*. In: Martin Wind / Detlef Kröger (Hrsg.): *Handbuch IT in der Verwaltung*. *Handbuch IT in der Verwaltung*. Berlin / Heidelberg / New York, Springer 2006, S. 627–655.

Mann, Thomas / Sennekamp, Christoph / Uechtritz, Michael (Hrsg.): *Verwaltungsverfahrensgesetz – Großkommentar*. 2. Auflage, Baden-Baden, Nomos 2019.

Martens, Tarvi: Electronic identity management in Estonia between market and state governance. *Identity in the Information Society*. Nr. 1 Jg. 3 (2010), S. 213–233.

Martini, Mario: *Transformation der Verwaltung durch Digitalisierung*. Jan Ziekow (Hrsg.). Baden-Baden 2018.

Maurer, Hartmut / Waldhoff, Christian: *Allgemeines Verwaltungsrecht*. 19. Auflage, Grundrisse des Rechts. München, Beck 2017.

Ministerium des Innern und für Kommunales des Landes Brandenburg (Hrsg.): *Die Umsetzung des Onlinezugangsgesetzes – Ein praktischer Leitfaden für Land und Kommunen*. Potsdam 2020.

Ministerium des Innern und für Sport des Landes Rheinland-Pfalz (Hrsg.): *Digitale Verwaltung Rheinland-Pfalz – E-Government- und IT-Strategie des Landes Rheinland-Pfalz*. Mainz 2018.

Nationaler Normenkontrollrat (Hrsg.): *Bürokratieabbau. Bessere Rechtsetzung. Digitalisierung. Erfolge ausbauen – Rückstand aufholen – Jahresbericht 2017 des Nationalen Normenkontrollrates*. Berlin 2017.

Nationaler Normenkontrollrat (Hrsg.): *Monitor Digitale Verwaltung – 01.01.2018*. Berlin 2018.

Nationaler Normenkontrollrat (Hrsg.): *Monitor Digitale Verwaltung #2 – Mai 2019*. Berlin 2019.

Nationaler Normenkontrollrat (Hrsg.): *Monitor Digitale Verwaltung #3 – Oktober 2019*. Berlin 2019.

Nationaler Normenkontrollrat (Hrsg.): *Monitor Digitale Verwaltung #4 – September 2020*. Berlin 2020.

Nationaler Normenkontrollrat (Hrsg.): *Monitor Digitale Verwaltung #6 – September 2021*. Berlin 2021.

IT-Planungsrat / Land Sachsen-Anhalt (Hrsg.): *Handbuch LeiKa-plus – Version 1.3*. Berlin 2014.

Punz, Matthias: *Großzügige Zählweise bei neuem OZG-Dashboard*. 2020, verfügbar unter: https://background.tagesspiegel.de/digitalisierung/grosszuegige-zaehlweise-bei-neuem-ozg-dashboard [Zugriff am 25.02.2022].

Richter, Markus: *Eröffnung & Begrüßung*. Vortrag vom 9. März 2022 beim 10. Fachkongress des IT-Planungsrats. 2022.

Richter-Schuppan, Heiko: Schutzbedarf darf nicht mit Vertrauensniveau gleichgesetzt werden. *OZG-Newsletter*. (Aug. 2021).

Riedel, Jörn: *Identitäten als Schlüsselfaktor für medienbruchfreie digitale Prozesse*. In: Andreas Schmid (Hrsg.): *Verwaltung, eGovernment und Digitalisierung*. *Verwaltung, eGovernment und Digitalisierung*. Wiesbaden, Springer 2019, S. 23–30.

Roßnagel, Alexander: *Elektronische Schriftkommunikation (De-Mail, Vertrauensdienste)*. In: Sylvia Veit / Christoph Reichard / Göttrik Wewer (Hrsg.): *Handbuch zur Verwaltungsreform*. *Handbuch zur Verwaltungsreform*. 5. Aufl. Wiesbaden 2019, S. 617–628.

Sächsische Anstalt für kommunale Datenverarbeitung (Hrsg.): *Nutzungsvereinbarung*. 2018, verfügbar unter: https://www.sakd.de/index.php?id=e-gov-plattform_rv [Zugriff am 22.02.2022].

Sächsische Anstalt für kommunale Datenverarbeitung / Zweckverband Kommunale Informationsverarbeitung Sachsen / Sächsischer Städte- und Gemeindetag / Sächsischer Landkreistag (Hrsg.): *Leitfaden zur Umsetzung kommunaler OZG-Projekte in Sachsen*. Dresden 2019.

