YSAS

Guirguis, K., et al. (2021). Datenschutz in der Schweiz – eine quantitative Analyse der gesellschaftlichen Bedenken und Erwartungen an den Staat. *Swiss Yearbook of Administrative Sciences,* 12(1), pp. 16–30. DOI: https://doi.org/10.5334/ssas.153

RESEARCH

Datenschutz in der Schweiz – eine quantitative Analyse der gesellschaftlichen Bedenken und Erwartungen an den Staat

Katharina Guirguis[1], Lyn E. Pleger[1], Simone Dietrich[2], Alexander Mertes[1] and Caroline Brüesch[1]

[1] Institute of Public Management, Zurich University of Applied Sciences, CH

[2] Institute of Social Planning, Organisational Change and Urban Development, University of Applied Sciences and Arts Nothwestern Switzerland, CH

Corresponding author: Katharina Guirguis (katharina.guirguis@zhaw.ch)

Datenschutz gewährt Bürgerinnen und Bürgern Schutz vor missbräuchlicher Verwendung ihrer persönlichen Daten. Insbesondere technologische Entwicklungen und die damit einhergehende Automatisierung von Datenerfassung und -verarbeitung erfordern die Überarbeitung bestehender Datenschutzgesetze. Vor dem Hintergrund der Revision des Datenschutzgesetzes in der Schweiz betrachtet der vorliegende Artikel den Datenschutz auf verschiedenen Ebenen. Auf staatlicher Ebene geht es primär um die Gesetzgebung, die den Schutz der Daten von Bürgerinnen und Bürgern gewährleisten soll. Darüber, was für Schweizer Bürgerinnen und Bürger im Kontext von Datenschutz wichtig ist, liegt jedoch wenig Evidenz vor. Mithilfe einer Online-Befragung von 500 Personen in der deutschsprachigen Schweiz untersucht der Artikel deshalb, was Datenschutz auf der Individualebene bedeutet und welche Aspekte den Befragten Bedenken bereiten. Die Resultate zeigen, dass die befragten Personen der Gewährleistung ihrer Privatsphäre hohen Wert beimessen. Ausserdem haben sie Bedenken im Hinblick auf einen möglichen Missbrauch ihrer Daten. Gleichzeitig sind sie nicht unzureichend vertraut mit der datenschutzrechtlichen Gesetzeslage. Diese Resultate zeigen auf, welche Bedeutung einer angemessenen Kommunikation und medialen Berichterstattung bei der Einführung des neuen Datenschutzgesetzes in der Schweiz zukommt. Für den Staat und staatliche Organisationen impliziert dies, dass neben der Anpassung des Datenschutzgesetzes auch Anstrengungen unternommen werden sollten, die Bevölkerung hinsichtlich dieser Gesetzesänderung und der Verwendung von Daten zielgerichteter und transparenter zu informieren. Auf diese Weise kann der Staat dazu beitragen, dass sich Bürgerinnen und Bürger aufgrund besserer Kenntnisse vorsichtiger im Umgang und der Bereitstellung persönlicher Daten verhalten und damit ihre persönlichen Daten besser schützen können.

Schlüsselwörter: Datenschutz; Schweiz; Onlinebefragung; Datenschutzgesetz

Data protection protects citizens against misuse of their personal data. In particular, technological developments and the associated automation of data collection and processing require the revision of existing data protection regulation. Against the background of the revision of the Swiss Data Protection Act, this article looks at data protection at various levels. At the state level, it is primarily a question of legislation that is intended to guarantee the protection of citizens› data. However, there is little evidence about what is important to Swiss citizens in the context of data protection. With the help of an online survey of 500 people in Switzerland, the article therefore investigates what data protection means at the citizen level and which aspects cause concern to the respondents. The results show that the respondents place a high value on the protection of their privacy. They also have concerns about the possible misuse of their data. At the same time, they are not sufficiently familiar with the legal situation underlying data protection. These results emphasize the importance of appropriate communication and media coverage of the introduction of the new Data Protection Act in Switzerland.

For the state and state organizations, this implies that in addition to adapting the Data Protection Act, efforts should also be made to inform the population about the legislation in a more targeted and transparent manner. This can help individuals to be more cautious in handling and providing personal data due to better knowledge and thus better protect their personal data.

Keywords: data protection; Switzerland; online survey; Data Protection Act

La protection des données offre aux citoyens une protection contre l'utilisation abusive de leurs données personnelles. En particulier, les développements technologiques et l'automatisation de la collecte et du traitement des données qui en découle nécessitent la révision des lois existantes sur la protection des données. Dans le contexte de la révision de la loi fédérale sur la protection des données en Suisse, cet article examine la protection des données à différents niveaux. Au niveau de l'État, c'est avant tout une question de législation qui vise à garantir la protection des données des citoyens. Cependant, il existe peu de données sur ce qui est important pour les citoyens suisses dans le contexte de la protection des données. À l'aide d'une enquête en ligne menée auprès de 500 personnes en Suisse, l'article examine donc ce que signifie la protection des données au niveau des citoyens et quels aspects préoccupent les personnes interrogées. Les résultats montrent que les personnes interrogées attachent une grande importance à la garantie de leur vie privée. Ils s'inquiètent également d'une éventuelle utilisation abusive de leurs données. En même temps, ils n'ont pas un niveau uniformément élevé de connaissance de la situation juridique qui sous-tend la protection des données. Ces résultats soulignent l'importance d'une communication et d'une couverture médiatique appropriées de l'introduction de la nouvelle loi sur la protection des données en Suisse. Pour l'Etat et les organisations étatiques, cela implique qu'outre l'adaptation de la loi sur la protection des données, des efforts doivent également être faits pour informer la population sur la législation de manière plus ciblée et plus transparente. Cela peut aider les individus à être plus prudents dans la manipulation et la fourniture de données personnelles grâce à une meilleure connaissance, et donc à mieux protéger leurs données personnelles.

Mots-clés: Protection des données; Suisse; enquête en ligne; loi sur la protection des données

1 Einleitung

Datenschutz bezeichnet den Schutz von Bürgerinnen und Bürgern «vor unerwünschten Folgen (...) aufgrund des Zugriffs auf (gespeicherte) Daten, beziehungsweise des ungewollten Datenverlusts» (Witt 2010, S. 3). Dabei umfasst Datenschutz «gesellschaftspolitische, volkswirtschaftliche, rechtliche, organisatorische und technische Aspekte» (Pommerening, 1991, S.1). Für einen effektiven Datenschutz braucht es das Zusammenspiel von drei Aspekten: Erstens Regulierungen, wie insbesondere Datenschutzgesetze, zweitens Selbstverpflichtung zum Datenschutz durch die Organisationen, die mit den Daten in Kontakt kommen, also staatliche und private Organisationen wie Verwaltungseinheiten oder Online-Shops und drittens Massnahmen zum Selbstschutz durch Individuen und Systeme (Petrlic & Sorge, 2017).

Die Thematik des Datenschutzes ist aufgrund der Revision des Datenschutzgesetzes in der Schweiz (Schweizerisches Parlament, 2020a) sowie des ihr vorhergegangenen Inkrafttretens der Datenschutzgrundverordnung (DSGVO) in der Europäischen Union (EU) im Jahr 2018 (siehe bspw. Jorzig & Sarangi, 2020) von grosser Aktualität. Gründe für diese Revisionen gibt es mehrere: So hatte die Revision der DSGVO zum Ziel, innerhalb der EU zu einer Vereinheitlichung des Datenschutzes beizutragen und die Rechte der Datensubjekte zu stärken (Jorzig & Sarangi, 2020). Unter anderem führten aber auch die technologischen Entwicklungen und die damit verbundene Automatisierung der Datenverarbeitung zu neuen Herausforderungen (Witt, 2010), denen mit der neuen DSGVO Rechnung getragen werden sollte, indem die Datensubjekte verstärkt betont werden (Griesinger, 2020).

Die Anpassung der DSGVO fand auch Eingang in die Revision des Schweizer Datenschutzgesetzes, indem dieses den Grundsätzen der revidierten DSGVO angeglichen wird (siehe bspw. Sury, 2017). Analog zur DSGVO besteht ein primäres Ziel der Schweizer Gesetzesrevision darin, bei der Erhebung und Bearbeitung

personenbezogener Daten mehr Transparenz zu schaffen und das informationelle Selbstbestimmungsrecht von Bürgerinnen und Bürgern zu stärken (Schweizerische Eidgenossenschaft, 2019). Nachdem das Parlament das schweizerische Datenschutzgesetz nach dreijähriger Ratsdebatte 2020 angenommen hat, wird dieses voraussichtlich in den nächsten Jahren in Kraft gesetzt (siehe bspw. Griesinger, 2020).

Dass die Gewährleistung des Datenschutzes keine Selbstverständlichkeit ist, zeigen unter anderem verschiedene Datenschutzskandale, wie beispielsweise die unautorisierte Weitergabe persönlicher Daten durch Facebook an die Firma Cambridge Analytica (siehe bspw. Isaak & Hanna, 2018). Solche Skandale wecken bei Bürgerinnen und Bürgern Sorgen um die Gewährleistung ihrer Privatsphäre (Tuttle, 2018). Gleichzeitig führte das Aufkommen des Internets dazu, dass Bürgerinnen und Bürger ihre Daten freiwillig preisgeben und damit den Schutz ihrer Persönlichkeitsrechte möglicherweise gefährden (Von Lewinski, 2012). Trotz dieser Gefahren sind Nutzerinnen und Nutzer aber nur bedingt gewillt, sich einzuschränken und deswegen auf digitale Angebote zu verzichten (Husi-Stämpfli, 2018).

