Heine, Moreen; Wessel, Daniel

E-Government und Datensouveränität – Einblicke und Lösungsansätze

HMD Praxis der Wirtschaftsinformatik

Provided in Cooperation with:
Springer Nature

Suggested Citation: Heine, Moreen; Wessel, Daniel (2021) : E-Government und Datensouveränität – Einblicke und Lösungsansätze, HMD Praxis der Wirtschaftsinformatik, ISSN 2198-2775, Springer Fachmedien Wiesbaden, Wiesbaden, Vol. 58, Iss. 5, pp. 1081-1091, https://doi.org/10.1365/s40702-021-00766-4

This Version is available at:
https://hdl.handle.net/10419/287580

HMD (2021) 58:1081–1091
https://doi.org/10.1365/s40702-021-00766-4

SCHWERPUNKT

E-Government und Datensouveränität – Einblicke und Lösungsansätze

Moreen Heine · Daniel Wessel

Eingegangen: 16. April 2021 / Angenommen: 17. Juli 2021 / Online publiziert: 19. August 2021

Zusammenfassung Die Digitalisierung hat alle Lebensbereiche erreicht – so auch den öffentlichen Sektor. Um bequeme E-Government-Angebote bereitstellen zu können, müssen bürgerbezogene Daten zwischen Verwaltungen geteilt werden. Gleichzeitig verfolgen viele Kommunen Smart-City-Strategien und sind dabei auch auf den Zugang zu Daten der Bürger angewiesen. Damit stellt die Digitalisierung und Digitale Transformation im öffentlichen Sektor zunehmend mehr Anforderungen an die Datensouveränität der Bürger. Im privaten Bereich geschieht dieses Teilen und die Weitergabe von Daten häufig unreflektiert oder wenig informiert. Zwar stimmen viele Personen zu, dass ihnen Datenschutz wichtig sei, diese Einstellung zeigt sich allerdings oft nicht im Verhalten (Privacy Paradox). Ziel des Beitrags ist es, basierend auf aktueller Forschung, für die Datensouveränität relevante Eigenschaften von Websites im privaten und öffentlichen Kontext anhand von exemplarischen Fällen zu beschreiben. Unterschieden wird dabei zwischen öffentlichen Angeboten (z. B. Bürgerportale von Kommunen), besonders regulierten Angeboten (z. B. Portale von Banken und Versicherungen) und privaten Angeboten, deren Geschäftsmodell darauf beruht, möglichst umfangreiche Daten über ihre Nutzer zu sammeln (z. B. Soziale Netzwerke). Ziel ist es, Eigenschaften der Websites zu erfassen, die Auswirkungen auf die Datensouveränität auf Nutzerseite haben können und Gestaltungsempfehlungen zur Erhöhung der Datensouveränität, insbesondere für den öffentlichen Sektor, abzuleiten.

Schlüsselwörter Datensouveränität · One-Stop-Government · E-Government · Mensch-Computer-Interaktion · Datenschutz

Moreen Heine (✉) · Daniel Wessel
Institut für Multimediale und Interaktive Systeme, Universität zu Lübeck, Lübeck, Deutschland
E-Mail: heine@imis.uni-luebeck.de

E-Government and Data Sovereignty – Insights and Solutions

Abstract Digitalisation has reached all areas of life—including the public sector. To provide convenient e-government services, citizen-related data must be shared between administrations. At the same time, many municipalities are pursuing smart city strategies and are dependent on access to citizen data. Digitalisation and digital transformation in the public sector are thus placing increasing demands on the data sovereignty of citizens. In the private sector, sharing and transmission of data often happen unthinkingly or while lacking information. Although many people agree that privacy is important to them, this attitude is often not reflected in their behaviour (privacy paradox). Based on current research, this article aims to describe the characteristics of websites relevant to data sovereignty in private and public contexts using illustrative cases. A distinction is made between public services (e.g., citizens' portals of municipalities), particularly regulated services (e.g., portals of banks and insurance companies), and private services whose business model is based on collecting as much data as possible about their users (e.g., social networks). The aim is to identify characteristics of the websites that can have an impact on data sovereignty on the user side and to derive design recommendations for increasing data sovereignty, especially for the public sector.