Sächsische Staatskanzlei (Hrsg.): *Schutzbedarfsfeststellung für die E-Government-Basiskomponenten und -Anwendungen*. 2016, verfügbar unter: https://extranet.egovernment.sachsen.de/schutzbedarfsfeststellung-3986.html [Zugriff am 22.02.2022].

Sächsische Staatskanzlei (Hrsg.): *Amt24*. 2017, verfügbar unter: https://www.egovernment.sachsen.de/amt24.html [Zugriff am 22.02.2022].

Sächsische Staatskanzlei (Hrsg.): *E-Government-Basiskomponenten mitnutzen*. 2017, verfügbar unter: https://www.egovernment.sachsen.de/vereinbarung-zur-mitnutzung-der-e-government-basiskomponenten-des-freistaates-sachsen-durch-die-saechsischen-kommunalverwaltungen-4074.html [Zugriff am 22.02.2022].

Sächsische Staatskanzlei (Hrsg.): *Masterplan Digitale Verwaltung Sachsen*. Dresden 2019.

Sächsische Staatskanzlei (Hrsg.): *Servicekonto*. 2019, verfügbar unter: https://www.egovernment.sachsen.de/servicekonto.html [Zugriff am 22.02.2022].

Sächsische Staatskanzlei (Hrsg.): *Verfahrensmanagement*. 2019, verfügbar unter: https://www.egovernment.sachsen.de/verfahrensmanagement-amt24-5347.html [Zugriff am 22.02.2022].

Sächsische Staatskanzlei (Hrsg.): *Kommunikation auf höchstem Sicherheitsniveau*. 2020, verfügbar unter: https://www.medienservice.sachsen.de/medien/news/238320 [Zugriff am 22.02.2022].

Sächsische Staatskanzlei (Hrsg.): *Amt24 – Servicekonto Anmeldung*. 2022, verfügbar unter: https://sso.amt24.sachsen.de/idp/profile/SAML2/Redirect/SSO?execution=e2s1 [Zugriff am 22.02.2022].

Sächsische Staatskanzlei / Seitenbau GmbH: *Amt24 – Das Serviceportal Sachsen*. Vortrag zum Tag der Fachverfahren zur OZG-Umsetzung in Sachsen am 30.01.2020. 2020, verfügbar unter: https://ozg.sakd.de/assets/files/05_20200130_TdFV_SK-Seitenbau.pdf [Zugriff am 22.02.2022].

Schaeff, Alexander: *Signal für Digitalisierung*. 2018, verfügbar unter: https://www.kommune21.de/meldung_30141.html [Zugriff am 25.02.2022].

Schnattinger, Thomas: Von Insellösungen zu einheitlichen Zugangsmöglichkeiten – Sicherheit von eID-Verfahren geprüft. *BSI-Magazin*. Nr. 2 (2019), S. 16–17.

Schönen, Rainer: Elektronische Identitäten auf dem Smartphone – Wie mobile Identitäten sicher verwendet werden können. *Mit Sicherheit*. Nr. 1 (2020), S. 24–25.

Schröder, Miriam: *OZG: Linke bemängelt fehlende Transparenz*. 2021, verfügbar unter: https://background.tagesspiegel.de/digitalisierung/ozg-linke-bemaengelt-fehlende-transparenz [Zugriff am 25.02.2022].

Schubert, Dino André: *Umsetzung des Onlinezugangsgesetzes bis Ende 2022 nicht mehr zu schaffen*. 2021, verfügbar unter: https://www.optiso-consult.de/umsetzung-des-onlinezugangsgesetzes-bis-ende-2022-nicht-mehr-zu-schaffen/ [Zugriff am 22.02.2022].

Schüür-Langkau, Anja: Zentrale Lösungen können Kommunen entlasten. *Innovative Verwaltung*. Nr. 5–6 (2021), S. 24–25.

Sobania, Kathrin: *Wirtschaftsfreundliches E-Government – Positionspapier*. Berlin / Brüssel, Deutscher Industrie- und Handelskammertag e. V. 2019.

Stadt Jena (Hrsg.): *Recherche im Ratssitzungssystem*. 2022, verfügbar unter: https://rathaus.jena.de/de/recherche-im-ratssitzungssystem [Zugriff am 27.03.2022].

