IRDG Institut für das Recht der digitalen Gesellschaft

UNIVERSITY OF PASSAU Faculty of Law

UNIVERSITY OF PASSAU IRDG RESEARCH PAPER SERIES NO. 23-5

CULTURAL INFLUENCES ON PERSONAL DATA DISCLOSURE DECISIONS

Swiss Perspectives

Veronika Thir, Daniela Wawra, Katharina Kindsmüller and Vanessa Vollenschier

June 2023

Place of Publication

Institute for Law of the Digital Society, University of Passau

c/o Chair of German and European Private Law, Civil Procedure, and Legal Theory

Innstraße 39, 94032 Passau

https://www.jura.uni-passau.de/irdg/

Authors

Daniela Wawra is professor of linguistics and cultural studies at the University of Passau. Veronika Thir is a research assistant in the project *Vectors of data disclosure – A comparative study of the use of personal data from a legal, cultural studies, and information systems perspective*. The co-authors are student assistants. They work together in an interdisciplinary research team that explores the disclosure of personal data from a legal, cultural studies, and information systems perspective.

Abstract

This paper provides an overview of survey findings from Switzerland on key parameters that can influence the willingness to share (WTS) personal data. It provides insights into Swiss mentalities towards data disclosure on a macro level and thus into the cultural preconditions of information governance. This 'country report' is one of several that have been compiled as part of the interdisciplinary project *Vectors of data disclosure – A comparative study of the use of personal data from a legal, cultural studies, and information systems perspective*[1], funded by the Bavarian Research Institute for Digital Transformation[2].

Cite as

Thir, V., Wawra, D. et al. (2023). Cultural Influences on Personal Data Disclosure Decisions – Swiss Perspectives. *University of Passau Institute for Law of the Digital Society Research Paper Series No. 23-5*. https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/.

Keywords

Culture, Data Disclosure, Digitalization, Information Governance, Privacy, Switzerland, Willingness to Share (WTS) Data.

---

[1] Lead principal investigator: Moritz Hennemann, further principal investigators: Kai von Lewinski, Daniela Wawra, and Thomas Widjaja; external advisor: Urs Gasser.

[2] https://www.bidt.digital/ (last access: 03/13/2023).

Contents

I. Introduction

This paper focuses on cultural influences on the willingness to share (WTS) personal data as expressed in surveys that reflect the prevailing views, assumptions, attitudes, evaluations, and reported behaviors of Swiss citizens and residents regarding data disclosure. As a first step in our research project, we focus on surveys in order to get a general picture of a culture's mentality towards data disclosure based on as broad a data base as possible. This provides us with insights into the cultural preconditions of information governance in Switzerland. Our approach can be described as a macro-level analysis (cf. Wawra 2022). We have compiled similar 'reports' for other countries in our project[3], as we are planning a cross-cultural comparative study as a next research step. This has also led to the decision that we will primarily rely on extensive global surveys in our reports whenever possible in order to facilitate the following country comparisons. Secondarily, we have integrated surveys that cover at least some of our study countries. When international surveys lacked data on a particular country, we resorted to national surveys. Wawra (2022) is an introduction to our project from a cultural perspective, providing background information on the research context and detailing the cultural research design. The paper also introduces the parameters according to which all our cultural reports are structured. The following parameters have been identified as central to capturing the narrower cultural context of data disclosure decisions on a macro level (cf. Wawra 2022): Digital Competitiveness (section III.), General Value of Informational Privacy (IV.), Degree of Privacy of Data (V.), Benefits Associated with Data Disclosure (VI.), Privacy Concerns and Risks (VII.), Data Protection Literacy (VIII.), Attitudes towards Data Receiver (IX.), and Communication on Data Use (X.) (see Fig. 1). Data Protection Laws is another parameter that is detailed in separate legal country reports. Depending on the specific situational context, all parameters may have more or less influence on people's willingness to share (WTS) personal data. Overall, the structure of the country reports that have been compiled in our project is the same. The descriptions of the individual parameters have been adopted from Wawra (2022) and are given in italics.

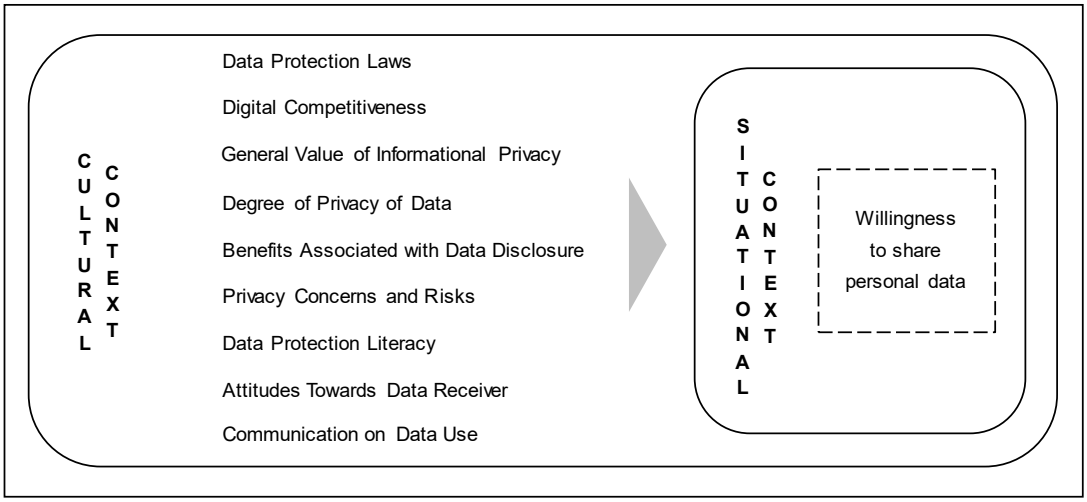

Fig. 1. Central parameters of data disclosure (from Wawra 2022).

[3] The first report produced as part of our project focuses on the US context (cf. Kessel 2022).

II. Selected Survey Data

Crucially, Switzerland was not included in several large-scale, international surveys (Bruce 2021; CIGI-Ipsos 2019a, b, c; Cisco 2021; GfK 2017; Ipsos 2019). This report therefore summarizes relevant findings primarily from large recent national surveys on informational privacy, data control, data protection, and data disclosure in Switzerland. Where available, findings from international surveys are reported as well. The sample size was usually 1000 or more and always comprised at least 500 respondents. Appendix 1 provides an overview and details of the surveys included, such as sample size and demographic information on respondents.

Switzerland consists of four different language regions: German-speaking, French-speaking, Italian-speaking, and Romansh-speaking Switzerland. It is possible that these regions exhibit cultural differences regarding people's views and assumptions on data-related matters and their behavior towards data disclosure. Unfortunately, no survey examining such differences could be found for the parameters studied here.[4] However, most of the surveys were either representative of the three largest language regions of Switzerland (German-, French- and Italian-speaking parts of Switzerland)[5] or at least included respondents from all three language regions. Two further studies were representative of the German- and French speaking population of Switzerland. For more details, see the description of the survey demographics in Appendix 1.