Um Bürgerinnen und Bürger vor dem Missbrauch ihrer Daten zu schützen, bedarf es nicht nur einer Anpassung der regulatorischen Rahmenbedingungen. Es bedingt gleichermassen, dass sie sich mit der komplexen Thematik des Datenschutzes auseinandersetzen und sich ihrer Rechte bei der Datenverarbeitung durch Dritte bewusst sind. Das Recht auf informationelle Selbstbestimmung setzt voraus, dass Bürgerinnen und Bürger über entsprechendes Wissen im Umgang mit ihren Daten verfügen. Erst dann sind sie in der Lage, im Sinne einer informierten Einwilligung (unter Kenntnis von Umfang und Zweck) einer Verarbeitung der eigenen Daten zuzustimmen oder diese abzulehnen (Schmidt, 2020).

Die Relevanz des gesetzlich verankerten Datenschutzes und dessen Gewährleistung manifestiert sich in den jüngsten Rechtsreformen in der Schweiz und in der EU. Ein primäres Ziel von Revisionen gesetzlicher Rahmenbedingungen besteht stets darin, den Bedürfnissen der Bevölkerung gerecht zu werden und eine regulatorische Voraussetzung dafür besteht in der Verständlichkeit von Gesetzen durch die Bürgerinnen und Bürger (Hauck & Lötscher, 1994). Entsprechend argumentieren Hauck & Lötscher (1994, S. 91), dass ein Gemeinwesen nur dann funktionieren kann, «wenn seine Bürgerinnen und Bürger vom Sinn und Nutzen der Gesetze überzeugt sind», was wiederum eine Verständlichkeit der Gesetze voraussetzt. Welche Bedeutung Schweizer Bürgerinnen und Bürger dem Datenschutz beimessen, ob sie mit den gesetzlichen Rahmenbedingungen vertraut sind und welche Aspekte ihnen dabei besonders wichtig sind, wurde bis anhin empirisch kaum untersucht.

Der vorliegende Artikel untersucht daher mit Hilfe einer Online-Befragung in der Schweiz einerseits, welche Aspekte des Datenschutzes für Schweizer Einwohnerinnen und Einwohner wichtig sind. Zum anderen wird untersucht, welche Bedenken sie im Zusammenhang mit Datenschutz haben, welche Rolle der Staat und staatliche Organisationen bezüglich der Gewährleistung des Datenschutzes einnehmen (sollten) und ob dies mit der ermittelten Relevanz und der Bedenken der Einwohnerinnen und Einwohner im Einklang ist.

Der vorliegende Artikel widmet sich den folgenden Forschungsfragen:

Welche Aspekte von Datenschutz sind für Schweizer Einwohnerinnen und Einwohner relevant?

Welche Bedenken haben Schweizer Einwohnerinnen und Einwohner hinsichtlich des Datenschutzes?

Welche Rolle spielt der Staat bezüglich der Gewährleistung von Datenschutz und Datensicherheit?

Um diese Fragen zu beantworten, folgt zunächst eine Erläuterung der theoretischen Bedeutung des Datenschutzes aus Sicht von Bürgerinnen und Bürgern auf der einen und dem Staat auf der anderen Seite. Dabei geht es insbesondere um das Zusammenspiel von Gesetzen, Bedenken und Kenntnissen. Anschliessend erfolgt die Darlegung des Forschungsdesigns und des methodischen Vorgehens, gefolgt von der Präsentation der Ergebnisse und deren Diskussion. Dabei werden die empirischen Daten in einen konzeptionellen Kontext gestellt und im Hinblick auf die Forschungsfrage beurteilt. Der Artikel schliesst mit einem Ausblick für Forschung und Praxis.

2 Datenschutz aus institutioneller und individueller Perspektive

Neben Regulierungen und Gesetzen sind beim Datenschutz verantwortungsvolles Handeln durch Organisationen und den Staat sowie das Verhalten von Bürgerinnen und Bürgern von zentraler Bedeutung (Petrlic & Sorge, 2017). In der Forschung werden diese Bereiche aufgrund der thematischen Interdisziplinarität oft isoliert voneinander betrachtet, was nicht der Realität entspricht und den Einbezug der verschiedenen Ebenen und Perspektiven umso relevanter macht (Ginosar & Ariel, 2017). Nachfolgend

wird deshalb zunächst eine begriffliche Abgrenzung von Datenschutz vorgenommen, bevor die Darlegung der gesetzlichen Grundlagen, die den Datenschutz sicherstellen, erfolgt. Anschliessend wird die Bedeutung des Datenschutzes aus Sicht der Bürgerinnen und Bürger betrachtet, indem das Recht auf Privatsphäre diskutiert wird.

2.1 Definition Datenschutz

Allgemein kann Datenschutz als «grundlegendes Recht» verstanden werden, «das sowohl bei der manuellen als auch bei der maschinellen Datenverarbeitung zu beachten ist» (Witt, 2010, S. 1). Dies umfasst Gesetze, die den Datenschutz regeln oder technische Massnahmen, welche die Datensicherheit gewährleisten sollen (EDÖB, 2015). Datenschutz wird in der Literatur nicht einheitlich definiert. Dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB (2015, S. 3) zufolge umfasst Datenschutz «alle Massnahmen zur Verhinderung einer unerwünschten Bearbeitung von Personendaten und deren Folgen». Personendaten in diesem Sinne enthalten Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Ähnlich definiert auch Witt (2010,S. 4) Datenschutz als «Schutz des Einzelnen vor Beeinträchtigung seines Persönlichkeitsrechts beim Umgang mit seinen persönlichen Daten.» Dieser Artikel folgt der begrifflichen Abgrenzung von Datenschutz nach Pommerening (1991, S. 10), wonach unter Datenschutz «der Schutz von Daten vor Mi[ss]brauch, unberechtigter Einsicht oder Verwendung, Änderung oder Verfälschung, aus welchen Motiven auch immer» verstanden wird. «Im engeren Sinne, etwa in der Gesetzgebung, handelt es sich dabei nur um personenbezogene Daten; im allgemeinen Sprachgebrauch (…) werden aber alle Daten, die irgendwo gespeichert sind, einbezogen» (Pommerening, 1991, S. 10).

2.2 Institutionelle Rahmenbedingungen

Wenngleich die Anerkennung der Bedeutung von Privatsphäre und deren Präsenz im gesellschaftlichen Diskurs keine neuen Phänomene darstellen, so hat sich doch die Relevanz der Privatsphäre vor dem Hintergrund der technologischen Entwicklungen seit den 1960er-Jahren verstärkt (Petrlic & Sorge, 2017, S. 140). Ein moderner Staat soll durch regulierende Massnahmen in die Gesellschaft eingreifen, wenn es für die Gewährleistung des Datenschutzes erforderlich ist (Jantz & Veit, 2019). Im Kontext von Datenschutz besteht eine wesentliche Schwierigkeit darin, den schnellen technologischen Entwicklungen Rechnung zu tragen, woraus «(…) Verunsicherungen in der Rechtsanwendung [resultieren](…)» (Bock & Meissner, 2012, S. 452). Entsprechend manifestierten sich die Herausforderungen im Datenschutz nicht zuletzt durch die schnellen technologischen Entwicklungen in «gesetzgeberische[n] Aktivitäten», indem beispielsweise in Deutschland 1970 das weltweit erste Datenschutzgesetz in Kraft trat (Petrlic & Sorge, 2017, S. 141).

Artikel 13 der Bundesverfassung der Schweizerischen Eidgenossenschaft regelt, dass «[j]ede Person Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs [hat]» (BV, SR 101, Art. 13). Das Bundesgesetz über den Datenschutz (DSG) verankert die Wahrung dieses Rechts gesetzlich (EDÖB, 2021). Die Revision des DSG orientiert sich an der revidierten DSGVO in der EU (siehe bspw. Griesinger, 2020; Sury, 2017). Vom bisherigen DSG unterscheidet es sich jedoch insbesondere dadurch, dass der Geltungsbereich nur noch natürliche Personen – und nicht wie bisher auch juristischen Personen – umfasst (Sury, 2017). Ausserdem werden Sanktionen festgelegt, die eine Bestrafung bei vorsätzlicher Verletzung des DSG ermöglichen und es erfolgt eine Auflistung besonders schützenswerter Personendaten (Griesinger, 2020). Sanktioniert werden können ebenfalls Verletzungen der Sorgfaltspflichten (Griesinger, 2020). Die Datenverantwortlichen werden ausserdem in die Pflicht genommen, eine Datenschutz-Folgeabschätzung zu machen, insbesondere «wenn es zur umfangreichen Bearbeitung besonders schützenswerter Personendaten kommt (…) oder wenn umfangreiche öffentliche Bereiche systematisch überwacht werden» (Griesinger, 2020, S. 47). In Fällen von Datenschutzverletzungen mit «grosse[m] Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person» muss der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) unverzüglich informiert werden (Griesinger, 2020, S. 46).