Stadt Leipzig (Hrsg.): *eID-Station*. 2022, verfügbar unter: https://www.leipzig.de/buergerservice-und-verwaltung/aemter-und-behoerdengaenge/eid-station [Zugriff am 27.03.2022].

Stadt Leipzig (Hrsg.): *Erteilung von Besucherparkausweisen für die Bewohnerparkbereiche in der Stadt Leipzig*. 2022, verfügbar unter: https://www.leipzig.de/buergerservice-und-verwaltung/aemter-und-behoerdengaenge/behoerden-und-dienstleistungen/dienstleistung/erteilung-von-besucherparkausweisen-fuer-die-bewohnerparkbereiche-in-der-stadt-leipzig-nach-46-absatz-1-stvo-5dfc9c16d4eb8 [Zugriff am 20.03.2022].

Stadt Leipzig (Hrsg.): *Geburtsurkunde/Beglaubigte Abschrift aus dem Geburtenregister, Anforderung beim Standesamt (Geburt/Nachbeurkundung in Leipzig)*. 2022, verfügbar unter: https://amt24.sachsen.de/web/guest/leistung/-/sbw/GeburtsurkundeBeglaubigte+Abschrift+aus+dem+Geburtenregister+Anforderung+beim+Standesamt+GeburtNachbeurkundung+in+Leipzig-6000981-leistung-0/z-04288/a-14713000 [Zugriff am 17.03.2022].

Stadt Leipzig (Hrsg.): *Gehölzschnitt und Baumfällen beantragen*. 2022, verfügbar unter: https://amt24.sachsen.de/web/guest/leistung?p_p_id=zustaendigestelle_WAR_suchegui&p_p_lifecycle=0&p_r_p_-358194435_id=6002339&p_r_p_-358194435_t=leistung&p_r_p_-358194435_title=Gehoelzschnitt+und+Baumfaellen+beantragen&_zustaendigestelle_WAR_suchegui_tab=0&p_r_p_-358194435_plz=04288&_zustaendigestelle_WAR_suchegui_ags=14713000&_zustaendigestelle_WAR_suchegui_rq=04288+Leipzig%2C+Stadt [Zugriff am 17.03.2022].

Stadt Leipzig (Hrsg.): *Urkundenanforderung im Standesamt*. 2022, verfügbar unter: https://www.leipzig.de/buergerservice-und-verwaltung/lebenslagen-und-themen/urkundenanforderung-standesamt [Zugriff am 17.03.2022].

Stelkens, Paul / Bonk, Heinz Joachim / Leonhardt, Klaus: *Verwaltungsverfahrensgesetz: VwVfG – Kommentar*. Michael Sachs / Heribert Schmitz (Hrsg.). 9. Auflage, C. H. Beck 2018.

Stocksmeier, Dirk / Hunnius, Sirko: *OZG-Umsetzungskatalog – Digitale Verwaltungsleistungen im Sinne des Onlinezugangsgesetzes*. 1. Auflage, Version 0.98. Auflage, Berlin, Bundesministerium des Innern, für Bau und Heimat 2018.

Weber, Max: *Wirtschaft und Gesellschaft*. Tübingen 1922.

Weiße, Michaela / Martin, Matthias: Online-Antragsverfahren mit Dokumentenablage unter Anwendung des OZG-Leitfadens. *Sachsenlandkurier*. Nr. 3 Jg. 30 (2019), S. 141–144.

Wölbert, Christian / Bager, Jo / Gerber, Tim: Halbdigital – Digitalisierung der Verwaltung: eine Bestandsaufnahme. *c't*. Nr. 6 (2022), S. 60–64.

ZEIT ONLINE (Hrsg.): *Angebot digitaler Behördenleistungen soll verbessert werden*. 2021, verfügbar unter: https://www.zeit.de/news/2021-12/27/angebot-digitaler-behoerdenleistungen-soll-verbessert-werden [Zugriff am 22.02.2022].