III. Digital Competitiveness

[The parameter Digital Competitiveness] is understood in the sense of the "IMD World Digital Competitiveness Ranking" (WDCR), a well-established and widely accepted regularly published ranking, as the "capacity of economies to use digital technologies to transform themselves" (IMD 2021, p. 3). The WDCR "analyzes and ranks the extent to which countries adopt and explore digital technologies leading to transformation in government practices, business models and society in general" (IMD 2021, p. 32).[6] *Specifically, the WDCR aggregates scores to compare 64 countries in terms of 52 criteria relating to "knowledge", "technology", and "future readiness" (IMD 2021, p. 3, 32, 33). Knowledge describes the "[k]now-how necessary to discover, understand and build new technologies" (IMD 2021, p. 33) and is further divided into the subfactors of talent, training and education, as well as scientific concentration relating to, e.g., expenditure on research & development, and high-tech patent grants. The factor technology comprises the "[o]verall context that enables the development of digital technologies" (IMD 2021, p. 33), including the subfactors "regulatory framework", "capital", and "technological framework". Future readiness explains the "[l]evel of country preparedness to exploit digital transformation" (IMD 2021, p. 33) and measures adaptive attitudes, business agility, and IT integration to rank the level of how countries are prepared for exploiting digital transformation (cf. IMD 2021, p. 33).*[7]

For its overall performance, Switzerland is ranked 6th out of 64 countries in 2021 for digital competitiveness. Switzerland receives the 1st rank for its advances in **knowledge**, 11th rank in the category **technology**, and 3rd rank in the **future readiness** for digitalization. When looking at the

---

[4] However, for language-regional differences regarding the uptake and use of the SwissCovid App, see Geber and Friemel (2021) and von Wyl et al. (2021).

[5] Data from 2020 shows that only 0.5% of the permanent resident population in Switzerland uses Romansh as their main language, whereas 62.3% use German, 22.8% use French, 8.0% use Italian and 23.1% use a 'non-national' language, such as English or Portuguese (cf. Federal Statistical Office 2022; respondents could name more than one main language).

[6] Wawra (2022, IV. 2.).

[7] The paragraph from "Specifically […]" to "transformation […]" has been added in all country reports and taken verbatim from the first country report (Kessel 2022).

development over five years, Switzerland's rankings have mostly improved: Overall (from 8th in 2017 to 6th in 2021), as well as in the categories **knowledge** (from 4th in 2017 to 1st in 2021) and **future readiness** (from 13th in 2017 to 3rd in 2021). Only the **technology** ranking has deteriorated slightly (from 8th in 2017 to 11th in 2021) (cf. IMD 2021, p. 158).

Rankings of the subfactors with regard to **knowledge** place Switzerland 3rd in the subfactor **talent** and 11th for the digital and technological skills of staff, which is one of the items of this subfactor. Switzerland ranks 7th in the **training and education** subfactor and 8th in **scientific concentration**[8] (cf. IMD 2021, p. 159).

In the field of **technology**, Switzerland ranks at least among the top 20% of all countries for all three subfactors (regulatory framework, capital and technological framework). It ranks 9th in the subfactor **regulatory framework** and 6th in development & application of technology, but only 37th in starting a business (two of the items of this subfactor). Switzerland occupies 12th place in the subfactor capital and 9th place in the funding of technological development. It ranks 11th for the subfactor **technological framework**[9], and here 8th for communications technology (cf. IMD 2021, p. 159). Overall, Switzerland is among the top 20-30% of all countries regarding most items in the field of technology; for the others, it is mostly in the midfield.

In terms of **future readiness**, Switzerland ranks 10th for the subfactor **adaptive attitudes**, 4th for **business agility** and 4th for **IT integration**. In the adaptive attitudes subfactor, it ranks 18th for e-participation[10] and 4th for smartphone ownership. In the business agility subfactor, it occupies 23rd place for the use of big data and analytics. In the final subfactor, IT integration, it ranks 16th for e-government[11] and 7th for cyber security (cf. IMD 2021, p. 159).

IV. General Value of Informational Privacy

Informational privacy is understood "as the claim of an individual to determine what information about himself or herself should be known to others" (Westin 2003, p. 431) and as the demand to be protected from unwanted access to personal data (Rössler 2001, p. 25). [This] parameter […] indicates how important or unimportant [respondents from Switzerland consider this demand].[12]

The following survey questions allow conclusions to be drawn in this regard. The World Values Survey (cf. EVS/WVS 2021a, b) asked respondents from Switzerland to assess the governmental collection of personal data for surveillance purposes. A majority of Swiss respondents approve of governmental video surveillance in public: 62% agree that their government should have this right (cf. EVS/WVS 2021c, p. 428) (Fig. 2).

---

[8] The subcategory "scientific concentration" comprises the items "Total expenditure on R&D (%) (Percentage of GDP)" (R&D=Research and Development), "Total R&D personnel per capita (Full-time work equivalent (FTE) per 1000 people)", "Female researchers (% of total (headcount FT&PT))", "R&D productivity by publication (No. of scientific articles over R&D expenditure (as % GDP))", "Scientific and technical employment (% of total employment)", "High-tech patent grants (% of all patents granted by applicant's origin (average 2014-2016))", and "Robots in Education and R&D (number of robots)" (IMD 2021, p. 180).

[9] The subcategory "technological framework" includes the items "Communications technology" (IMD 2021, p. 105), "Mobile broadband subscribers (4G & 5G market, % of mobile market)", "Wireless broadband (Penetration rate (per 100 people))", "Internet users (Number of Internet users per 1000 people)", "Internet bandwidth speed (Average speed)", and "High-tech exports (%) (Percentage of manufactured exports)" (IMD 2021, p. 181-182).

[10] "Use of online services that facilitate public's interaction with government" (IMD 2021, p. 182).

[11] "Provision of online government services to promote access and inclusion of citizens" (IMD 2021, p. 183).

[12] Wawra (2022, IV. 2.).