2.3 Wahrung des Rechts auf Privatsphäre

Institutionelle Rahmenbedingungen vermögen das Verhalten von Personen zu beeinflussen. Gesetze, beziehungsweise die glaubhafte Darlegung deren Einhaltung durch eine Organisation, schaffen bei den Bürgerinnen und Bürgern ein gewisses Vertrauen im Umgang mit ihren Daten (Roßnagel, 2020). Wenngleich Gesetze einen gewissen Schutz der persönlichen Daten bieten und öffentliche und private Organisationen Bemühungen durchsetzen, um den durch die Gesetze festgelegten Datenschutz zu

gewährleisten, erzeugen Datenschutzverletzungen[1] oder Datenschutzskandale[2] bei Individuen Bedenken (siehe bspw. Tuttle, 2018). Zur DSGVO, die im ganzen EU-Raum gilt, kommentiert beispielsweise Schaar (2020, S. 182), «(…), dass die neuen Gesetze noch weit davon entfernt sind, die von den Gesetzgebern beabsichtigten Wirkungen zu entfalten». Er begründet dies damit, dass Nutzerinnen und Nutzer oft keine Wahl haben, als der Verwendung ihrer Daten zuzustimmen, da sie durch die «(…) Marktmacht einiger weniger digitaler Unternehmen und der Einschliessungs-(Lock-in-)Effekte (…)» der Datenverwendung faktisch zustimmen müssen (Schaar, 2020, S. 182).

Aus der Perspektive von Bürgerinnen und Bürgern geht es um die Wahrung ihres Rechts auf Privatsphäre, das gemäss der Allgemeinen Erklärung der Menschenrechte 1948 ein Menschenrecht darstellt (Vereinte Nationen, 1948, Art. 12). Aufgrund der Komplexität des Begriffs der Privatsphäre ist es schwierig, diesen in die Legislation zu überführen (Hallinan et al., 2012). Beispielsweise kann Privatsphäre als das Recht von Individuen zur Selbstbestimmung über die Bekanntgabe von eigenen Informationen an andere verstanden werden (Westin, 2003).

Der Schutz der eigenen Privatsphäre durch das eigene Verhalten ist von individuellen Kontextfaktoren (beispielsweise frühere Erfahrungen oder der kulturelle Hintergrund) und persönlichen Faktoren (beispielsweise Bedenken, Einstellungen und Überzeugungen) geprägt (Dinev et al., 2015). Vereinfacht gesagt, beeinflussen diese Faktoren das individuelle Verhalten und bestimmen somit darüber, wie schützend sich eine Person ihren Daten gegenüber verhält (Dinev et al., 2015). Das Recht auf Privatsphäre ist für Individuen von grosser Bedeutung und sie fürchten mögliche Verletzungen dieses Rechts. Beispielsweise bestehen Bedenken darüber, wie Organisationen persönliche Informationen behandeln und ob die Individuen die Kontrolle über ihre persönlichen Daten verlieren könnten (Yun et al., 2019). Studien zeigen aber gleichzeitig, dass Individuen ihre Daten trotz bestehenden Bedenken teilen (Kummer & Schulte, 2016; Sutanto et al., 2013). Das sogenannte *Privacy Paradox* beschreibt diese Diskrepanz zwischen der Einstellung von Personen, ihre Privatsphäre zu schützen einerseits und ihrem tatsächlichen Verhalten, persönliche Daten bereitzustellen andererseits (siehe bspw. Kokolakis, 2017). Konkret bezieht sich das Privacy Paradox auf das in verschiedenen Studien wiederholt festgestellte Verhalten von Personen, wonach diese ihre Privatsphäre online durch die Preisgabe ihrer Daten gefährden, obwohl dieses Verhalten ihrer Einstellung zum Datenschutz widerspricht (Barth & de Jong, 2017). In der Wissenschaft gibt es für dieses Verhalten unterschiedliche Erklärungsansätze (siehe bspw. Hallam & Zanella, 2017). Kokolakis (2017) begründet das Verhalten damit, dass Nutzerinnen und Nutzer eine Kosten-Nutzen-Abwägung zwischen erwartetem Nutzen und Kosten treffen. Bemerkenswert daran ist, dass dieser Tausch von Daten gegen Leistung auch dann vollzogen wird, wenn die erhaltene Leistung relativ gering ist (Kummer & Schulte, 2016; Sutanto et al., 2013).

2.4 Zusammenfassung des Untersuchungskontextes

Bürgerinnen und Bürger befinden sich beim Datenschutz in einem Spannungsfeld zwischen erstens Gesetzen, die ihren Schutz durchsetzen und zweitens Organisationen, die ihn gewährleisten sollen, drittens ihrem persönlichen Verhalten, sich zu informieren, um die Preisgabe ihrer Daten zumindest teilweise zu steuern sowie viertens ihren Ansprüchen gegenüber dem Datenschutz und Bedenken vor fehlbarer Verwendung ihrer Daten, die unter anderem durch Verletzungen des Datenschutzes verursacht werden.

Aus diesem multidimensionalen Spannungsfeld zwischen Bürgerinnen und Bürgern und Staat ergeben sich verschiedene Sichtweisen auf den Datenschutz. **Abbildung 1** zeigt diese verschiedenen Sichtweisen anhand der unterschiedlichen Betrachtungsebenen schematisch auf. Hierbei kommt dem Staat als Gesetzgeber eine wesentliche Rolle zu, indem er entsprechende Gesetze erlässt und durchsetzt (Schweizerisches Parlament, 2020b). Gleiches gilt für Organisationen, die durch geeignete Sicherungsmechanismen das Risiko von Datenschutzverletzungen mindern können (siehe bspw. Petrlic & Sorge, 2017). Bedenken auf individueller Ebene werden einerseits durch Gesetze gelindert, gleichzeitig aber durch diese nicht aus der Welt geschafft (siehe bspw. Lwin et al., 2007). Auch wenn Gesetze und Organisationen einen gewissen Schutz bieten, so ist auch das individuelle Verhalten durch das Erfordernis einer Selbstverantwortung gekennzeichnet, die eigenen Daten gewissenhaft zu behandeln.

[1] Für eine Übersicht über ausgesprochene Bussen wegen Verletzungen gegen die DSGVO siehe bspw. https://www.enforcementtracker.com/ (12.01.2021).

[2] Für eine Übersicht der Datenschutzverletzungen bei Facebook seit 2018 inkl. dem Beispiel von Cambridge Analytica siehe https://netzpolitik.org/2018/die-ultimative-liste-so-viele-datenskandale-gab-es-2018-bei-facebook/ (12.01.2021).

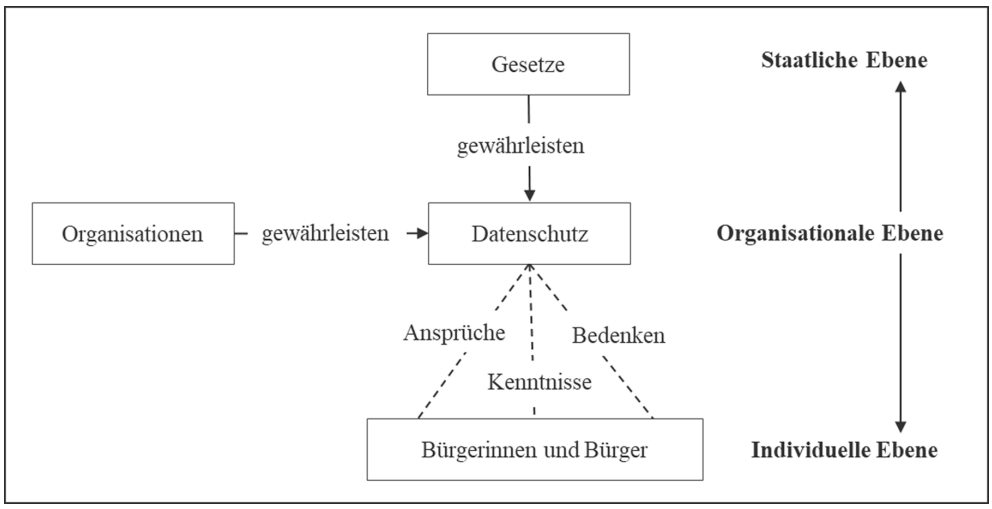

Abbildung 1: Zusammenspiel zwischen individueller und staatlicher Ebene hinsichtlich des Datenschutzes.

3 Methodik

3.1 Stichprobe

Der vorliegende Artikel basiert auf einer Online-Befragung von 500 Personen aus der Deutschschweiz in einem Zeitraum von zwei Wochen im Juli 2019. Die Deutschschweiz wurde deshalb ausgewählt, da das Verständnis von Datenschutz stark mit sprachlichen Aspekten verknüpft ist und deshalb in einem ersten Schritt die Beschränkung auf einen Sprachraum als sinnvoll erachtet wurde. Die Personen der Stichprobe wurden vom Unternehmen *Qualtrics* rekrutiert und kontaktiert. Die Stichprobe enthält 500 Personen (N = 500).[3] Die durchschnittliche Beantwortungszeit lag bei 8.9 Minuten (SD: 2.75; N = 500).