Verzeichnis amtlicher Schriften

Abl. Jena 19/21 – Amtsblatt der Stadt Jena 19/21, 32. Jahrgang, vom 13. Mai 2021

BSI 200-1 – Standard des Bundesamtes für Sicherheit in der Informationstechnik 200-1: Managementsysteme für Informationssicherheit (ISMS)

BSI 100-2 – Standard des Bundesamtes für Sicherheit in der Informationstechnik 100-2: IT-Grundschutzmethodik [vor Oktober 2017]

BSI 200-2 – Standard des Bundesamtes für Sicherheit in der Informationstechnik 200-2: IT-Grundschutzmethodik [seit Oktober 2017]

BSI 200-3 – Standard des Bundesamtes für Sicherheit in der Informationstechnik 200-3: Risikomanagement

BT-Drs. 14/4987 – Drucksache des Deutschen Bundestages 14/4987 vom 14. Dezember 2000: Entwurf eines Gesetzes zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr

BT-Drs. 14/9000 – Drucksache des Deutschen Bundestages 14/9000 vom 13. Mai 2002: Entwurf eines Dritten Gesetzes zur Änderung verwaltungsverfahrensrechtlicher Vorschriften

BT-Drs. 17/10720 – Drucksache des Deutschen Bundestages 17/10720 vom 13. September 2012: Bericht der Bundesregierung nach Artikel 5 des Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften

BT-Drs. 17/1473 – Drucksache des Deutschen Bundestages 17/1473 vom 14. November 2012: Entwurf eines Gesetzes zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften c

BT-Drs. 18/9177 – Drucksache des Deutschen Bundestages 18/9177 vom 11. Juli 2016: Bericht der Bundesregierung zur Verzichtbarkeit der Anordnungen der Schriftform und des persönlichen Erscheinens im Verwaltungsrecht des Bundes

BT-Drs. 18/10183 – Drucksache des Deutschen Bundestages 18/10183 vom 2. November 2016: Entwurf eines Gesetzes zum Abbau verzichtbarer Anordnungen der Schriftform im Verwaltungsrecht des Bundes

BT-Drs. 18/11135 – Drucksache des Deutschen Bundestages 18/11135 vom 13. Februar 2017: Entwurf eines Gesetzes zur Neuregelung des bundesstaatlichen Finanzausgleichssystems ab dem Jahr 2020 und zur Änderung haushaltsrechtlicher Vorschriften

BT-Drs. 19/26311 – Drucksache des Deutschen Bundestages 19/26311 vom 29. Januar 2021: Schriftliche Fragen mit den in der Woche vom 25. Januar 2021 eingegangenen Antworten der Bundesregierung

ISO/IEC 29115:2013 – Standard Nr. 29115 der Internationalen Organisation für Normung, veröffentlicht 2013: Information technology – Security techniques – Entity authentication assurance framework

FIMLeiKaTypisierung 20210114 – Codes für Typisierungen von Leistungen des Leistungskatalogs (FIM Baustein Leistungen) vom 27. Januar 2021, herausgegeben durch die Geschäfts- und Koordinierungsstelle Förderales Informationsmanagement beim Ministerium der Finanzen des Landes Sachsen-Anhalt

LT-Drs. NRW 16/10379 – Drucksache des Landtags Nordrhein-Westfalen 16/10379 vom 2. Dezember 2015: Gesetzentwurf der Landesregierung – Gesetz zur Förderung der elektronischen Verwaltung in Nordrhein-Westfalen

LT-Drs. NI 17/3195 – Drucksache des Landtags Nordrhein-Westfalen 16/10379 vom 19. März 2015: Unterrichtung (zu Drs. 17/3110)

LT-Drs. RP 18/1908 – Drucksache des Landtags Rheinland-Pfalz 18/1908 vom 21. Dezember 2021: Unterrichtung durch die Landesregierung – Bericht der Landesregierung Rheinland-Pfalz zur Verzichtbarkeit der Anordnungen der Schriftform und des persönlichen Erscheinens in den verwaltungsrechtlichen Rechtsvorschriften des Landes Rheinland-Pfalz

LT-Drs. SL 16/1806 – Drucksache des Landtags des Saarlandes 16/1806 vom 6. Oktober 2021: Gesetzesentwurf der Regierung des Saarlandes – Gesetz zur Förderung der Digitalisierung durch Abbau von Formerfordernissen im Landesrecht des Saarlandes (Saarländisches Digitalisierungsgesetz – SDigG)

Plenarprotokoll [TH] 7/58 – Protokoll der 58. Sitzung des Thüringer Landtages, 7. Wahlperiode am 23.09.2021

NKR-Nr. 3703 – Stellungnahme des Nationalen Normenkontrollrates gem. § 6 Abs. 1 NKRG von 21. Juli 2016: Entwurf eines Gesetzes zum Abbau verzichtbarer Anordnungen der Schriftform im Verwaltungsrecht des Bundes