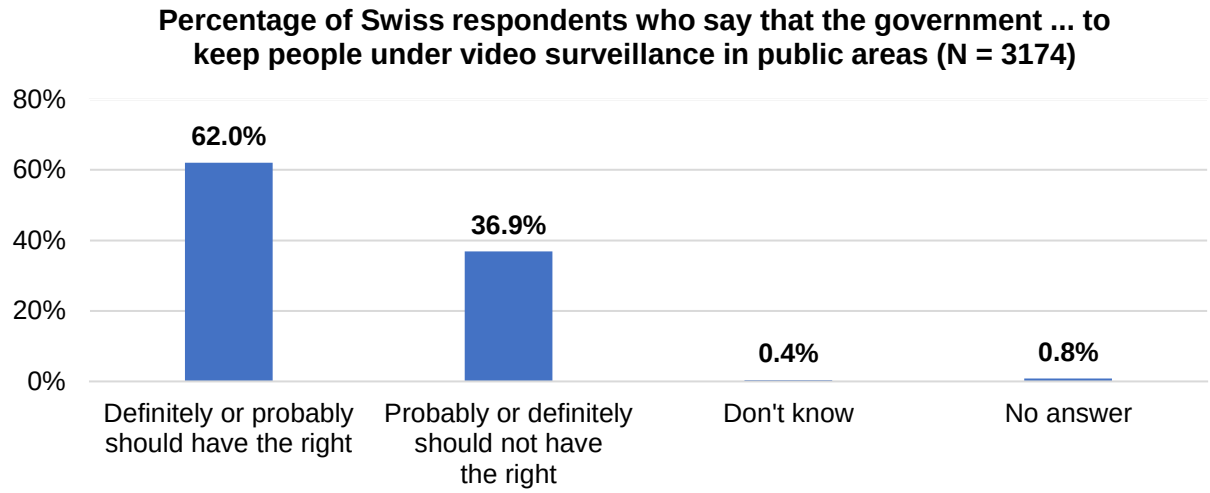

Fig. 2. Swiss respondents' attitudes towards video surveillance by their government (cf. EVS/WVS 2021c, p. 428).

By contrast, Swiss respondents (81%) are opposed to the idea that their government should have the right to collect data on anyone living in Switzerland without their knowledge (cf. EVS/WVS 2021c, p. 432) (Fig. 3).

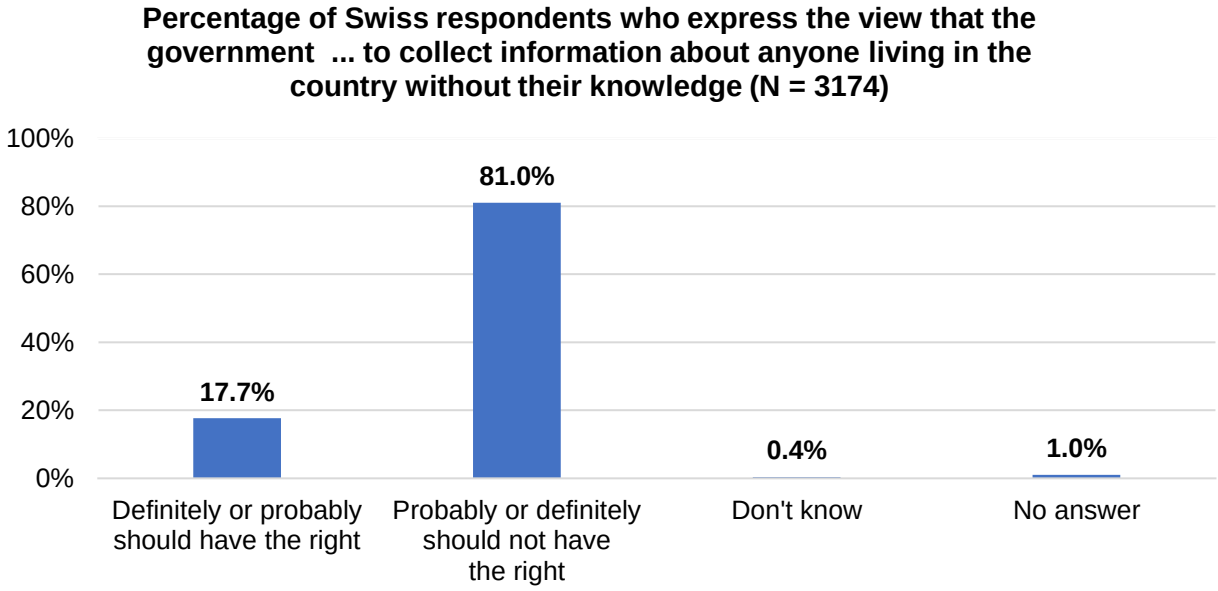

Fig. 3. Swiss respondents' attitudes towards data collection by the government without consent (cf. EVS/WVS 2021c, p. 432).

With regard to online surveillance, a minority (44%) of Swiss respondents express a critical attitude according to a survey by Latzer et al. (2019), in that they believe that it is harmful to society (Fig. 4). However, according to a recent survey (Latzer et al. 2021b), a large majority of Swiss Internet users (74%) clearly value their informational privacy online, in that they are vigilant regarding the protection of their privacy on the Internet (Fig. 5).

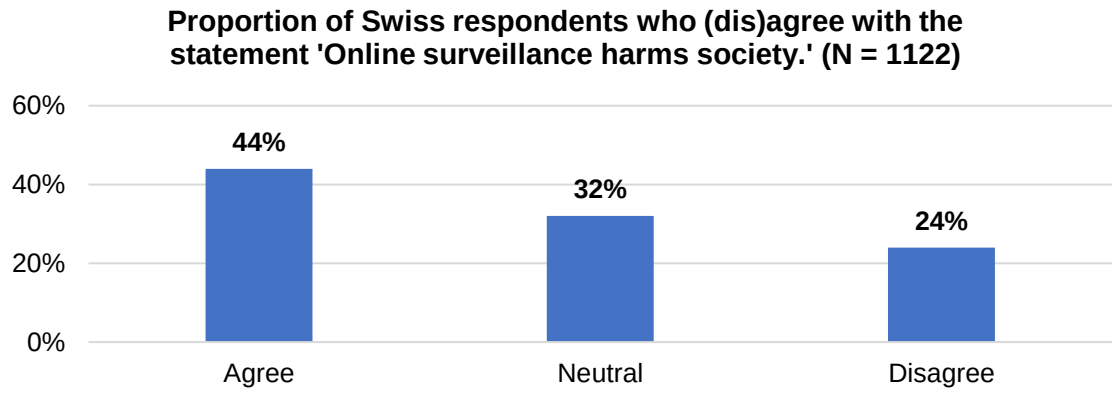

Fig. 4. Swiss respondents' attitudes regarding the societal risks of online surveillance (cf. Latzer et al. 2019).[13]