Keywords Data sovereignty · One-stop government · E-government · Human-computer interaction · Privacy

1 Einleitung

Digitalisierung durchdringt alle Lebensbereiche. Über vielfältige Geräte mit umfassender Sensorik und Anwendungen, zum Beispiel Smart Watches, geben Nutzer persönliche Daten preis. Mit Blick auf Lösungen und Konzepte zu *Once Only, One-Stop-Government* und *No-Stop-Government* sind auch öffentliche Verwaltungen Akteure, die zunehmend erfasste Daten weitergeben, um Nutzern Dienstleistungen bequem bereitstellen zu können. Einmal eingegebene Daten sollen nicht erneut abgefragt werden (*Once Only*). Anliegen sollen, unabhängig von behördlichen Zuständigkeiten an einem Kontaktpunkt erledigt werden können (*One-Stop-Government*) oder gar ganz ohne Antragstellung (*No-Stop-Government*), also auf Basis eines behördlich erfassten Ereignisses, bearbeitet werden. Ein häufig genanntes Beispiel hierfür ist die antragslose Familienhilfe in Österreich. Darüber hinaus basieren Entwicklungen und Initiativen im Bereich Smart-City ebenfalls auf einer umfassenden Erfassung und Verarbeitung von Daten, darunter auch personenbezogene Daten wie zum Beispiel Mobilitätsdaten oder Besucherdaten (z. B. in Bibliotheken oder Museen). Auf Basis solcher Daten sollen Ressourcen und Leistungen bedarfsgerecht und effizient zur Verfügung gestellt werden. Der fortschreitende E-Government- und Smart-City-Reifegrad ist daher mit hohen Anforderungen an Datensouveränität verbunden. Datensouveränität adressiert dabei die Wahlfreiheit, Selbstbestimmung, Selbstkontrolle und Sicherheit auf Seiten der Nutzer und damit die Fähigkeit, digitale Lösungen gemäß der eigenen Interessen und Wünsche zu nutzen, was sowohl bei der Verwen-

dung von E-Government-Anwendungen als auch im privaten Kontext relevant ist. Dieser Beitrag rückt die Anbieter in den Fokus, das heißt Verwaltungen und Unternehmen in vergleichender Perspektive. Welche Angebote gibt es in der Praxis auf Anbieterseite bereits, um Datensouveränität zu erhöhen? Wir betrachten, inwiefern es Unterschiede zwischen öffentlichen und privaten Anbietern von Online-Diensten gibt. Dabei unterscheiden wir Unternehmen in einem hoch regulierten Umfeld, darunter Banken und Versicherungen, von Unternehmen, deren Geschäftsmodell in hohem Maß auf Nutzerdaten basiert, zum Beispiel Soziale Netzwerke. Dieser Beitrag präsentiert auf Basis eines divergent-konvergenten Vorgehens Lösungsansätze zur Erhöhung von Datensouveränität. Im Folgenden werden Grundlagen zum Konzept der Datensouveränität dargelegt. Es folgen Ausführungen zum Vorgehen sowie die Darstellung und Diskussion der Ergebnisse.

2 Datensouveränität

Digitale Souveränität im E-Government wird aus unterschiedlicher Perspektive diskutiert. Dabei wird neben der Souveränität des Bürgers auch die Digitale Souveränität auf Seiten des Staates und einzelner Verwaltungen erörtert – zum Beispiel in Bezug auf die Rolle öffentlicher Rechenzentren, die Abhängigkeit von Software-Anbietern, oder auch auf die Frage, inwiefern Digitale Souveränität trotz der umfangreichen Anforderungen an integrierte Datenbestände aus E-Government-Sicht sichergestellt werden kann (vgl. Friedrichsen und Bisa 2016). Zusammengefasst meint Digitale Souveränität das selbstbestimmte Handeln und Entscheiden von Personen, Organisationen und Staaten im digitalen Raum (Krupka 2020). Die Förderung von digitaler Souveränität erfordert die Betrachtung der drei voneinander abhängigen Handlungsfelder *digitaler Kompetenz, Technologie* und *Regulierungen* (vgl. SVRV 2017). Der Fokus dieses Beitrags liegt auf der Souveränität von Individuen, die E-Government-Dienste nutzen und dabei insbesondere auf Datensouveränität in Bezug auf Websites.

Im privaten Nutzungskontext erfolgt das Teilen und die Weitergabe von Daten häufig bedenkenlos oder gar unwissend, insbesondere was die möglichen Konsequenzen betrifft. Das betrifft unter anderem die Beeinflussung von Erleben und Verhalten, zum Beispiel mit Blick auf Kaufentscheidungen durch personalisierte Werbung. Zwar stimmen viele Personen zu, dass ihnen Datenschutz wichtig sei, diese Einstellung zeigt sich allerdings oft nicht im Verhalten (Privacy Paradox). Daten werden häufig unreflektiert geteilt und Nutzungsrichtlinien oft ungelesen akzeptiert (Gerber et al. 2018).