TR-03107-1 – Technische Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik: Elektronische Identitäten und Vertrauensdienste im E-Government – Teil 1: Vertrauensniveaus und Mechanismen

TR-03107-2 – Technische Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik: Elektronische Identitäten und Vertrauensdienste im E-Government – Teil 2: Schriftformersatz mit elektronischem Identitätsnachweis

VII-DS-01074-NF-01 – Neufassung Beschlussvorlage des Dezernats Stadtentwicklung und Bau der Stadt Leipzig VII-DS-01074-NF-01: Satzung der Stadt Leipzig über Erlaubnisse und Gebühren für Sondernutzungen an öffentlichen Straßen, Wegen und Plätzen (Sondernutzungssatzung) und der Entgeltordnung der Stadt Leipzig für die sonstige Benutzung öffentlicher Straßen

VII-DS-06203 – Beschlussvorlage des Dezernats Umwelt, Klima, Ordnung und Sport der Stadt Leipzig VII-DS-06203: Zweite Satzung zur Änderung der Baumschutzsatzung

Rechtsprechungsverzeichnis

BVerwG, Urteil vom 5. Juni 1974 – VIII C 1.74 –, BVerwGE 45, 189–197

Rechtsquellenverzeichnis

Abgabenordnung – in der Fassung der Bekanntmachung vom 1. Oktober 2002 (BGBl. I S. 3866; 2003 I S. 61), die zuletzt durch Artikel 33 des Gesetzes vom 5. Oktober 2021 (BGBl. I S. 4607) geändert worden ist

Bundesfernstraßengesetz – in der Fassung der Bekanntmachung vom 28. Juni 2007 (BGBl. I S. 1206), das zuletzt durch Artikel 11 des Gesetzes vom 10. September 2021 (BGBl. I S. 4147) geändert worden ist

Bundesnaturschutzgesetz – in der Fassung der Bekanntmachung vom 29. Juli 2009 (BGBl. I S. 2542), das zuletzt durch Artikel 1 des Gesetzes vom 18. August 2021 (BGBl. I S. 3908) geändert worden ist

Das Erste Buch Sozialgesetzbuch (SGB I) – Allgemeiner Teil – (Artikel I des Gesetzes vom 11. Dezember 1975, BGBl. I S. 3015), das zuletzt durch Artikel 32 des Gesetzes vom 20. August 2021 (BGBl. I S. 3932) geändert worden ist

Gästetaxesatzung der Stadt Leipzig (GTS) – Beschluss Nr. VI-DS-05645 der Ratsversammlung vom 27.09.2018 (Fortsetzung der Sitzung vom 19.09.2018), veröffentlicht im Leipziger Amtsblatt Nr. 18 vom 13. Oktober 2018, zuletzt geändert mit Beschluss Nr. VII-DS-00753-NF-01 der Ratsversammlung vom 09.07.2020 (Fortsetzung der Sitzung vom 08.07.2020), veröffentlicht im Leipziger Amtsblatt Nr. 14 vom 18.07.2020

Gesetz über die elektronische Verwaltung in Bayern (Bayerisches E-Government-Gesetz – BayEGovG) in der Fassung vom 22. Dezember 2015 (GVBl. [BY] S. 458)

Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) – vom 16. Mai 2001 (BGBl. I S. 876), in Kraft getreten am 22. Mai 2001 – außer Kraft getreten aufgrund Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) m. W. v. 29. Juli 2017

Außer Kraft getreten aufgrund Gesetzes vom 18.07.2017 (BGBl. I S. 2745) m.W.v. 29.07.2017 Außer Kraft

Gesetz zum Abbau verzichtbarer Anordnungen der Schriftform im Verwaltungsrecht des Bundes – in der Fassung der Bekanntmachung vom 29. März 2017 (BGBl. I S. 626)

Gesetz zum Abbau verzichtbarer Anordnungen der Schriftform im Verwaltungsrecht des Landes Sachsen-Anhalt – in der Fassung der Bekanntmachung vom 7. Juli 2020 (GVBl. LSA S. 372)

Gesetz zum Abbau verzichtbarer Formerfordernisse [des Landes Baden-Württemberg] – in der Fassung der Bekanntmachung vom 11. Februar 2020 (GBl. [BW] S. 37)