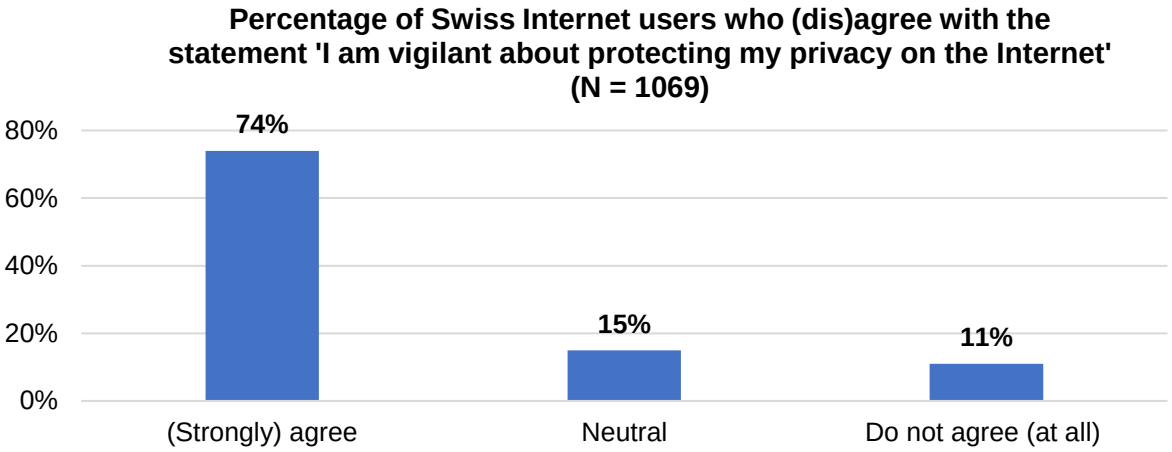

Fig. 5. Swiss Internet users' views on protecting their online privacy (cf. Latzer et al. 2021b, p. 22).[14]

Moreover, a large majority (73.2%) of Swiss respondents agree that their government should not be allowed to monitor emails and other information exchanged online (EVS/WVS 2021c, p. 430) (Fig. 6).

[13] Translation according to Latzer et al. (2020, p. 27); own calculation for the entire sample, based on the percentages for the subsamples of Internet users (N = 1035) and non-users (N = 85) in Latzer et al. (2019, p. 15-16).

[14] Translation according to Latzer et al. (2020, p. 28).

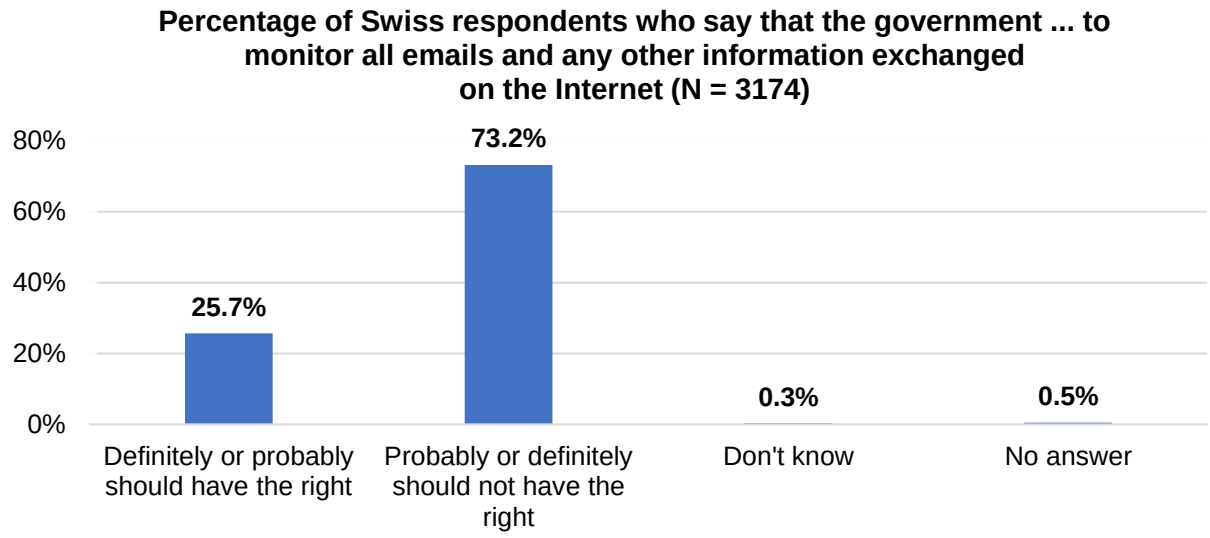

Fig. 6. Swiss respondents' attitudes towards email and Internet monitoring by their government (cf. EVS/WVS 2021c, p. 430).

No recent large-scale survey on the attitude of the Swiss population towards surveillance in the workplace could be found. Switzerland is not included in PwC (2021a, b) and Unisys (2021), which contain relevant data on this topic for other countries. Thus, there are no data available for Switzerland, for example, on whether people mind their employer using technology, such as sensors and wearable devices, to monitor their performance or whether they object to their employer having access to their personal data such as their social media profile.

Moreover, Ipsos (2019) does not provide any data for Switzerland regarding the questions of whether consumers should be able to refuse the use of collected data by companies or whether they should be paid or rewarded for allowing it. However, another study has shown that only 9% of expert respondents from Switzerland (i.e. respondents who deal with 'big data' in some way) believe that people receive fair compensation for disclosing their data on the Internet (cf. Jarchow and Estermann 2015, p. 50).

V. Degree of Privacy of Data

[This] parameter […] surveys how private or sensitive […] certain kinds of personal data [are for Swiss respondents].[15]

In order to get an indication of what types of personal data are considered particularly private in Switzerland, let us take a look at their legal definition: According to the Federal Act on Data Protection (FADP)[16], personal data comprise "all information relating to an identified or identifiable natural or legal person", and are categorized as sensitive when they reveal "[r]eligious, ideological, political or trade union […] views or activities", or are related to "[h]ealth, the intimate sphere or racial or ethnic origin", "[s]ocial security measures", or "[a]dministrative or criminal proceedings and sanctions". Furthermore, the revised DPA defines "genetic […] and biometric data which unequivocally identifies a natural person" (DLA Piper 2021) as sensitive.

[15] Wawra (2022, IV. 2.).

[16] FADP (Federal Act on Data Protection) of 19 June 1992 (Status as of 1 March 2019), https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/en (last access: 02/28/2022).

No recent large-scale survey on Swiss people's opinions on what constitutes sensitive data could be found. Neither Trepte and Masur (2016), Fukuta et al. (2017), nor Markos, Milne, and Peltier (2017), which contain relevant data for other countries, provide data on this topic for Switzerland. In general, research on Swiss people's perceptions of sensitivity regarding different data types is scarce. Some tentative evidence in this respect may be deduced from the results presented in Fig. 7. The graph lists different types of personal data shared by Swiss respondents on the Internet in 2021 in descending order (Bundesamt für Statistik 2021a, b). More than two-thirds of respondents shared contact information (72%) or payment information online (68%). Fewer respondents, just over half (56%), provided personal details such as their name or their date of birth, and half of respondents shared their current location. In contrast, only one in five respondents shared data such as photos or information about their health or employment status. These results may to some extent reflect Swiss perceptions of the sensitivity of these types of data, although it should be noted that they are certainly also strongly influenced by practical constraints. For example, providing contact information and/or payment information is a necessary step when using many online services, notably e-commerce, and thus much more widespread among the Swiss than sharing photos or health or employment status information online, for which external pressures are usually much lower on a practical level.