Die Stichprobe stellt eine nicht-probabilistische Quotenstichprobe mit einer merkmalsspezifischen Repräsentativität hinsichtlich *Alter* und *Geschlecht* der Schweiz dar (siehe Eurostat 2019). Stichproben mit merkmalsspezifischer Repräsentativität zeichnen sich dadurch aus, dass sie bezogen auf relevante Merkmale mit der Zusammensetzung der Gesamtpopulation übereinstimmen (Döring & Bortz, 2016). Als relevante Merkmale wurden in diesem Fall die Eigenschaften *Alter* und *Geschlecht* gewählt, da sie wichtige Merkmale der Schweizer Bevölkerung widerspiegeln. Entsprechend der Geschlechterverteilung in der Schweiz (siehe Eurostat 2019) waren 49 Prozent der Befragten männlich und 51 Prozent weiblich (N = 500). Die Befragten waren mindestens 18 Jahre alt und das Alter der Befragten war folgendermassen verteilt: Zehn Prozent waren zwischen 18 und 24 Jahre alt, 17 Prozent zwischen 25 und 34 Jahre alt, 27 Prozent zwischen 35 und 49 Jahre alt, 25 Prozent zwischen 50 und 64 Jahre alt und 21 Prozent waren über 65 Jahre alt (N = 500). Die deskriptiven Statistiken zur Stichprobe sind in Appendix A dargestellt.

Da sich bei merkmalsspezifischer Repräsentativität immer die Frage nach den einzubeziehenden Merkmalen und möglicher Verzerrung durch deren Nicht-Einbezug stellt (Döring & Bortz, 2016), ist es wichtig, anzumerken, dass auch weitere Merkmale, wie beispielsweise Herkunft oder Einkommensklasse, die in der vorliegenden Studie nicht untersucht wurden, eine Rolle spielen könnten.[4] Mehr zu den Limitationen der vorliegenden Studie findet sich in Kapitel 6 Ausblick und Limitationen.

3.2 Fragebogenkonstruktion

Der Fragebogen enthielt 31 Fragen aufgeteilt in fünf Blöcke. Die Fragen wurden theoriegestützt aus bestehender Literatur abgeleitet. Im Fragebogen waren sowohl offene als auch geschlossene Fragen enthalten. Im Anhang finden sich zusammenfassende Statistiken und Häufigkeiten zu den Variablen, die Eingang in die Studie gefunden haben (siehe Appendix B). Der erste Block enthielt Fragen zur Charakterisierung der

[3] Insgesamt wurde der Fragebogen von mehr als 500 Personen beantwortet, wobei der Datensatz um die unvollständigen Antworten bereinigt wurde. Es wurden ausserdem nur jene Fälle berücksichtigt, die eine Beantwortungszeit von mindestens einem Drittel der Medianzeit aufwiesen (Median = 8.7 min), sodass 500 vollständig beantwortete Fragebögen die Grundlage für die vorliegende Studie bilden.

[4] In der vorliegenden Studie wurde ex-post die Verteilung der Merkmale *Höchster Bildungsabschluss* und *Wohnregion* betrachtet, um allfällige Verzerrungen zu ermitteln. Dabei hat sich gezeigt, dass wenngleich beide in gewissen Punkten von den offiziellen Quoten abweichen, dies keinen Hinderungsgrund für die Analyse darstellt. Das detaillierte Vorgehen ist in Appendix A dargestellt. Ebenso sind dort deskriptive Statistiken zur Stichprobe zu finden.

Befragten. Die erste Frage widmete sich dem Land, in dem die Befragten wohnhaft waren. Damit sollte sichergestellt werden, dass nur Einwohnerinnen und Einwohner aus der Schweiz an der Umfrage teilnahmen. Danach wurden die Personen gebeten, ihren Wohnkanton sowie ihr Alter und ihr Geschlecht anzugeben. Insbesondere die beiden letzten Informationen sind wichtig für die merkmalsspezifische Repräsentativität der Stichprobe.

Der zweite Block widmete sich Fragen der Definition und des Verständnisses von Datenschutz. Darin wurde beispielsweise abgefragt, welche Begriffe die Befragten mit Datenschutz assoziierten. Der dritte Block widmete sich der Vertrautheit mit dem Datenschutz und verfolgte das Ziel, die Bekanntheit beispielsweise der rechtlichen Grundlage des Datenschutzes bei den Befragten zu ermitteln. Daraufhin folgte der vierte Block, der sich mit den Bedenken der Teilnehmenden im Zusammenhang mit Datenschutz befasste. Im letzten Block waren Kontrollvariablen wie beispielsweise das Vertrauen in den Staat und in Organisationen, aber auch soziodemografische Informationen wie der höchste Bildungsabschluss der Teilnehmenden enthalten.

Die Antworten auf die offenen Fragen wurden codiert, um sie auswerten zu können. Dies erfolgte durch die gleiche Forscherin, um die Reliabilität der Codierungen zu gewährleisten. Die Codierungen wurden anschliessend von den anderen Forschenden überprüft. Die quantitative Auswertung der Daten erfolgte mithilfe der Statistiksoftware SPSS. Bei der Analyse wurden Häufigkeiten, t-Tests für unabhängige Stichproben und einfaktorielle Varianzanalysen berechnet. Im Folgenden werden die Resultate dargestellt.

4 Resultate

Um einen ersten Anhaltspunkt für das Verständnis und die wahrgenommene Beschaffenheit von Datenschutz durch Bürgerinnen und Bürger zu erhalten, wurde in einem ersten Schritt in einer offenen Frage nach spontanen Assoziationen zu Datenschutz gefragt. Dafür wurden die Befragten gebeten, ein Schlagwort zu notieren, das ihnen in den Sinn käme, wenn sie an den Begriff 'Datenschutz' dächten. Im Anschluss wurden diese offenen Antworten codiert, indem Kategorien gebildet und die Antworten diesen Kategorien zugeordnet wurden. Dabei zeigte sich, dass die häufigsten Assoziationen (25%) sich auf Gefahren wie 'Hacking' oder 'Datendiebstahl' bezogen (**Tabelle 1**). Danach folgten Schlagworte wie 'Schutz' oder 'Sicherheit von Daten'

Tabelle 1: Spontane Assoziationen mit Datenschutz.

Kategorien	Beispielantworten	Prozent	N
Gefahren	«Datendiebstahl» «Hacking»	25%	500
Sicherheit/Schutz/Vertrauen	«Schutz» «Sicherheit von Daten»	16%	500
Neutrale Begriffe	«Internet» «Bank»	13%	500
Schutzmassnahmen	«Antivirusprogramm» «Firewall»	13%	500
Privatsphäre	«Persönlichkeitsschutz» «Anonymität»	10%	500
Ungültige Antworten	«Keine» «Weiss nicht»	9%	500
Persönliche Daten	«Personenbezogene Daten» «Persönlich»	8%	500
Datenschutzrichtlinien/Gesetze	«Gesetze» «GDPR»	2%	500
Datenspeicherung	«Speicherung meiner Daten» «Ort der Aufbewahrung»	1%	500
Gleichgültigkeit	«redundant» «Hype»	1%	500

Anmerkung: Die Frage lautete «Ganz allgemein: Welches Schlagwort kommt Ihnen bei den Begriffen «Datensicherheit» und «Datenschutz» in den Sinn?». Die offenen Antworten wurden anschliessend thematisch kategorisiert. (N = 500).

mit 16 Prozent der Nennungen. 13 Prozent der genannten Begriffe betrafen an sich neutrale Schlagworte wie 'Internet' oder 'Bank'. Ebenfalls 13 Prozent der Assoziationen liessen sich Massnahmen technischer oder persönlicher Natur zuordnen, die Schutz vor allfälligen Datenschutzverletzungen bieten sollten. Beispiele dafür sind 'Antivirusprogramm' oder 'Firewall'. Jeder zehnte genannte Begriff betraf Aspekte der Privatsphäre wie 'Persönlichkeitsschutz' oder 'Anonymität'. Neun Prozent der Antworten waren ungültig (leer, 'keine', 'weiss nicht' etc.). Schlagworte zu persönlichen Daten wie 'personenbezogene Daten' und 'persönlich' folgten mit acht Prozent der Nennungen. Die verbleibenden vier Prozent teilten sich auf in Nennungen zu Gesetzen (2%, Beispiel 'Datenschutzgrundverordnung'), Begriffen zur Datenspeicherung (1%) und in Begriffe, die eine gewisse Gleichgültigkeit gegenüber der Thematik ausdrückten wie «Hype» (ebenfalls 1%) (N = 500).

In einer Anschlussfrage an die freien Assoziationen wurden die Befragten erneut darum gebeten, anzugeben, welche Begriffe sie mit Datenschutz verbänden, wobei mittels einer geschlossenen Frage eine Liste mit neun Begriffen präsentiert wurde, aus welcher jede befragte Person diejenigen drei Begriffe auswählen sollte, die sie am stärksten mit 'Datensicherheit' und 'Datenschutz' verbände. Dabei wurden die Begriffe so ausgewählt, dass sie je drei Ausprägungen darstellen, die mit der technischen Ebene (Speicherung von Daten, Big-Data-Analysen, Privatisierung von Daten), der rechtlichen Ebene (Datenschutzrichtlinien, Datenschutzbeauftragte, Dateneigentum) und der individuellen Ebene (Persönliche Daten, Datenkontrolle, Recht auf Privatsphäre) von Datenschutz in Verbindung gebracht werden können, um verschiedene Perspektiven von Datenschutz abzudecken. **Tabelle 2** fasst die Ergebnisse zusammen. Die Prozentzahlen geben hierbei jeweils an, wie viel Prozent der Befragten einen bestimmten Begriff ausgewählt haben. Dabei zeigte sich, dass mit 'persönliche Daten' – 67 Prozent der Befragten wählten dies aus – und 'Recht auf Privatsphäre' (60%) zwei Begriffe am häufigsten angegeben wurden, die persönliche Aspekte von Datenschutz betreffen. 43 Prozent der Befragten wählten 'Speicherung von Daten' aus, gefolgt von 'Datenschutzrichtlinien' und 'Dateneigentum' (37% und 36% respektive). 'Datenkontrolle' wurde von 15 Prozent der Befragten mit Datenschutz assoziiert. Je zwölf Prozent wählten die Begriffe 'Datenschutzbeauftragte' und 'Privatisierung von Daten'. Mit fünf Prozent am wenigsten häufig wurde 'Big-Data-Analysen' mit Datenschutz assoziiert (N = 500).