Im Vergleich zwischen behördlichem und privatem Kontext sind durchaus Unterschiede festzustellen. Öffentliche Verwaltungen erheben und verarbeiten unter anderem besonders sensible Daten zum Einkommen, der Gesundheit, der Familie und zu Ordnungswidrigkeiten oder gar Straftaten. Privatunternehmen hingegen verfügen über umfangreiche Daten zur Nutzung von Anwendungen, Kaufpräferenzen, Interessen, Kontakten sowie über Texte, Bilder, Videos und Bewegungsdaten. Je nach Geschäftsfeld fallen auch im privaten Kontext Finanz- und Gesundheitsdaten an. Im privaten Kontext besteht in der Regel die Wahl, bestimmte Angebote überhaupt zu

nutzen oder einen Anbieter auszuwählen. Im öffentlichen Sektor ist dies nicht oder nur unter Einbußen in der Versorgung mit staatlichen Leistungen möglich. Daraus lässt sich durchaus eine besondere Sorgfaltspflicht und Verantwortung hinsichtlich geeigneter Maßnahmen zur Gewährleistung und Erhöhung der Datensouveränität ableiten. Bizer (2019) sieht neben staatlichen Einrichtungen auch Bildungseinrichtungen, Unternehmen, Zivilgesellschaft und Non-Profit-Organisationen als relevante Akteure. Dieser Beitrag fokussiert auf den jeweiligen Diensteanbieter.

Zur Erzielung von Datensouveränität sind sowohl digitale Kompetenzen, Eigenschaften der eingesetzten Anwendungen und Technologien sowie Regulierungen zu adressieren (orientiert an SVRV 2017; Gräf et al. 2018).

Diese drei Handlungsfelder betreffen alle Akteure. Auch Unternehmen können Angebote zur Kompetenzerhöhung und unternehmensweite Regelungen umsetzen.

2.1 Kompetenzen

Mit dem europäischen Referenzrahmen für digitale Kompetenz (DigCom) existiert ein Raster, das als Basis für nötige Kenntnisse und Fähigkeiten für einen souveränen Umgang mit Online-Diensten dienen kann (Vourikari et al. 2016). Der Referenzrahmen umfasst zum Beispiel die Einschätzung der Glaubwürdigkeit von Angeboten, den Schutz der eigenen Reputation und den Schutz persönlicher Daten. In diesem Zusammenhang ist auch Medienkompetenz relevant. Hier wird unter anderem *Information Literacy* (Fähigkeit zum kompetenten Umgang mit Informationen) und *Online Privacy Literacy* (Fähigkeit zum kompetenten Schutz der eigenen Privatsphäre in Online-Umgebungen) adressiert (Masur et al. 2017). Auch im E-Government werden Maßnahmen zur Erhöhung der Medienkompetenz als Voraussetzung für eine erfolgreiche Nutzung und Akzeptanz der Anwendungen und Dienste diskutiert (Czernohorsky und Weiler 2012) – wobei Angebote zur Erhöhung der Medienkompetenz eng mit Situationen verbunden sein sollen, in denen genau solche Kompetenzen erforderlich sind, zum Beispiel direkt bei der Nutzung von E-Government-Diensten. Denkbar sind hier kompakte Informationen, zum Beispiel in Form von Texten oder Videos, die begleitend zum E-Government-Dienst angeboten werden. Mit Blick auf den *Digital Divide* stehen Ansätze zur Messung von Medienkompetenz im E-Government-Kontext zur Verfügung (Bergquist et al. 2017). Der Begriff *Digital Divide* adressiert Unterschiede im Zugang und in der Nutzung digitaler Infrastruktur und digitaler Angebote und basiert auf verschiedenen Faktoren, zum Beispiel dem Einkommensniveau, die im Rahmen von Angeboten zum Kompetenzaufbau zu berücksichtigen sind (Helbig et al. 2009). Neben Kompetenzen sind auch Einstellungen zu berücksichtigen, zum Beispiel wie gerne und intensiv jemand mit Technik interagieren möchte (Technikaffinität der Nutzer, Franke et al. 2019).

2.2 Technologische Lösungsansätze

Vertraulichkeit, Privatsphäre und Datenschutz können als Grundbestandteile in Kommunikationssysteme integriert werden, indem Forderungen nach *privacy by design* und *privacy by default* umgesetzt werden (SVRV 2017). *Privacy by design* umfasst Grundsätze bei der Gestaltung von Systemen, die einen proaktiven Datenschutz

ermöglichen (vgl. Rost und Bock 2011). Unter anderem soll der Schutz der Privatsphäre ganzheitlich in Systeme integriert werden, ohne deren Funktionalität zu beeinträchtigen. Ein Beispiel dafür ist die stets verschlüsselte Übermittlung personenbezogener Daten. *Privacy by default* ist ein weiterer Grundsatz von *privacy by design*. Gefordert wird, dass die Standardeinstellungen das höchste Maß an Privatsphäre und Datenschutz gewährleisten. Ein konzeptionelles Rahmenwerk zur Abbildung Digitaler Souveränität in Softwaresystemen weitet den Ansatz *privacy by design* auf Datensouveränität aus und fokussiert dabei auf die Portabilität von Daten zwischen Anwendungen, die Nachverfolgbarkeit der eigenen Daten, die Einflussnahme auf die Datennutzung und die Löschung von Daten (Diepenbrock und Sachweh 2018).