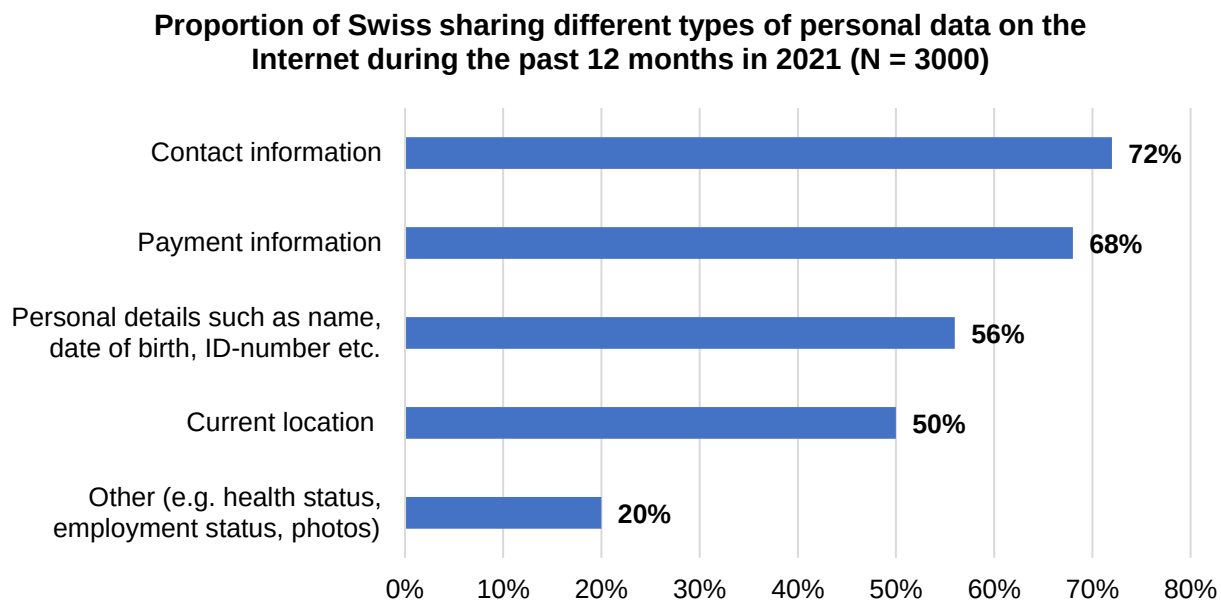

Fig. 7. Proportion of Swiss people sharing different types of personal data on the Internet during the past 12 months in 2021 (cf. Bundesamt für Statistik 2021a, b).[17]

Some further insights regarding the perceived sensitivity of certain types of online data in Switzerland can be gained from a survey by Latzer et al. (2015). They asked respondents how important it is to them that only they or people they authorize know certain types of personal online data (Fig. 8). For all five data types examined, a majority of Swiss Internet users believed that it was either important or very important that they remain confidential, i.e. that they are known only to them and authorized people. However, the size of this majority varied between the five data categories, suggesting differences in perceived sensitivity. The largest majority was found for the category 'content of e-mails and other correspondence', the confidentiality of which three-quarters (76%) of respondents considered important or very important. This was followed by the

[17] Own translation.

confidentiality of online contacts (i.e. with whom one communicates over the Internet), to which two-thirds (67%) attributed (great) importance. Slightly more than 60%, believed it was (very) important that the websites they visit or their location remain known only to them or authorized people. The smallest majority was found for the category 'performed search queries', the confidentiality of which more than half (56%) of the respondents considered (very) important.

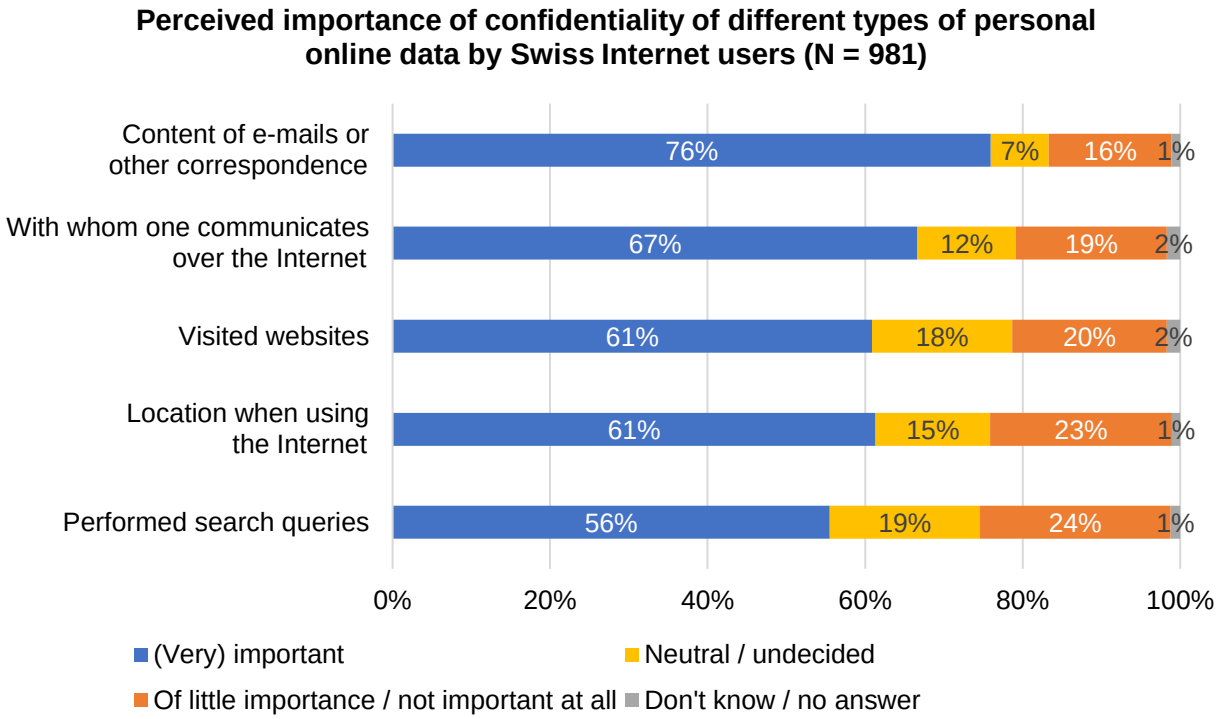

Fig. 8. Perceived importance of confidentiality of different types of personal online data by Swiss Internet users (cf. Latzer et al. 2015, p. 17).[18]

A survey by Brall et al. (2021) shows the influence that context, purpose, and type of data collection can have on the willingness to share personal data. Thus, health data are often considered to be rather sensitive (cf. Howe 2022, p. 7; Thir and Wawra 2023, Wawra et al. 2022). This is also reflected in the fact that this data category is part of all sensitive data definitions of the most important data protection laws of our countries of investigation (cf. Wawra 2022, Wawra 2023). Brall et al. (2021) asked Swiss residents whether they would hypothetically provide certain health-related data and biological samples for a research project (Fig. 9). While a slight majority of respondents (53.6 %) stated that they would to be willing to provide such data, slightly less than half (45.6%) would not want to disclose their health-related data and biological samples in this context.