Um das Wissen der Befragten über die Datenschutzgrundverordnung (DSGVO) zu erfassen,[5] wurde nach der Vertrautheit mit der DSGVO gefragt. Während 40 Prozent angaben, überhaupt nicht oder eher nicht damit vertraut zu sein, beurteilten 27 Prozent ihre Vertrautheit als mittelmässig und 28 Prozent gaben an, eher vertraut oder sehr vertraut mit der DSGVO zu sein. 4 Prozent beantworteten die Frage mit 'weiss nicht' (N = 500). Dies zeigt, dass hinsichtlich der Vertrautheit mit den gesetzlichen Grundlagen des Datenschutzes bei den befragten Personen ein heterogenes Bild vorherrscht.

Anschliessend wurden die Teilnehmenden gefragt, welches ihre grössten Bedenken im Zusammenhang mit Datenschutz und Datensicherheit darstellten. **Tabelle 3** zeigt die Bedenken der Befragten in absteigender Reihenfolge auf. 'Datenmissbrauch' (N = 495) und 'Verkauf persönlicher Daten an Dritte' (N = 495) wurden am häufigsten genannt. 87 Prozent, respektive 84 Prozent der Befragten gaben an, grosse oder sehr grosse

Tabelle 2: Gestützte Abfrage von mit Datenschutz assoziierten Begriffen.

Begriff	Prozent	N
Persönliche Daten	67%	500
Recht auf Privatsphäre	60%	500
Speicherung von Daten	43%	500
Datenschutzrichtlinien	37%	500
Dateneigentum	36%	500
Datenkontrolle	15%	500
Datenschutzbeauftragte	12%	500
Privatisierung von Daten	12%	500
Big-Data-Analysen	5%	500

Anmerkung: Die Frage lautete: Wählen Sie bitte aus folgender Liste diejenigen drei Begriffe aus, welche Sie am stärksten mit «Datensicherheit» und «Datenschutz» verbinden.

[5] Da zum Zeitpunkt der Befragung das revidierte Datenschutzgesetz der Schweiz noch nicht in Kraft war, wurde nach der DSGVO gefragt.

Tabelle 3: Bedenken betreffend Datenschutz.

Dimension	Grosse bis sehr grosse Bedenken	Mittlere Bedenken	Keine bis schwache Bedenken	N
Datenmissbrauch	87%	9%	2%	495
Verkauf persönlicher Daten an Dritte	84%	13%	2%	495
Datendiebstahl	83%	13%	3%	496
Unternehmen, die von meinen Daten profitieren	70%	21%	7%	491
Identitätsdiebstahl	63%	23%	11%	491
Unverhältnismässige Datensammlung	57%	29%	9%	478
Fake News	53%	28%	26%	482
Wahlmanipulation	51%	24%	22%	482
Einschränkung von Meinungs- und Kunstfreiheit	46%	25%	25%	480

Anmerkung: Angaben in Zeilenprozenten. Die Befragten konnten auf einer Skala von 1 bis 5 ihre Bedenken für jede der Dimensionen angeben. Die Skala reichte von 1 = keine Bedenken bis 5 = sehr grosse Bedenken. Für die Auswertung wurden die Werte 1 und 2 sowie 4 und 5 zusammengefasst.

Bedenken bezüglich möglichen Missbrauchs ihrer Daten, respektive des Verkaufs ihrer Daten zu haben. 83 Prozent nannten grosse oder sehr grosse Bedenken bezüglich eines 'Datendiebstahls' (N = 496). Die geringsten Bedenken hatten die Befragten bezüglich einer 'Einschränkung von Meinungs- und Kunstfreiheit'. Dabei gaben 25 Prozent keine bis schwache oder mittlere Bedenken an und 46 Prozent taten grosse bis sehr grosse Bedenken kund (N = 480).

Um zu ermitteln, ob die Befragten Vertrauen in den Umgang von staatlichen Institutionen mit ihren Daten haben, wurden sie gebeten, ihre Zustimmung zu folgender Aussage abzugeben: 'Die meisten staatlichen Institutionen behandeln die personenbezogenen Daten, die sie über Nutzerinnen und Nutzer sammeln, ordnungsgemäss und vertraulich.' Überhaupt nicht zu stimmten dieser Aussage zwei Prozent und eher nicht zu deren 24. Zwei Drittel (66%) stimmte eher zu und die restlichen acht Prozent stimmten vollständig zu.

Weiter sollte untersucht werden, ob sich das Vertrauen in staatliche Organisationen im Grad ihrer Bedenken, im Internet Daten preiszugeben, niederschlage. Entsprechend wurden die Befragten anhand ihrer Antworten zum Vertrauen in den Umgang mit persönlichen Daten in staatlichen Organisationen in vier verschiedene Gruppen (keine Zustimmung, eher keine Zustimmung, eher Zustimmung und vollständige Zustimmung) aufgeteilt. Mithilfe einer einfaktoriellen Varianzanalyse wurde untersucht, ob sich diese Gruppen hinsichtlich des Grads ihrer Bedenken, im Internet persönliche Daten preiszugeben, unterscheiden. Die Befragten gaben ihre Bedenken dabei auf einer Skala von 1 (=keine Bedenken) bis 10 (=sehr grosse Bedenken) an.[6]

Die Ergebnisse deuten darauf hin, dass sich die Gruppen signifikant nach ihren Bedenken unterscheiden (**Tabelle 4**). Demnach weisen diejenigen Personen mit einem höheren Vertrauen in staatliche Organisationen hinsichtlich der ordnungsgemässen Datenverwendung signifikant tiefere Bedenken auf, im Internet persönliche Daten preiszugeben ($F(3,496) = 2.886$, $p = .035$).

Um zu untersuchen, ob sich das Vertrauen in geltende Gesetze in den Bedenken, Daten preiszugeben, niederschlägt, wurden analog zum obigen Vorgehen deshalb wieder vier Gruppen gebildet. Gruppenunterschiede wurden jedoch diesmal unter Berücksichtigung der Antworten hinsichtlich der Zustimmung zur Aussage, ob bestehende Gesetze und organisatorische Praktiken einen ausreichenden Schutz der Privatsphäre der Nutzerinnen und Nutzer böten, analysiert. Wiederum konnten die Befragten ihre Zustimmung auf einer vierstufigen Skala zwischen 0 (=überhaupt keine Zustimmung) bis 3 (=vollständige Zustimmung) bewerten. Hierbei stimmten sieben Prozent der Aussage überhaupt nicht zu. Mit 45 Prozent am meisten Befragte befanden, dass sie der Aussage eher nicht zustimmten. 43 Prozent stimmen der Aussage eher und vier Prozent voll zu (N = 500).[7]

[6] Es wurde bei der Frage, wie gross die Bedenken sind, im Internet persönliche Daten preiszugeben kontrolliert, ob das Alter der Befragten hierbei eine Rolle spielt, was aufgrund fehlender Signifikanz ausgeschlossen werden konnte.

[7] Es wurde bei der Frage, ob bestehende Gesetze und organisatorische Praktiken heute bereits ein angemessenes Schutzniveau für die Privatsphäre der Nutzerinnen und Nutzer böten, kontrolliert, ob das Alter der Befragten hierbei eine Rolle spielt, was aufgrund fehlender Signifikanz ausgeschlossen werden konnte.

Tabelle 4: Gruppenunterschiede hinsichtlich der Bedenken der Preisgabe von Daten.

	Durchschnittliche Bedenken, im Internet persönliche Daten preiszugeben[a]	**F**	**N**
Grad der Zustimmung zur Aussage «Die meisten staatlichen Institutionen behandeln die personenbezogenen Daten, die sie über Nutzerinnen und Nutzer sammeln, ordnungsgemäss und vertraulich.»		2.886*	
Keine Zustimmung	8.89		9
Eher keine Zustimmung	7.11		120
Eher Zustimmung	7.02		329
Volle Zustimmung	6.64		42
Insgesamt	7.05		500
Grad der Zustimmung zur Aussage «Bestehende Gesetze und organisatorische Praktiken bieten einen ausreichenden Schutz der Privatsphäre»		5.945***	
Keine Zustimmung	8.12		34
Eher keine Zustimmung	7.25		227
Eher Zustimmung	6.72		217
Volle Zustimmung	6.55		22
Insgesamt	7.05		500

Anmerkung: * $p \leq .05$,** $p \leq .01$,*** $p \leq .001$, [a] Die Frage hierzu lautete: Ganz allgemein: Wie gross sind Ihre Bedenken, persönliche Daten im Internet preiszugeben? 1 heisst, dass Sie überhaupt keine Bedenken haben und 10 heisst, dass Sie sehr grosse Bedenken haben, persönliche Daten im Internet preiszugeben. Mit den Zahlen dazwischen können Sie Ihre Meinung abgestuft benoten.