2.3 Regulation

Mit Blick auf die rechtlichen Rahmenbedingungen stellt der Datenschutz eine dominante Rahmenbedingung für die E-Government-Entwicklung in Deutschland dar (Hunnius et al. 2016). Eine hohe Digitale Souveränität könnte hier zu einer Versachlichung der Diskussion um die Abwägung zwischen effizienten E-Government-Prozessen und individueller Datensouveränität führen. Die Europäische Datenschutzgrundverordnung regelt unter anderem die Informationspflichten zur Verarbeitung personenbezogener Daten und schreibt eine präzise und verständliche Form für die Informationsvermittlung vor. Demgegenüber wird bei der Information über die Nutzungsbedingungen von Online-Diensten die Textlänge und Textverständlichkeit bemängelt (Derguech et al. 2018). Sie werden selten gelesen und ihnen wird oft unkritisch zugestimmt (Tabassum et al. 2018). Mögliche Lösungen zu einer kritischen Auseinandersetzung betreffen die Nutzung von *privacy languages* (Zhao et al. 2016) oder *privacy icons*. Beide Ansätze versuchen, die Verständlichkeit von Datenschutzeinstellungen zu verbessern und die Nutzer in die Lage zu versetzen, ihre Präferenzen korrekt auszudrücken. Auch die Eignung andere graphischer Darstellungen wird diskutiert (z. B. die Verwendung von Comics, vgl. Tabassum et al. 2018).

Es zeigt sich, dass für die drei Handlungsfelder Kompetenzen, Technologie und Regulation vielversprechende Lösungsansätze bestehen. Es stellt sich die Frage, welche Maßnahmen die Anbieter ergreifen.

3 Vorgehen

Die Lösungsfindung im vorliegenden Beitrag basiert auf einer zunächst divergenten Phase mit unterschiedlichen Perspektiven, der eine konvergente Phase folgt (Nestler et al. 2020), die vorhandene Literatur zu Datensouveränität und Datenschutz im Kontext menschzentrierter Gestaltung nutzt. Die divergente Phase basiert auf Arbeiten von Studierenden im Bachelor-Studiengang Medieninformatik, die im 5. Fachsemester bereits über fortgeschrittene Kenntnisse in der Mensch-Computer-Interaktion verfügen. Auf diese Weise wird das Potenzial mehrerer Beteiligter ausgeschöpft. Die Studierenden haben Online-Dienste in den gegebenen drei Kategorien (öffent-

liche Verwaltungen, Unternehmen im hoch regulierten Umfeld und Unternehmen mit datenbasiertem Geschäftsmodell) selbst ausgewählt. War eine Kategorie bereits mit ausreichend Beispielen abgedeckt, konnte sie nicht mehr gewählt werden. Untersucht wurden elf Websites öffentlicher Verwaltungen, sieben Websites von Unternehmen im hochregulierten Umfeld und zehn Websites von Unternehmen mit datenbasiertem Geschäftsmodell. Hier ist zu beachten, dass die Studierenden die Aufgabe hatten, Verbesserungen hinsichtlich der Datensouveränität zu erarbeiten. Daher wurden womöglich Beispiele gewählt, die offensichtliche Mängel aufweisen. Auf Grundlage einer Literaturrecherche und den daraus gewonnenen Erkenntnissen haben die Studierenden die Online-Dienste hinsichtlich Schwächen zur Datensouveränität untersucht. Anschließend haben die Studierenden Gestaltungsempfehlungen zur Erhöhung der Datensouveränität erarbeitet. Auf diese Weise entstanden 28 unterschiedliche Lösungsansätze. Ein Großteil der Lösungen (16) beschäftigte sich mit Cookies. Außerdem standen Informationen zum Datenschutz im Fokus, zum Beispiel mittels *FAQ (Frequently Asked Questions)*, Visualisierung oder auch mit Blick auf die Lesbarkeit von Datenschutzhinweisen (5). Für Privatsphäre-Einstellungen wurden virtuelle Assistenten, Datenschutzportale und *Dashboards* betrachtet (6). Eine weitere Arbeit beschäftigte sich mit der Identifikation von *Phishing* und eine andere Arbeit mit der Identifikation von *Dark Patterns* durch ein Browser-Plug-In. Die Lösungen wurden durch die Studierenden mittels eines standardisierten Online-Fragebogens bewertet. Die Lösungen wurden im Kurs präsentiert und von zwei bis sieben Studierenden auf Basis des Inhalts beurteilt. Die Lösungen im oberen Drittel der Bewertung wurden jeweils von mindestens vier Personen mit einer Punktzahl höher als 80 (von maximal 100 Punkten) bewertet und für die konvergente Phase ausgewählt. In der konvergenten Phase wurden diese neun Lösungen (Umgang mit Cookies (vier Ansätze), Visualisierung, Phishing-Identifikation, Datenschutz-Dashboard, virtuelle Assistenz, FAQ) durch die Autoren auf Basis des Forschungsstandes zu Datensouveränität in der menschzentrierten Gestaltung kategorisiert und kritisch gewürdigt. Ausgewählte Lösungsansätze werden in diesem Beitrag präsentiert, wobei die Qualität und die Visualisierung des Lösungsansatzes bei der Zusammenstellung im Fokus standen. Die folgenden Ergebnisse basieren daher auf exemplarischen Beobachtungen in der Praxis und umfassen Lösungsansätze, die auf Grundlage ausgewählter wissenschaftlicher Studien entwickelt wurden. Die jeweiligen Studien werden im Zug der Vorstellung der Lösungsansätze genannt.