Gesetz zur Anpassung der Formanforderungen im Berliner Landesrecht (FormAnpassG) – in der Fassung der Bekanntmachung vom 15. Februar 2018 (GVBl. [BE] S. 160)

Gesetz zur Förderung der Digitalisierung durch Abbau von Formerfordernissen im Landesrecht des Saarlandes (Saarländisches Digitalisierungsgesetz – SDigG) – in der Fassung der Bekanntmachung vom 16. Dezember 2021 (Amtsbl. [SL] I S. 2629)

Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz – E-GovG) – in der Fassung der Bekanntmachung vom 25. Juli 2013 (BGBl. I S. 2749), das zuletzt durch Artikel 1 des Gesetzes vom 16. Juli 2021 (BGBl. I S. 2941) geändert worden ist

Gesetz zur Förderung der elektronischen Verwaltung im Freistaat Sachsen (Sächsisches E-Government-Gesetz – SächsEGovG) – in der Fassung der Bekanntmachung vom 8. November 2019 (SächsGVBl. S. 718), das zuletzt durch Artikel 3 der Verordnung vom 12. April 2021 (SächsGVBl. S. 517) geändert worden ist

Gesetz zur Förderung der elektronischen Verwaltung in Nordrhein-Westfalen (E-Government-Gesetz Nordrhein-Westfalen – EGovG NRW) – in der Fassung der Bekanntmachung vom 8. Juli 2016 (GV. NRW. S. 551), das zuletzt durch Artikel 1 des Gesetzes vom 30. Juni 2020 (GV. NRW. S. 644, 702) geändert worden ist

Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften – in der Fassung der Bekanntmachung vom 25. Juli 2013 (BGBl I S. 2749)

Gesetz zur Regelung des Verwaltungsverfahrens- und des Verwaltungszustellungsrechts für den Freistaat Sachsen – in der Fassung der Bekanntmachung vom 19. Mai 2010 (SächsGVBl. S. 142), das durch Artikel 3 des Gesetzes vom 12. Juli 2013 (SächsGVBl. S. 503) geändert worden ist

Gesetz zur Stärkung der medienbruchfreien Digitalisierung [des Landes Nordrhein-Westfalen] – Beschlossenes Gesetz Vorabdruck 17/196 27.01.2022 32 S.

Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG) in der Fassung der Bekanntmachung vom 14. August 2017 (BGBl. I S. 3122, 3138), das zuletzt durch Artikel 16 des Gesetzes vom 28. Juni 2021 (BGBl. I S. 2250) geändert worden ist

Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 u. 2 Satz 2 des Gesetzes vom 29. September 2020 (BGBl. I S. 2048) geändert worden ist

Landesgesetz zur Förderung der elektronischen Verwaltung in Rheinland-Pfalz (E-Government-Gesetz Rheinland-Pfalz – EGovGRP) – in der Fassung der Bekanntmachung vom 26. Oktober 2020 (GVBl. [RP] S. 573)

Personenstandsgesetz – in der Fassung der Bekanntmachung vom 19. Februar 2007 (BGBl. I S. 122), das zuletzt durch Artikel 3 des Gesetzes vom 4. Mai 2021 (BGBl. I S. 882) geändert worden ist

Sächsisches Naturschutzgesetz – in der Fassung der Bekanntmachung vom 6. Juni 2013 (SächsGVBl. S. 451), das zuletzt durch das Gesetz vom 9. Februar 2021 (SächsGVBl. S. 243) geändert worden ist

Sächsisches Straßengesetz – in der Fassung der Bekanntmachung vom 21. Januar 1993 (SächsGVBl. S. 93), das zuletzt durch Artikel 1 des Gesetzes vom 20. August 2019 (SächsGVBl. S. 762; 2020 S. 29) geändert worden ist

Saarländisches Gaststättengesetz (SGastG) – vom 13. April 2011 (Amtsbl. [SL] I S. 206), zuletzt geändert durch Artikel 23 des Gesetzes vom 8. Dezember 2021 (Amtsbl. [SL] I S. 2629)

Satzung der Stadt Leipzig über die Durchführung, Zulassung und Gebührenerhebung auf Wochen- und Spezialmärkten (Marktsatzung) – Beschluss Nr. VI-DS-04733 der Ratsversammlung vom 13.12.2017, (veröffentlicht im Leipziger Amtsblatt Nr. 23 vom 23.12.2017), zuletzt geändert am 07.10.2020 durch Beschluss Nr. VII-Ds-01122 (veröffentlicht im Leipziger Amtsblatt Nr. 19 vom 17.10.2020)