Entsprechend der Zustimmung zu obengenannter Aussage wurde danach untersucht, ob sich die Gruppen in der Ausprägung ihrer Bedenken, im Internet persönliche Daten preiszugeben, unterschieden (**Tabelle 4**). Auch hierbei deuten die Ergebnisse einer einfaktoriellen Varianzanalyse darauf hin, dass diejenigen, welche die Ansicht vertreten, dass bestehende Gesetze und organisatorische Praktiken heute ein angemessenes Schutzniveau für die Privatsphäre der Nutzerinnen und Nutzer bieten, signifikant geringere Bedenken aufweisen, im Internet persönliche Daten preiszugeben ($F(3,496) = 5.945$, $p = .001$).

Dass 74 Prozent der Befragten der Ansicht sind, die meisten staatlichen Institutionen würden die von ihnen gesammelten persönliche Daten ordnungsgemäss behandeln, zeugt von grundsätzlichem Vertrauen gegenüber diesen Institutionen. Gleichzeitig zeigten die Befragten auch eine Erwartungshaltung gegenüber dem Staat zur Sicherung von Datenschutz. So nennen 63 Prozent den Staat als Hauptverantwortlichen in der Gewährleistung von Datensicherheit und Datenschutz. 32 Prozent sehen die Verantwortung bei privaten Unternehmen, während die restlichen Befragten weitere Verantwortliche nennen oder die Verantwortung gleichermassen bei privaten Unternehmen sowie dem Staat sehen (N = 500). Jene Befragten, die Unternehmen mehrheitlich in der Pflicht sehen, Datensicherheit und Datenschutz hauptsächlich zu gewährleisten, haben ein höheres Vertrauen in privatwirtschaftliche Unternehmen (M = 6.15, SD = 1.76) verglichen mit jenen, welche primär den Staat in der Verantwortung sehen (M = 5.36, SD = 1.92), $t(470) = -4.364$, $p = .000$). Umgekehrt konnte aber nicht gezeigt werden, dass jene, die den Staat als Hauptverantwortlichen in der Gewährleistung des Datenschutzes sehen (M = 6.67, SD = 1.87), ein signifikant stärkeres Vertrauen in den Staat hätten als jene, die privatwirtschaftliche Unternehmen in der Verantwortung sehen (M = 6.44, SD = 1.96), $t(470) = 1.217$, $p = .224$).

5 Diskussion

Auf der individuellen Ebene zeigt die vorliegende Untersuchung, dass unter den Befragten kein einheitliches Bild bezüglich des Wissens um die rechtliche Datenschutzgrundlage besteht. Von den Befragten wurde das gesamte Spektrum an Vertrautheit mit der Gesetzgebung abgedeckt. Während einige damit nicht vertraut waren, zeigten andere starke Vertrautheit. So war fast jeder Zehnte der Befragten nicht in der Lage, einen

beliebigen Begriff zu nennen, den er oder sie mit Datenschutz assoziiert. Spontan verband kaum jemand der Befragten Datenschutz mit Gesetzen. Auch waren sich die Befragten nicht einig, ob bestehende Gesetze die Privatsphäre der Nutzerinnen und Nutzer angemessen schützen. Die Wissenslage um die rechtlichen Grundlagen des Datenschutzes ist bei den Befragten sehr heterogen und generell ausbaufähig.

Die Resultate implizieren darüber hinaus, dass Bürgerinnen und Bürger mit Datenschutz insbesondere mögliche Gefahren assoziieren. Gleichzeitig sind ihnen die Wahrung der Privatsphäre und der eigenen persönlichen Daten sehr wichtig. Ferner weisen die Ergebnisse auf ein insgesamt relativ hohes Mass an Bedenken bezüglich des Schutzes der persönlichen Daten unter den Befragten hin. Insbesondere Aspekte, die den Missbrauch und die Weiterverwendung persönlicher Daten betreffen, führen demnach zu grosser Besorgnis unter den Befragten. Dies deutet daraufhin, dass die Verletzung des Schutzes persönlicher Daten als reale Bedrohung wahrgenommen wird. Damit stützt die Untersuchung die Resultate anderer Studien, die ebenfalls ein grosses Mass an Bedenken um die Gewährung der Privatsphäre bei der Bevölkerung feststellen (siehe bspw. Dutton & Blank, 2013; Pleger, Guirguis & Mertes, 2021).

Dass Bürgerinnen und Bürger einerseits nicht einheitlich vertraut sind mit der dem Datenschutz zu Grunde liegenden Gesetzeslage und andererseits viele Gefahren im Kontext von Datenschutz wahrnehmen, betont die Wichtigkeit einer angemessenen Kommunikation und medialen Berichterstattung der Einführung des neuen Datenschutzgesetzes in der Schweiz. Gemäss Renn & Kastenholz (2008, S. 105) ist «Risikokommunikation eine notwendige Voraussetzung für die rationale Bewertung und Bewältigung von technischen Risiken.».. Es ist sowohl im Sinne des Staates als auch seiner Bürgerinnen und Bürger, wenn die Bevölkerung über die gesetzliche Grundlage des Datenschutzes informiert ist und sich deren Bedeutung bewusst ist (siehe bspw. Hauck & Lötscher, 1994).

Mit der im Rahmen der Gesetzesrevision neu aufkommenden Informationspflicht soll unter anderem auch das Ziel einer verstärkten Sensibilisierung der Bevölkerung im Umgang mit Daten erreicht werden. Dadurch sollen Nutzerinnen und Nutzer zukünftig über ein besseres Wissen im Zusammenhang mit Datenschutz verfügen und somit einen sensibleren Umgang mit ihren Daten pflegen und sich besser vor Eingriffen in ihre Privatsphäre schützen können. Insofern trägt die Revision mit der aus Art. 17 E-DSG hervorgehenden Informationspflicht dazu bei, dass Nutzerinnen und Nutzer ein stärkeres Bewusstsein für das Thema Datenschutz entwickeln und sich eingehender damit auseinandersetzen.

Das individuelle Verhalten von Bürgerinnen und Bürgern ist jedoch hochkomplex, was durch das geschilderte *Privacy Paradox* verdeutlicht wird. Reine Information mag nicht zu verhindern, dass Individuen nicht wider besseren Wissens ihre Privatsphäre gefährden (siehe bspw. Oomen & Leenes, 2008). Die Existenz des Privacy Paradox bedeutet nicht, dass nicht auch die Bürgerinnen und Bürger in der Pflicht seien, sich aktiv zu bemühen, Informationen hinsichtlich des Datenschutzes zu verstehen, um ihre Verhaltensweise besser reflektieren zu können. So argumentieren beispielsweise Dinev et al. (2015), dass stärkere Bemühungen hinsichtlich des Verhaltens zum Schutz der eigenen Privatsphäre dazu führen können, dass Informationen besser verarbeitet werden, was wiederum das eigene Verhalten beeinflussen kann. Wichtig für ein datenschützendes Verhalten scheinen also unter anderem neben reiner Information auch die eigenen Bemühungen zu sein.

Die Resultate deuten ausserdem darauf hin, dass je grösser das Vertrauen in die geltenden Gesetze bezüglich des Datenschutzes ist, desto tiefer die Bedenken sind, Daten im Internet preiszugeben. Um Vertrauen in Gesetze haben zu können, müssen diese zumindest in den Grundzügen verstanden werden. Die hier präsentierten Ergebnisse zeigen, dass das Wissen der Befragten bezüglich der gesetzlichen Rahmenbedingungen verbesserungsbedürftig ist. Die Verständlichkeit von Gesetzen ist für das Funktionieren eines modernen Rechtsstaats unerlässlich (siehe bspw. Hauck & Lötscher, 1994). Rechtssicherheit «ist nur möglich, wenn ein Gesetz von allen gleich und gleich eindeutig verstanden werden kann» (Hauck & Lötscher, 1994, S. 91). Entsprechend wichtig ist es somit, bei der Formulierung von Gesetzen sicherzustellen, dass diese für die Bevölkerung verständlich sind. Das Wissen um die rechtlichen Rahmenbedingungen des Datenschutzes hilft der Bevölkerung dabei, dieses Recht auch einzufordern. Indem die Bürgerinnen und Bürger das Gesetz besser kennen, können sie auch besser abschätzen, welchen Schutz dieses bietet und welchen Beitrag sie selbst leisten können beziehungsweise zu leisten haben. Damit knüpfen die Resultate unserer Studie an frühere Ergebnisse an, die betonen, dass Kommunikationsbemühungen über die Gesetzeslage dazu beitragen können, die Unsicherheit über den Schutz ihrer Daten bei Individuen zu reduzieren (siehe bspw. Lwin et al., 2007). Für die staatliche Perspektive implizieren die Resultate folglich die Wichtigkeit, rechtliche Grundlagen – wie im konkreten Fall das revidierte Datenschutzgesetz – verständlich zu kommunizieren, sodass dieses von der Bevölkerung verstanden wird.