4 Ergebnisse

Im Rahmen der Betrachtung der exemplarisch ausgewählten Diensteanbieter konnte kein Unterschied zwischen den einzelnen Akteursgruppen beobachtet werden. Die Online-Services öffentlicher Verwaltungen und Unternehmen im hoch regulierten Umfeld zeichnen sich nicht durch besondere Maßnahmen zur Erhöhung der Datensouveränität auf Seiten der Nutzer aus. Mängel mit Blick auf die Datensouveränität traten bei allen Anbietern auf. Ein Ansatzpunkt kann sein, dass gleiche Dienstleister beauftragt und gleiche Werkzeuge genutzt werden und Mängel auf diese Weise unabhängig von der anbietenden Organisation auftreten. Es zeigt aber auch, dass

die notwendige Sorgfaltspflicht und Verantwortung der Organisationen zum Umgang mit Nutzerdaten zumindest auf Ebene der jeweiligen Websites, die Online-Dienste anbieten, in den betrachteten Fällen nicht sichtbar ist – auch nicht bei denen des öffentlichen Sektors. Maßnahmen im Bereich Kompetenzen hat keiner der untersuchten Anbieter ergriffen.

Auf Basis einer Literaturrecherche durch die Studierenden wurden Ansatzpunkte für Schwächen und Herausforderungen bei der Sicherstellung von Datensouveränität bei Online-Diensten identifiziert. *Dark Patterns* (Geronimo et al. 2020) stellten einen häufigen Ausgangspunkt für die Analyse dar. Dabei werden Nutzerschnittstellen so gestaltet, dass das Verhalten der Nutzer zum Vorteil der Diensteanbieter manipuliert wird. Ein typisches Beispiel ist die Cookie-Abfrage, die meist so gestaltet wird, dass die Option für das Akzeptieren aller Cookies besonders hervorgehoben wird. Cookies ermöglichen es, Nutzer bei erneutem Besuch zu identifizieren und Daten über das Nutzungsverhalten zu erheben. Dies bildet auch die Grundlage für spezifische – auch erwünschte – Funktionen (z. B. die Verfügbarkeit des Warenkorbs bei einem erneuten Besuch). Der Grundsatz *privacy by default* wird bei Cookie-Abfragen überwiegend nicht berücksichtigt, auch nicht von den untersuchten öffentlichen Anbietern. Vor diesem Hintergrund sind Suggestivformulierungen, wie zum Beispiel „Kurz zustimmen für eine optimale Nutzung“ zu vermeiden. Abb. 1 zeigt ein Beispiel mit manipulativ wirkender Gestaltung der Interaktionsmöglichkeiten und den entwickelten Lösungsansatz ohne *Dark Pattern*. Daneben wurde in weiteren Lösungsansätzen ergänzende Gestaltungsempfehlungen für die Cookie-Einstellungen erarbeitet. Die Positionierung des entsprechenden Banners erfolgt im Idealfall am unteren linken Bildschirmrand, um eine möglichst hohe Interaktion zu erreichen (vgl. Utz et al. 2019).

Darüber hinaus wurden auch klassische Usability-Mängel im Bereich der Erläuterungen zum Datenschutz einschließlich den Informationen zu Cookies aufgegriffen. So fehlten zum Beispiel Navigationsmöglichkeiten, um zwischen Teilabschnitten in