Satzung der Stadt Leipzig über Erlaubnisse und Gebühren für Sondernutzungen an öffentlichen Straßen, Wegen und Plätzen (Sondernutzungssatzung) – vom 11. November 2020

Satzung zum Schutz und zur Pflege des Baumbestandes der Stadt Leipzig (Baumschutzsatzung) – Beschluss Nr. 580/92 der Ratsversammlung vom 16.10.1992, veröffentlicht im Leipziger Amts-Blatt Nr. 3 vom 08.02.1993 – Änderung vom 20.02.2002, Beschluss Nr. III-979/02, Amtsblatt Nr. 6 vom 23.03.2002 – Änderung vom 09.02.2022, Beschluss Nr. VII-DS-06203, Amtsblatt vom 05.03.2022

Telekommunikationsgesetz – in der Fassung der Bekanntmachung vom 23. Juni 2021 (BGBl. I S. 1858), das zuletzt durch Artikel 8 des Gesetzes vom 10. September 2021 (BGBl. I S. 4147) geändert worden ist

Thüringer Gesetz zur Förderung der elektronischen Verwaltung (Thüringer E-Government-Gesetz – ThürEGovG) – in der Fassung der Bekanntmachung vom 10. Mai 2018 (GVBl. [TH] S. 212, ber. S. 294), das zuletzt durch Art. 2 des Gesetzes vom 23. November 2020 (GVBl. [TH] S. 562) geändert worden ist

Verordnung der Sächsischen Staatsregierung zur Durchführung des Sächsischen E-Government-Gesetzes (Sächsische E-Government-Gesetz-Durchführungsverordnung – SächsEGovGDVO) – in der Fassung der Bekanntmachung vom 13. Dezember 2016 (SächsGVBl. S. 664), die zuletzt durch die Verordnung vom 10. März 2020 (SächsGVBl. S. 93) geändert worden ist

Verordnung zur Gewährleistung der IT-Sicherheit der im Portalverbund und zur Anbindung an den Portalverbund genutzten IT-Komponenten (IT-Sicherheitsverordnung Portalverbund – ITSiV-PV)

Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates – in der Fassung der Bekanntmachung vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 S. 73)

Vertrag über die Arbeitsweise der Europäischen Union – Fassung aufgrund des am 1. Dezember 2009 in Kraft getretenen Vertrages von Lissabon (Konsolidierte Fassung bekanntgemacht im ABl. EG Nr. C 115 vom 9. Mai 2008, S. 47), zuletzt geändert durch die Akte über die Bedingungen des Beitritts der Republik Kroatien und die Anpassungen des Vertrags über die Europäische Union, des Vertrags über die Arbeitsweise der Europäischen Union und des Vertrags zur Gründung der Europäischen Atomgemeinschaft (ABl. EU L 112/21 vom 24.4.2012) m.W.v. 1. Juli 2013

Vertrauensdienstegesetz – in der Fassung vom 18. Juli 2017 (BGBl. I S. 2745), das durch Artikel 2 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist

Verwaltungsverfahrensgesetz für den Freistaat Sachsen – in der Fassung der Bekanntmachung vom 10. September 2003 (SächsGVBl. S. 614), das zuletzt durch Artikel 1 des Gesetzes vom 8. Dezember 2008 (SächsGVBl. S. 940) geändert worden ist

Verwaltungsverfahrensgesetz – in der Fassung der Bekanntmachung vom 23. Januar 2003 (BGBl. I S. 102), das zuletzt durch Artikel 24 Absatz 3 des Gesetzes vom 25. Juni 2021 (BGBl. I S. 2154) geändert worden ist

Verwaltungsverfahrensgesetz a. F. – in der Fassung der Bekanntmachung vom 23. Januar 2003 (BGBl. I S. 102)

Eidesstattliche Versicherung

Ich versichere hiermit an Eides Statt, dass ich die vorgelegte Bachelorarbeit selbständig verfasst, nur die angegebenen Quellen und Hilfsmittel benutzt sowie alle Stellen der Arbeit, die wörtlich oder sinngemäß aus anderen Quellen übernommen wurden, als solche kenntlich gemacht habe und die Bachelorarbeit in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorlegt wurde.

Die gedruckte und digitalisierte Version der Bachelorarbeit sind identisch.

Leipzig, 31.03.2021 Unterschrift