Ferner sind für den Staat und staatliche Organisationen insbesondere die Resultate zum Vertrauen relevant. Studien zeigen die Tendenz auf, dass Bedenken bezüglich der Privatsphäre umso tiefer ausfallen, je grösser das Vertrauen in die sachgemässe Handhabung von Daten ist (siehe bspw. Dinev et al., 2015; Joinson et al., 2010). Dies bestätigen auch die Resultate der vorliegenden Studie und es zeigt sich im Allgemeinen, dass die Befragten ein grosses Vertrauen in die sachgemässe Nutzung personenbezogener Daten durch staatliche Institutionen haben. Für den öffentlichen Sektor ist das ein positives Ergebnis – wobei im Umkehrschluss auch beachtet werden muss, dass etwa ein Viertel der Befragten ein geringeres Vertrauen aufwies. Dass die meisten Befragten den Staat als primär verantwortlich für die Gewährleistung von Datenschutz und Datensicherheit sehen, zeigt, welch grosse Verantwortung dem Staat diesbezüglich zugewiesen wird. In Zeiten von Open Data und einer allgemeinen Zunahme von Datenerfassung, -sammlung und -speicherung auch durch staatliche Organisationen gilt es, das vorhandene Vertrauen nicht zu verspielen und es bei jenen Personen zurückzugewinnen, die gegenwärtig kein Vertrauen in die sachgemässe Nutzung personenbezogener Daten durch den Staat haben. Nur so kann der Staat den Erwartungen an seine Gewährleistungsverantwortung auch gerecht werden und diese erfüllen.

Die Resultate deuten darauf hin, dass je höher das Vertrauen in den Staat ist, desto tiefer fallen die Bedenken, Daten im Internet preiszugeben, aus. Damit sind sie vergleichbar mit den Ergebnissen aus anderen Untersuchungen: So zeigen sich Bürgerinnen und Bürger beispielsweise auch gemäss Büllesbach (2008) eher dazu bereit, wahrheitsgetreue Angaben zu machen, wenn sie sicher sind, dass die Daten ordnungsgemäss verwendet werden. Ein Ansatz, der verfolgt werden könnte, um die Bedenken bei den Bürgerinnen und Bürgern zu lindern, besteht demnach darin, das Vertrauen in den Staat als Verantwortlichen der Gewährleistung des Datenschutzes zu erhöhen. Dabei ist einerseits auf die bereits angesprochene transparente und verständliche Kommunikation des neuen Datenschutzgesetzes Wert zu legen, andererseits können der Staat und staatliche Organisationen das ihnen von der Bevölkerung entgegengebrachte Vertrauen stärken, indem sie diese transparent über die Verwendung ihrer Daten informiert.

6 Ausblick und Limitationen

Vor dem Hintergrund der Revision des Datenschutzgesetzes in der Schweiz widmete sich der vorliegende Artikel den Fragen, welche Aspekte von Datenschutz für Schweizer Einwohnerinnen und Einwohner relevant sind und welche Bedenken sie haben. Ausserdem wurde die Rolle des Staates dabei untersucht. Datenschutz ist wie eingangs erklärt kein Phänomen, das sich nur auf individueller und staatlicher Ebene manifestiert, sondern auch auf organisationaler Ebene von Bedeutung ist. Entsprechend folgt an dieser Stelle ein Ausblick bezogen auf diese drei Ebenen.

Die Ergebnisse aus einer Online-Befragung unter 500 in der Deutschschweiz wohnhaften Personen haben auf individueller Ebene gezeigt, dass Datenschutz viele negative Assoziationen und Ängste hervorruft. Umso wichtiger ist den Befragten die Sicherung ihrer Privatsphäre und persönlichen Daten. Weiter zeigen die Resultate, dass die Bedenken von Schweizer Einwohnerinnen und Einwohnern hinsichtlich des Datenschutzes relativ stark ausgeprägt sind und insbesondere eine starke Angst vor Datenmissbrauch herrscht. Datenschutz stellt aus der Perspektive von Individuen ein komplexes Phänomen dar. Insbesondere scheinen die Information und das Wissen über Datenschutz bei Bürgerinnen und Bürgern nicht ausreichend vorhanden, um ihre Bedenken angemessen einzuordnen.

Für (staatliche) Organisationen bedeutet dies, dass sie den Bedenken der Bevölkerung begegnen können, indem sie Wert auf eine transparente Darlegung der Verwendung der gesammelten Daten legen. Durch eine Schaffung von Vertrauen können individuelle Bedenken gelindert werden, was im Sinne der datenverarbeitenden Organisationen ist. Die Befunde legen nahe, dass das Vertrauen in staatliche Organisationen hoch ist. Letztendlich ist es auch im Eigeninteresse der Organisationen, den Datenschutz zu gewährleisten, da ansonsten Sanktionen gemäss dem revidierten Datenschutzgesetz drohen. Staatliche Organisationen aller Ebenen sollten deshalb ihre Verantwortung zum sachgemässen Umgang mit Daten und die Bedenken der Einwohnerinnen und Einwohner ernst nehmen und für vermehrte Transparenz im Datenschutz sorgen, sodass sich diese hinsichtlich ihrer Daten verantwortungsvoller verhalten können.

Dem Staat kommt insbesondere bei der Information der Bevölkerung eine wichtige Funktion zu, indem es nicht ausreicht, wenn der Staat in Form einer angemessenen Gesetzeslage für Schutz sorgt – beispielsweise durch die Revision des Datenschutzgesetzes in der Schweiz. Vielmehr soll er auch für eine angemessen Kommunikation und Information der Bürgerinnen und Bürger über die Grundsätze des Datenschutzes sorgen, sodass diese ihren Bedenken hinsichtlich möglicher Datenschutzverletzungen begegnen können. Die Befunde zeigen auf, dass der Staat für die Erfüllung dieser Anforderungen insofern eine optimale Ausgangslage hat, als das Vertrauen in den Staat insgesamt hoch ist.

Die vorliegende Studie baut auf einer merkmalsspezifischen nicht-probabilistischen Quotenstichprobe basierend auf den Merkmalen Alter und Geschlecht auf. Entsprechend ist sie für diese Merkmale repräsentativ, enthält aber bezüglich nicht einbezogener Merkmale mögliche Verzerrungen. So sind beispielsweise leichte Verzerrungen aufgrund der Merkmale Bildungsabschluss und Wohnregion denkbar, die in der vorliegenden Studie nicht als Quoten, sondern zur Ex-Post-Überprüfung beigezogen wurden. Weitere Studien könnten hier anknüpfen und den Sachverhalt anhand weiterer Merkmale (beispielsweise Einkommen oder Herkunft) untersuchen. Ebenso bezieht sich die vorliegende Studie ausschliesslich auf die Deutschschweiz. Eine Studie, die alle Schweizer Sprachregionen einbezöge, könnte weitere hilfreiche Hinweise auf die Situation in der gesamten Schweiz liefern.

Zukünftige Forschung kann an diesen Resultaten anknüpfen, indem beispielsweise die hier dargestellten quantitativen Resultate mit qualitativen Informationen aus Interviews ergänzt würden. Datenschutz aus individueller Perspektive ist ein Forschungsfeld, welches in der Forschung bis anhin nur wenig Beachtung erfahren hat, weswegen weitere Studien, welche vertieft die komplexen Interaktionen auf individueller Ebene untersuchen, dazu beitragen können, das Verständnis über Datenschutz zu steigern. Weitere empirische Befunde zu Datenschutz aus der Perspektive der Bürgerinnen und Bürger könnten in der Praxis für den Staat und staatliche Organisationen zudem als evidenzbasierte Hilfestellung fungieren, um zu analysieren, welche Kommunikationsmassnahmen nötig sind, um den Bedenken von Bürgerinnen und Bürgern adäquat zu begegnen und das Vertrauen in den Staat und staatliche Organisationen weiterhin hoch zu halten.

Additional Files

The additional files for this article can be found as follows:

- **Appendix A.** Ex-post-Validierung der Merkmale *Höchster Bildungsabschluss* und *Wohnsitzregion* sowie deskriptive Statistiken. DOI: https://doi.org/10.5334/ssas.153.s1
- **Appendix B.** Zusammenfassende Statistiken und Häufigkeiten. DOI: https://doi.org/10.5334/ssas.153.s2

Konkurrierende Interessen

Die Autorinnen und Autoren haben keine konkurrierenden Interessen zu erklären.