[18] We contacted the authors after noticing an inconsistency in their presentation of the data at this point in their report. We are grateful to them and their research assistant, Kiran Kappeler, for clarifying our enquiry and for providing us with a more detailed breakdown of the results by email.

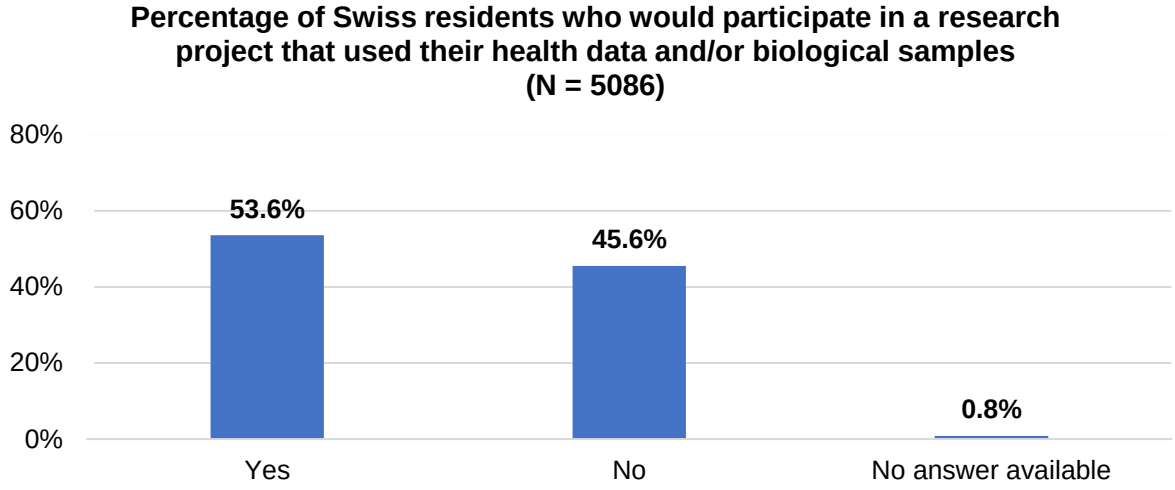

Fig. 9. Swiss residents' willingness to participate in a research project that uses their health data and/or biological samples.[19]

Those respondents who said they were willing to participate in the research using their health data and/or biological samples were then asked to indicate what types of data or samples they would be willing to provide (Fig. 10). A majority of over 80% indicated that they would provide information about their health status via questionnaires, as well as blood samples or biological samples that they could collect themselves (e.g. saliva or hair). Considerably fewer respondents, though still a majority of about 60%, indicated a hypothetical willingness to provide biological samples taken by medical staff or medical records about themselves. Half of the respondents were hypothetically willing to share their family's medical history. The reason for these high levels of willingness to disclose health-related data is likely to be the research context, and here the possibility of contributing to the improvement of treatments in the future. However, only just over one-third (36.2%) were theoretically willing to provide data via health and lifestyle apps and less than 15% were theoretically willing to share social media data. One possible factor influencing respondents' willingness to share data in this regard could be the time and effort involved in disclosing data: Using a health or lifestyle app, for example, seems to be a much greater and longer commitment than filling out a questionnaire about one's health status. In addition, these types of data collection might be considered less trustworthy as they are deemed more vulnerable to data breaches.

[19] Own analysis based on the dataset included in the supplementary material of Brall et al. (2021).

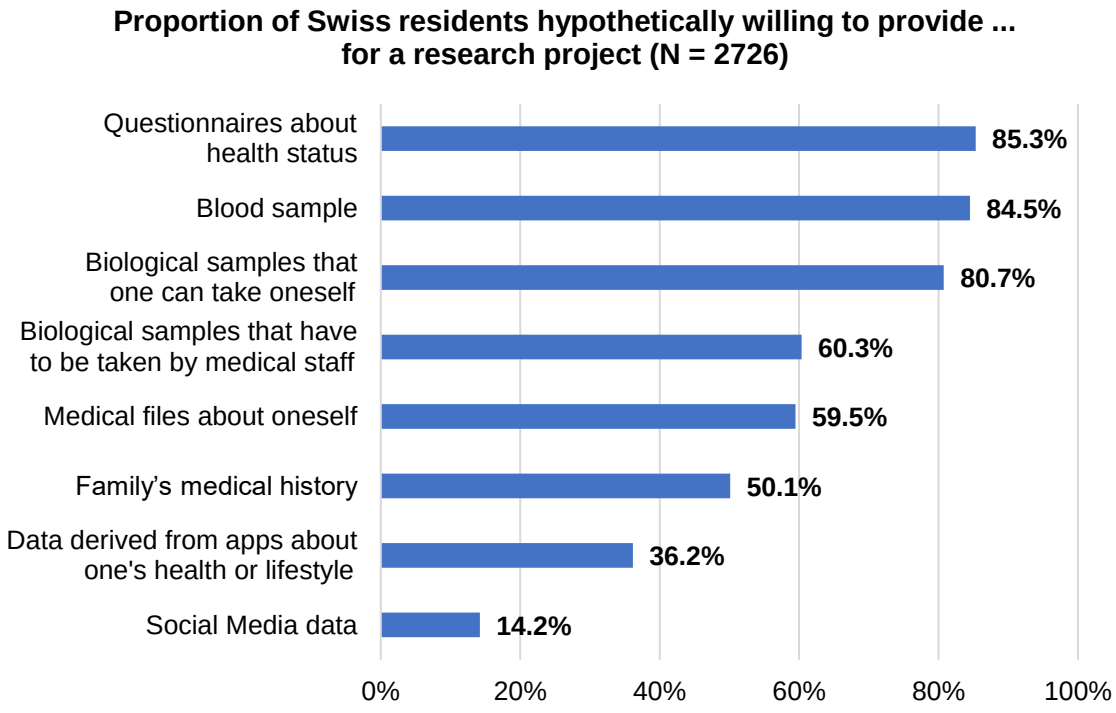

Fig. 10. Proportion of Swiss residents hypothetically willing to provide different types of data for a research project (cf. Brall et al. 2021).[20]

VI. Benefits Associated with Data Disclosure

[This] parameter […] renders the positive effects [Swiss respondents] expect from the disclosure of their personal data.[21]

No recent large-scale survey could be found on Swiss people's assessment of potential benefits of data disclosure (e.g. better information, products and services for individual customer needs, easier access to relevant information, saving time and money). Ipsos (2019), which provides such data for other countries, did not survey the Swiss population. Nor could a representative survey be found that investigates the willingness to share personal data in exchange for benefits in Switzerland. The survey by GfK (2017), for example, does not include Switzerland.