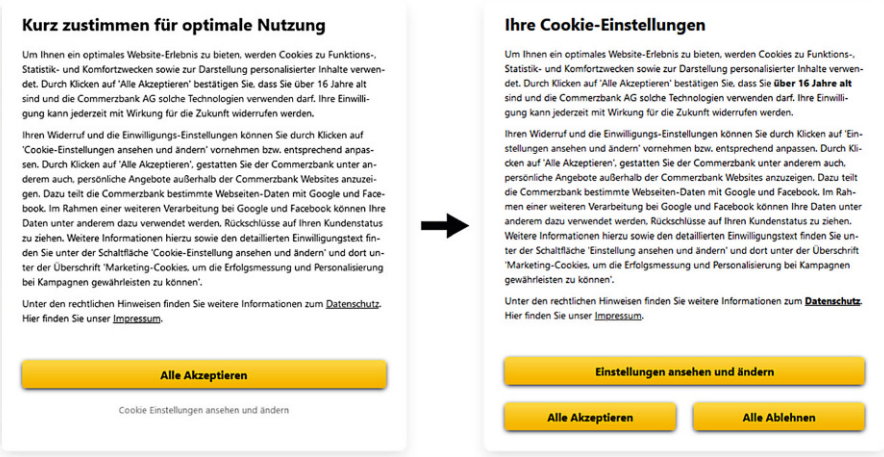

Abb. 1 Dark Pattern: Cookie-Einstellungen (Canzler 2020)

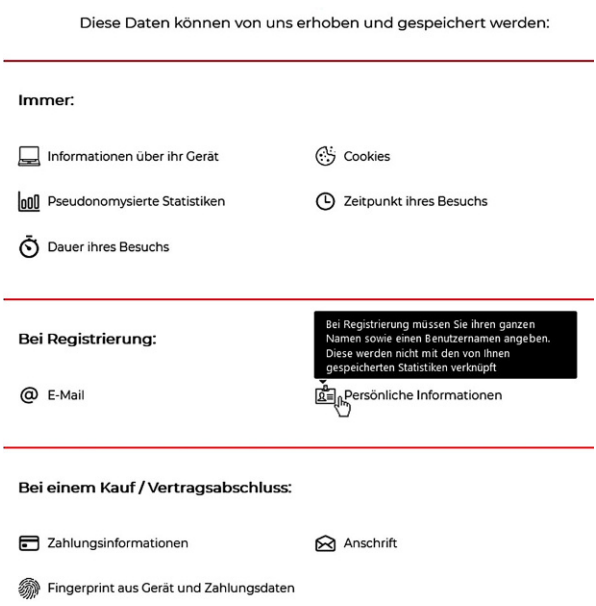

Abb. 2 Verwendung von Privacy Icons (Rohden 2020)

langen Texten zu wechseln. Häufig kann durch die umfassenden Texte nur durch Scrollen navigiert werden. Die Nutzung von Lesbarkeitsindizes (z. B. LIX, Lenhard und Lenhard 2017) kann helfen, schwer verständliche Datenschutzhinweise zu identifizieren. Um Informationen schnell erfassen zu können, sind darüber hinaus Symbole, auch Privacy Icons genannt, denkbar. Dies wird auch durch die Datenschutz-Grundverordnung abgedeckt (DSGVO Art. 12(7)). Allerdings stellen die existierenden Icon-Bibliotheken nicht alle notwendigen Visualisierungen zur Verfügung (De Jong und Spagnuelo 2020). Abb. 2 zeigt einen Entwurf, bei dem neben den entworfenen Icons auch kurze textuelle Erläuterungen ergänzt werden, um die Verständlichkeit zu erhöhen. Außerdem ist es möglich, über die Icons direkt in die Texte zu wechseln, um zu den vollständigen Erläuterungen zu gelangen. Auf diese Weise wird vermieden, dass Inhalte übermäßig vereinfacht werden, was einer angemessenen Informationsvermittlung entgegenstehen kann. Privacy Icons stellen somit auch einen geeigneten Weg dar, digitale Kompetenzen im Bereich der Datensouveränität zu erhöhen.

Eine weitere Option, Informationen über erhobene personenbezogene Daten präzise und einfach zu übermitteln und eine Kontrollmöglichkeit zu erhalten, die umständliche Anfragen beim Anbieter ersetzen, sind *Privacy Dashboards* (Herder und Maaren 2020). Werden solche Dashboards Website-übergreifend in standardisierter Form zur Verfügung gestellt, stärkt dies das Vertrauen gegenüber den jeweiligen Online-Services (vgl. Habib et al. 2020). Durch eine einheitliche Gestaltung erhöht sich auch die Kompetenz im Kontext der Datensouveränität. Abb. 3 zeigt einen Lösungsansatz für ein *Privacy Dashboard*.