Literaturverzeichnis

Barth, S., & **de Jong, M. D. T.** (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058. DOI: https://doi.org/10.1016/j.tele.2017.04.013

Bock, K., & **Meissner, S.** (2012). Datenschutz-Schutzziele im Recht: Zum normativen Gehalt der Datenschutz-Schutzziele. *Datenschutz und Datensicherheit – DuD*, *36*(6), 425–431. DOI: https://doi.org/10.1007/s11623-012-0152-0

Büllesbach, A. (2008). Persönlichkeitsschutz in der Informationsgesellschaft. In *Informationelles Vertrauen für die Informationsgesellschaft* (S. 215–224). Berlin, Heidelberg: Springer. DOI: https://doi.org/10.1007/978-3-540-77670-3_16

Bundesamt für Statistik. (2000, Dezember 31). *Grossregionen und Kantone der Schweiz*. https://www.bfs.admin.ch/bfs/de/home/statistiken/querschnittsthemen/raeumliche-analysen/raeumliche-gliederungen/analyseregionen.assetdetail.1031445.html

Bundesamt für Statistik. (2020a, Oktober 8). *Ständige Wohnbevölkerung in Privathaushalten nach Kanton und Haushaltsgrösse, 2010–2019*. https://www.bfs.admin.ch/bfs/de/home/statistiken/bevoelkerung/stand-entwicklung.assetdetail.14407048.html

Bundesamt für Statistik. (2020b, Dezember 16). *Höchste abgeschlossene Ausbildung, nach Migrationsstatus, verschiedenen soziodemografischen Merkmalen und Grossregion*. https://www.bfs.admin.ch/bfs/de/home/statistiken/bevoelkerung/migration-integration/integrationindikatoren/indikatoren/abgeschlossene-ausbildung.assetdetail.14876535.html

Bundesverfassung der Schweizerischen Eidgenossenschaft, § **Artikel 13.** (1999). https://www.admin.ch/opc/de/classified-compilation/19995395/index.html

Dinev, T., McConnell, A. R., & **Smith, H. J.** (2015). Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box. *Information Systems Research*, *26*(4), 639–655. DOI: https://doi.org/10.1287/isre.2015.0600

Döring, N., & **Bortz, J.** (2016). Stichprobenziehung. In *Forschungsmethoden und Evaluation in den Sozial- und Humanwissenschaften* (S. 291–319). Berlin, Heidelberg: Springer. DOI: https://doi.org/10.1007/978-3-642-41089-5_9

Dutton, W. H., & **Blank, G.** (2013). *Cultures of the Internet: The Internet in Britain*, 64.

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB. (2015). *Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes*. https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2018/TOM.pdf.download.pdf/guideTOM_de_2015.pdf

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB. (2021, Januar 13). *Datenschutz*. https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/ueberblick/datenschutz.html#1934 11080

Eurostat. (2019). *https://ec.europa.eu/eurostat/home*

Ginosar, A., & **Ariel, Y.** (2017). An analytical framework for online privacy research: What is missing? *Information & Management*, *54*(7), 948–957. DOI: https://doi.org/10.1016/j.im.2017.02.004

Griesinger, M. (2020). Ein Überblick über das neue Schweizer Datenschutzgesetz (DSG). *PinG Privacy in Germany*, *1*, 11. DOI: https://doi.org/10.37307/j.2196-9817.2021.01.11

Hallam, C., & **Zanella, G.** (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, *68*, 217–227. DOI: https://doi.org/10.1016/j.chb.2016.11.033

Hallinan, D., Friedewald, M., & **McCarthy, P.** (2012). Citizens' perceptions of data protection and privacy in Europe. *Computer Law & Security Review*, *28*(3), 263–272. DOI: https://doi.org/10.1016/j.clsr.2012.03.005

Hauck, W., & **Lötscher, A.** (1994). *Verständlichkeit von Gesetzen als Problem der Gesetzgebung*, 9.

Husi-Stämpfli, S. (2018). Die DSG-Revision oder: Ein Beziehungsdrama in drei Akten… *Mai*, 11.

Isaak, J., & **Hanna, M. J.** (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*, *51*(8), 56–59. DOI: https://doi.org/10.1109/MC.2018.3191268

Jantz, B., & **Veit, S.** (2019). Entbürokratisierung und bessere Rechtsetzung. In *Handbuch zur Verwaltungsreform* (S. 509–520). Springer VS. DOI: https://doi.org/10.1007/978-3-658-21563-7_45

Joinson, A., Reips, U.-D., Buchanan, T., & **Schofield, C. B. P.** (2010). Privacy, Trust, and Self-Disclosure Online. *Human-Computer Interaction*, *25*(1), 1–24. DOI: https://doi.org/10.1080/07370020903586662

Jorzig, A., & **Sarangi, F.** (2020). *Digitalisierung im Gesundheitswesen: Ein kompakter Streifzug durch Recht, Technik und Ethik*. Berlin, Heidelberg: Springer. DOI: https://doi.org/10.1007/978-3-662-58306-7

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. DOI: https://doi.org/10.1016/j.cose.2015.07.002

Kummer, M., & **Schulte, P.** (2016). *When Private Information Settles the Bill: Money and Privacy in Google's Market for Smartphone Applications. Discussion Paper No. 16-031. Centre for European Economic Research*. http://ftp.zew.de/pub/zew-docs/dp/dp16031.pdf. DOI: https://doi.org/10.2139/ssrn.2764907

Lwin, M., Wirtz, J., & **Williams, J. D.** (2007). Consumer online privacy concerns and responses: A power–responsibility equilibrium perspective. *Journal of the Academy of Marketing Science*, *35*(4), 572–585. DOI: https://doi.org/10.1007/s11747-006-0003-3

Oomen, I., & **Leenes, R.** (2008). Privacy risk perceptions and privacy protection strategies. In *Policies and research in identity management* (S. 121–138). Boston, MA: Springer. DOI: https://doi.org/10.1007/978-0-387-77996-6_10

Petrlic, R., & **Sorge, C.** (2017). *Datenschutz*. Wiesbaden: Springer Fachmedien. DOI: https://doi.org/10.1007/978-3-658-16839-1

Pleger, L. E., Guirguis, K., & **Mertes, A.** (2021). Making public concerns tangible: An empirical study of German and UK citizens' perception of data protection and data security. *Computers in Human Behavior*, *122*, 106830. DOI: https://doi.org/10.1016/j.chb.2021.106830

Pommerening, K. (1991). *Datenschutz und Datensicherheit*. BI-Wiss.-Verlag.

Renn, O., & **Kastenholz, H.** (2008). Vertrauensverlust in Institutionen: Herausforderung für die Risikokommunikation. In *Informationelles Vertrauen für die Informationsgesellschaft* (S. 103–120). Berlin, Heidelberg: Springer. DOI: https://doi.org/10.1007/978-3-540-77670-3_8

Roßnagel, A. (2020). Vier Fragen der Redaktion zur Datenschutz-Grundverordnung an Alexander Roßnagel. *Informatik Spektrum*, *43*(5), 319–323. DOI: https://doi.org/10.1007/s00287-020-01300-4

Schaar, P. (2020). Datenschutz und Internet – Es ist kompliziert! *Informatik Spektrum*, *43*(3), 179–185. DOI: https://doi.org/10.1007/s00287-020-01275-2

Schmidt, K. J. (2020). *Datenschutz als Vermögensrecht: Datenschutzrecht als Instrument des Datenhandels*. Wiesbaden: Springer Fachmedien. DOI: https://doi.org/10.1007/978-3-658-30797-4

Schweizerische Eidgenossenschaft. (2019). *Stärkung des Datenschutzes. Revision des Bundesgesetzes über den Datenschutz (DSG).* https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html

Schweizerisches Parlament. (2020a). *Datenschutzgesetz. Totalrevision und Änderung weiterer Erlasse zum Datenschutz*. https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20170059

Schweizerisches Parlament. (2020b). *Gesetzgebung.* https://www.parlament.ch/de/%C3%BCber-das-parlament/parlamentsportraet/aufgaben-der-bundesversammlung/rechtsetzung/gesetzgebung

Sury, U. (2017). Revision Datenschutz in der Schweiz. *Informatik-Spektrum*, *40*(2), 221–226. DOI: https://doi.org/10.1007/s00287-017-1022-9

Sutanto, J., Palme, E., Tan, C.-H., & **Phang, C. W.** (2013). Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users. *MIS Quarterly*, *37*(4), 1141–1164. JSTOR. DOI: https://doi.org/10.25300/MISQ/2013/37.4.07

Tuttle, H. (2018). Facebook scandal raises data privacy concerns. *Risk Management*, *65*(5), 6–9.

Vereinte Nationen. (1948). *Resolution der Generalversammlung. 217 A (III). Allgemeine Erklärung der Menschenrechte*. https://www.un.org/depts/german/menschenrechte/aemr.pdf

Von Lewinski, K. (2012). *Zur Geschichte von Privatsphäre und Datenschutz–eine rechtshistorische Perspektive. Datenschutz–Grundlagen, Entwicklungen und Kontroversen*. Bonn: BPB Verlag.

Westin, A. F. (2003). Social and Political Dimensions of Privacy. *Journal of Social Issues*, *59*(2), 431–453. DOI: https://doi.org/10.1111/1540-4560.00072

Witt, B. C. (2010). *Datenschutz kompakt und verständlich: Eine praxisorientierte Einführung; [mit Online-Service]* (2., aktualisierte und erg. Aufl). Vieweg + Teubner. DOI: https://doi.org/10.1007/978-3-8348-9653-7

Yun, H., Lee, G., & **Kim, D. J.** (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. *Information & Management*, *56*(4), 570–601. DOI: https://doi.org/10.1016/j.im.2018.10.001

How to cite this article: Guirguis, K., Pleger, L. E., Dietrich, S., Mertes, A., & Brüesch, C. (2021). Datenschutz in der Schweiz – eine quantitative Analyse der gesellschaftlichen Bedenken und Erwartungen an den Staat. *Swiss Yearbook of Administrative Sciences,* 12(1), pp. 16–30. DOI: https://doi.org/10.5334/ssas.153

Submitted: 08 February 2021 **Accepted:** 28 April 2021 **Published:** 23 June 2021

]u[*Swiss Yearbook of Administrative Sciences* is a peer-reviewed open access journal published by Ubiquity Press.

OPEN ACCESS