A survey by Deloitte (2022) offers insight into the perceived benefits of using e-government services, i.e. disclosing personal data to the government via the Internet rather than in person. In the survey, Swiss respondents were asked which (beneficial) aspects of e-government services have priority for them (see Fig. 11). For three out of four respondents, the aspect of temporal flexibility, i.e. the ability to access the services at any time, stands out in particular. More than 70% value the aspect of spatial flexibility (i.e. being able to access the services from anywhere) and of saving time when using e-government services. More than two-thirds (68%) consider the simplicity and convenience of using such services, as well as the autonomy it offers, to be particularly important. Almost two-thirds (64%) prioritize the lower costs of using e-government services (i.e. saving

[20] Own analysis based on the dataset included in the supplementary material of Brall et al. (2021), using the subsample of participants hypothetically willing to participate in a research project using their health data and/or biological samples.

[21] Wawra (2022, IV. 2.).

money), and 60% consider the aspect of having freedom of choice in relation to such services to be a priority.

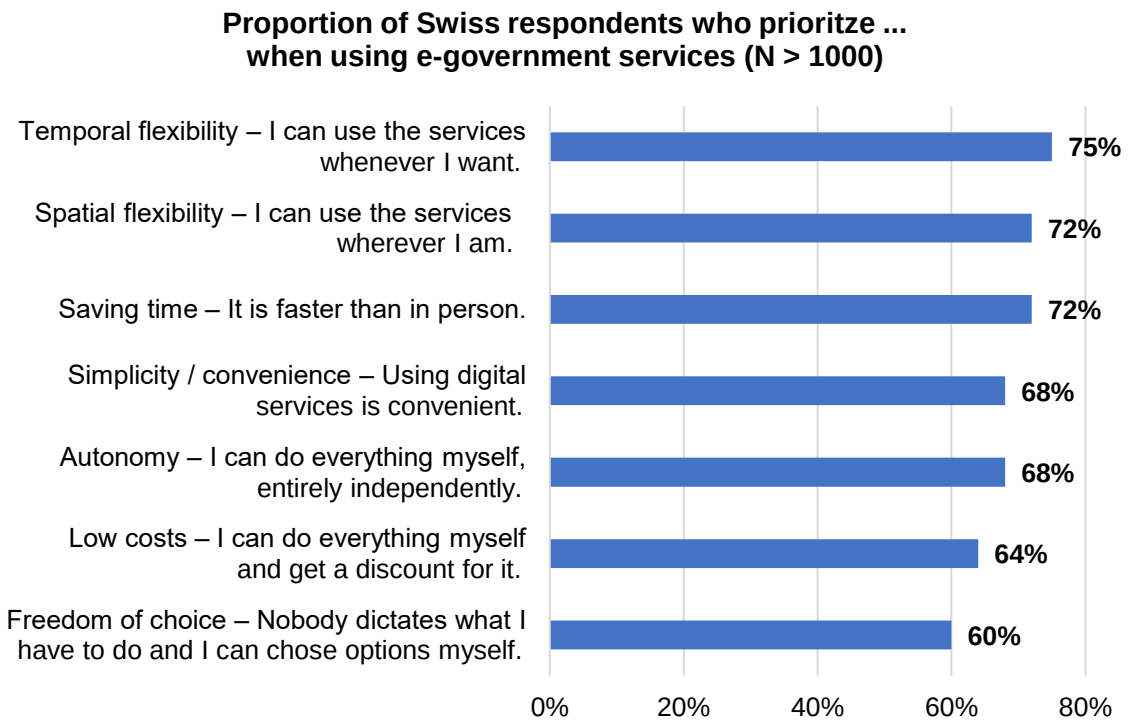

Fig. 11. Swiss respondents' priorities when using e-government services (cf. Deloitte 2022, p. 7).[22]

With regard to health-related data collected for research purposes, financial or material compensation seems to play a minor role for most Swiss people. In a recent survey among Swiss residents (Brall et al. 2022), most respondents (56.9%) stated that money or other material compensation would not or rather not be important to them if they disclosed data and provided samples to a Swiss publicly funded biobank (Fig. 12). A quarter (24.9%) consider this type of compensation moderately important, and less than 20% consider it rather or very important. Similarly, Pletscher et al. (2022, p. 6) found that more than three-quarters of Swiss people (78%) do not believe they would be more likely to share anonymized health data if they received money for it (see Fig. 13). Far more important in this context are altruistic motives, i.e. the perceived benefits for others: more than eight in ten respondents (86%) state that they would be more likely to share such data if it meant that other people received better treatment as a result, and just over two-thirds (67%) think that they would be more likely to do so if it benefited the healthcare system and lowered insurance premiums in the long-term (although this could ultimately also be to their own benefit).

[22] Own translation.

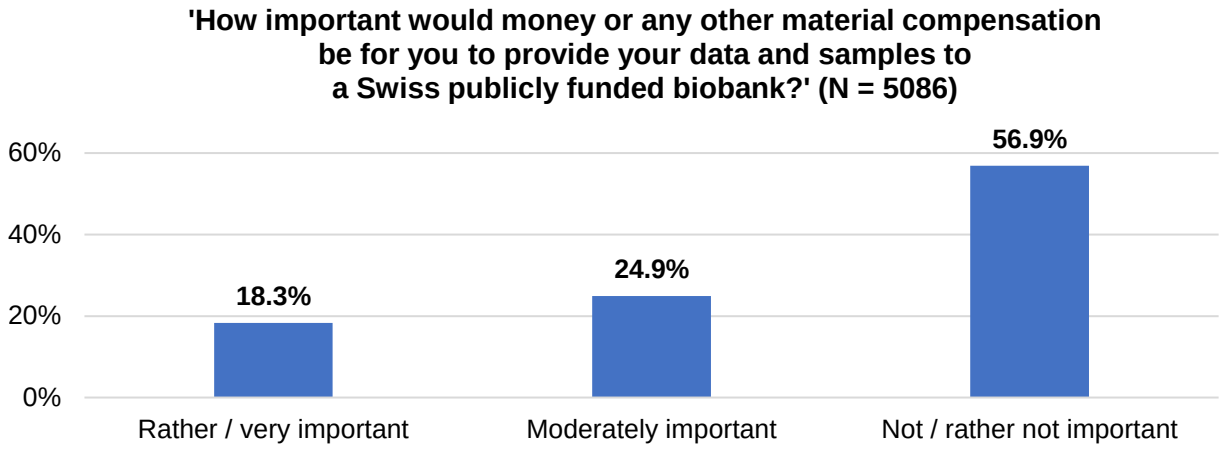

Fig. 12. Perceived importance of money or other material compensation for disclosure of health-related data and samples to a Swiss biobank by Swiss residents (cf. Brall et al. 2022, p. 3).