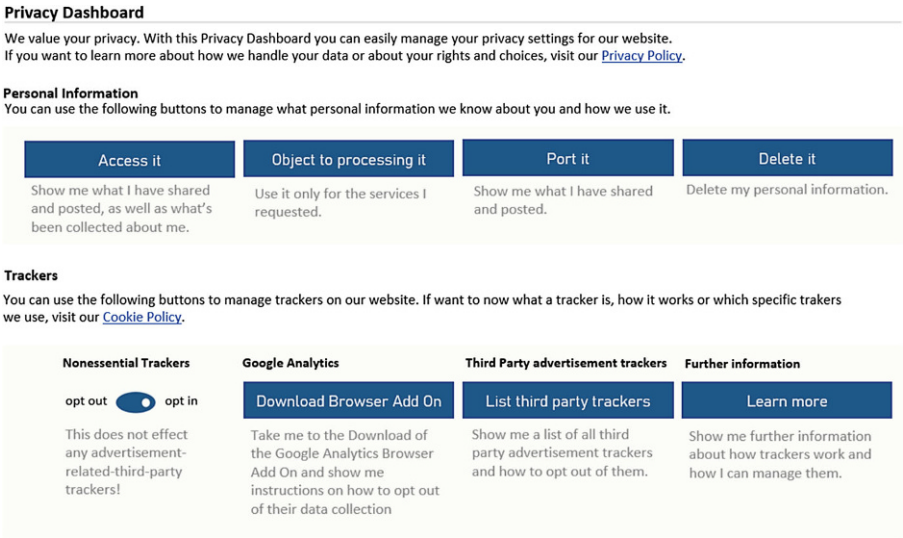

Abb. 3 Entwurf Privacy Dashboard (Krampe 2020)

5 Diskussion und Ausblick

Unabhängig von der verantwortlichen Organisation gibt es keine herausstechenden Maßnahmen bezogen auf die Erhöhung der Datensouveränität der Nutzer und sogar bewusste oder unbewusste Versuche, die Datensouveränität der Nutzer zu untergraben, wie zum Beispiel durch die Verwendung von *Dark Patterns* bei Cookie-Abfragen. Dies betrifft auch öffentliche Verwaltungen als Anbieter von E-Government-Dienstleistungen. Öffentliche Verwaltungen stehen in einer besonderen Verantwortung gegenüber E-Government-Nutzern, da die Wahlfreiheit zur Nutzung des jeweiligen Dienstes eingeschränkt oder nicht vorhanden ist. Mögliche Maßnahmen in den Handlungsfeldern Kompetenzen, Technologie und Regulierung werden nicht ausreichend ausgefüllt. Insgesamt müssen die Handlungsfelder übergreifend berücksichtigt werden. Zum Beispiel ist fraglich, inwieweit Nutzer Angebote zum Kompetenzaufbau annehmen würden, wenn die jeweiligen Betreiber Datensouveränität nicht konsequent berücksichtigten, zum Beispiel bei der Verwendung von *Dark Patterns*.

Aufgrund des explorativen Charakters ermöglicht das Vorgehen keine Ableitung allgemeingültiger Aussagen über die Berücksichtigung von Datensouveränität im öffentlichen Sektor. Die Ergebnisse basieren auf einem exemplarischen und gestaltungsorientierten Vorgehen. Die präsentierten Gestaltungsempfehlungen und Lösungsansätze wurden nicht im Rahmen von Nutzerstudien evaluiert. Die Verfeinerung der Lösungsansätze, eine systematische Abdeckung des Konzepts der Datensouveränität hinsichtlich der Handlungsfelder Kompetenzen, Technologie und Regulierung sowie eine Evaluierung durch Nutzerstudien ist Gegenstand anschließender Forschung. Daher sollten zukünftige Studien die Lösungsansätze evaluieren (z. B. in A/B-Tests) und die Auswirkungen auf die Datensouveränität der Nutzer unter-

suchen. Die hier erarbeiteten Ergebnisse zeigen zum Teil sehr leicht umzusetzende Lösungen, die das Vertrauen gegenüber Anbietern von Online-Services im privaten und öffentlichen Sektor stärken können.

Funding Open Access funding enabled and organized by Projekt DEAL.

Literatur

Bergquist M, Ljungberg J, Remneland B, Rolandsson B (2017) From e-government to e-governance: social media and public authorities legitimacy work. European Conference on Information Systems (ECIS), Guimarães, S 858–872

Bizer J (2019) Digitale Souveränität – wer steuert, organisiert und kontrolliert die digitale Verwaltung? In: Lühr H, Jabkoswki R, Smentek S (Hrsg) Handbuch Digitale Verwaltung. Kommunal- und SchulVerlag, Wiesbaden, S 23–36

Canzler R (2020) Dark Patterns und Zugänglichkeit von Informationen bezüglich des Datenschutzes. Seminararbeit, Universität zu Lübeck (unveröffentlicht)

Czernohorsky S, Weiler S (2012) Medienkompetenz. Grundlage der E-Government-Nutzung. In: E-Government und Netzpolitik im europäischen Vergleich. Nomos, S 321–339

Derguech W, Zainab SS, D'Aquin M (2018) Assessing the readability of policy documents: the case of terms of use of online services. Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance, S 247–256 https://doi.org/10.1145/3209415.3209498

Diepenbrock A, Sachweh S (2018) Ein konzeptionelles Rahmenwerk für die Integration Digitaler Souveränität in Softwarearchitekturen. Datenschutz Datensicher 42(5):281–285

Franke T, Attig C, Wessel D (2019) A personal resource for technology interaction: development and validation of the affinity for technology interaction (ATI) scale. Int J Hum Comput Interact 35(6):456–467. https://doi.org/10.1080/10447318.2018.1456150

Friedrichsen M, Bisa PJ (2016) Digitale Souveränität. Vertrauen in der Netzwerkgesellschaft. Springer, Wiesbaden

Gerber N, Gerber P, Volkamer M (2018) Explaining the privacy paradox: a systematic review of literature investigating privacy attitude and behavior. Comput Secur 77:226–261

Di Geronimo L, Braz L, Fregnan E, Palomba F, Bacchelli A (2020) UI dark patterns and where to find them: a study on mobile applications and user perception. In: Proceedings of the 2020 CHI conference on human factors in computing systems, S 1–14

Gräf E, Lahmann H, Otto P (2018) Die Stärkung der digitalen Souveränität. Wege der Annäherung an ein Ideal im Wandel. https://www.divsi.de/wp-content/uploads/2018/05/DIVSI-Themenpapier-Digitale-Souveraenitaet.pdf. Zugegriffen: 16. Apr. 2021

Habib H, Pearman S, Wang J, Zou Y, Acquisti A, Cranor LF, Sadeh N, Schaub F (2020) "It's a scavenger hunt": Usability of Websites' Opt-Out and Data Deletion Choices. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery. S 1–12. https://doi.org/10.1145/3313831.3376511

Helbig N, Gil-García JR, Ferro E (2009) Understanding the complexity of electronic government: Implications from the digital divide literature. Gov Inf Q 26(1):89–97
Herder E, van Maaren O (2020) Privacy dashboards: the impact of the type of personal data and user control on trust and perceived risk. In: Adjunct publication of the 28th ACM conference on user modeling, adaptation and personalization, S 169–174
Hunnius S, Schuppan T, Stocksmeier D (2016) Lebenslagenorientiertes E-Government. Verwalt Manag 22(4):187–193
de Jong S, Spagnuelo D (2020) Iconified representations of privacy policies: a GDPR perspective. World Conference on Information Systems and Technologies. Springer, Cham, S 796–806
Krampe L (2020) Datensouveränität fördern. Seminararbeit, Universität zu Lübeck (unveröffentlicht)
Krupka D (2020) Dimensionen digitaler Souveränität – ein Überblick. In: Schlüsselaspekte digitaler Souveränität. Arbeitspapier. Gesellschaft für Informatik. https://gi.de/fileadmin/GI/Allgemein/PDF/Arbeitspapier_Digitale_Souveraenitaet.pdf. Zugegriffen: 16. Apr. 2021
Lenhard W, Lenhard A (2017) Berechnung des Lesbarkeitsindex LIX nach Björnson. http://www.psychometrica.de/lix.html. Zugegriffen: 16. Apr. 2021
Masur PK, Teutsch D, Trepte S (2017) Entwicklung und Valdierung der Online-Privatheitskompetenzskala (OPLIS). Diagnostica 63:256–268
Nestler S, Quadflieg S, Neuburg K (2020) Das Design-Prisma-Interdisziplinäre Lösung gesellschaftlicher Herausforderungen. Mensch und Computer 2020-Usability Professionals.
Rohden J (2020) Ergänzende Visualisierung einer Datenschutzerklärung durch Privacy Icons. Seminararbeit, Universität zu Lübeck (unveröffentlicht)
Rost M, Bock K (2011) Privacy by design und die neuen Schutzziele. Datenschutz Datensicher 35(1):30–35
SVRV (2017) Digitale Souveränität. Gutachten des Sachverständigenrats für Verbraucherfragen. https://core.ac.uk/download/pdf/132283323.pdf. Zugegriffen: 16. Apr. 2021
Tabassum M, Alqhatani A, Aldossari M, Richter Lipford H (2018) Increasing user attention with a comic-based policy. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, S 200:1–200:6. https://doi.org/10.1145/3173574.3173774
Utz C, Degeling M, Fahl S, Schaub F, Holz T (2019) (un)informed consent: Studying gdpr consent notices in the field. In: Proceedings of the 2019 acm sigsac conference on computer and communications security, S 973–990
Vuorikari R, Punie Y, Carretero S, van den Brande L (2016) Digcomp 2.0: the digital competence framework for citizens. Publications office of the European Union. https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/digcomp-20-digital-competence-framework-citizens-update-phase-1-conceptual-reference-model. Zugegriffen: 16. Apr. 2021
Zhao J, Binns R, Van Kleek M, Shadbolt N (2016) Privacy languages: are we there yet to enable user controls? Proceedings of the 25th International Conference Companion on World Wide Web, S 799–806. https://doi.org/10.1145/2872518.2890590