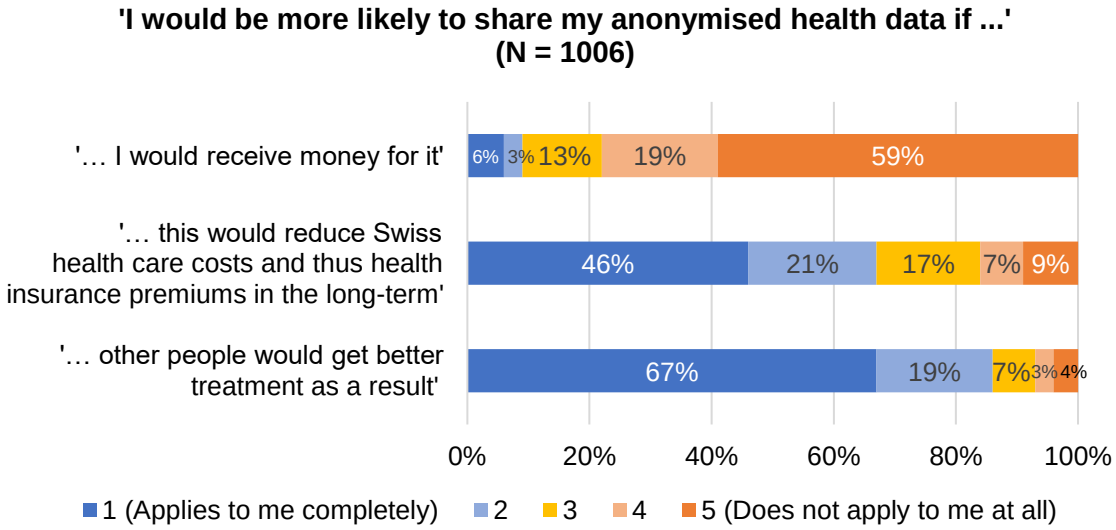

Fig. 13. Relevance of different benefits concerning the disclosure of anonymized health data for Swiss respondents (cf. Pletscher et al. 2022, p. 6).

A study by Brüesch et al. (2020) shows that such perceived benefits for society as a whole may indeed influence Swiss people's data disclosure behavior, in the form of their willingness to install a COVID-19 contact tracing app. On average, users of the app rated its societal benefit significantly higher than non-users of the app ($p < 0.001$; Brüesch et al. 2020, p. 25-26). However, the personal benefit perceived by the Swiss respondents, which here obviously does not relate to monetary or other compensation or better access to products and services, but to the protection of one's own health, may have been another important factor in their decision to (not) install the app: the average app user rated their personal benefit significantly higher than the non-users ($p < 0.001$; Brüesch et al. 2020, p. 25-26). A personal health benefit was also found to be a relevant factor for the Swiss by Pletscher et al. (2022): a majority of 60% of Swiss respondents stated that they would rather not share their anonymized health data if they personally had no direct health benefit from it (Fig. 14).

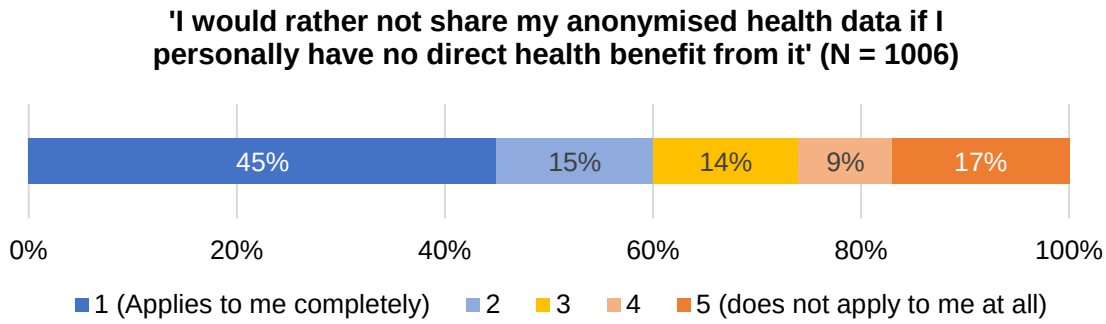

Fig. 14. Relevance of direct personal health benefit concerning the disclosure of anonymized health data for Swiss respondents (cf. Pletscher et al. 2022, p. 6).

VII. Privacy Concerns and Risks

[This] parameter […] comprises the negative effects [Swiss respondents] associate with data disclosure. These include their general concerns about the security of their personal data, and their control over them.[23]

1. Concerns and Risks related to Data Security

Ipsos (2019) does not provide data for Switzerland with regard to the question of whether people feel more comfortable with sharing their data with companies that have "never been subject to any breach, leak, or fraudulent usage of data" (Ipsos 2019, p. 14). Nor was the question asked in Switzerland whether people want their "online data & personal information" to be "stored on a secure server", preferably "in their own economy" (CIGI-Ipsos 2019b, pp. 13, 15) or abroad, and whether they care if their data left Switzerland (CIGI-Ipsos 2019b, pp. 17, 19).

However, the findings of several national surveys provide insights into Swiss people's concerns in relation to data security. Regarding online data specifically, a survey by Latzer et al. (2019) shows that around two out of three Swiss people (65%) believe that the secure handling of online data poses a challenge for society (Fig. 15). Furthermore, in a survey by Guirguis et al. (2021), 83% of the Swiss respondents indicated that they have great to very great concerns regarding data theft and 63% have such concerns regarding identity theft (Fig. 16). However, a study by Brall et al. (2021) shows that concerns about data theft by the Swiss may be less pronounced in certain contexts of data disclosure. Swiss residents were asked to select up to three concerns they would have when hypothetically providing their health data and/or biological samples for a research project. The fourth most frequent concern, selected by almost a third of respondents (31.9%), was that their data could be hacked and stolen (cf. Brall et al. 2021, p. 9).

[23] Wawra (2022, IV. 2.).

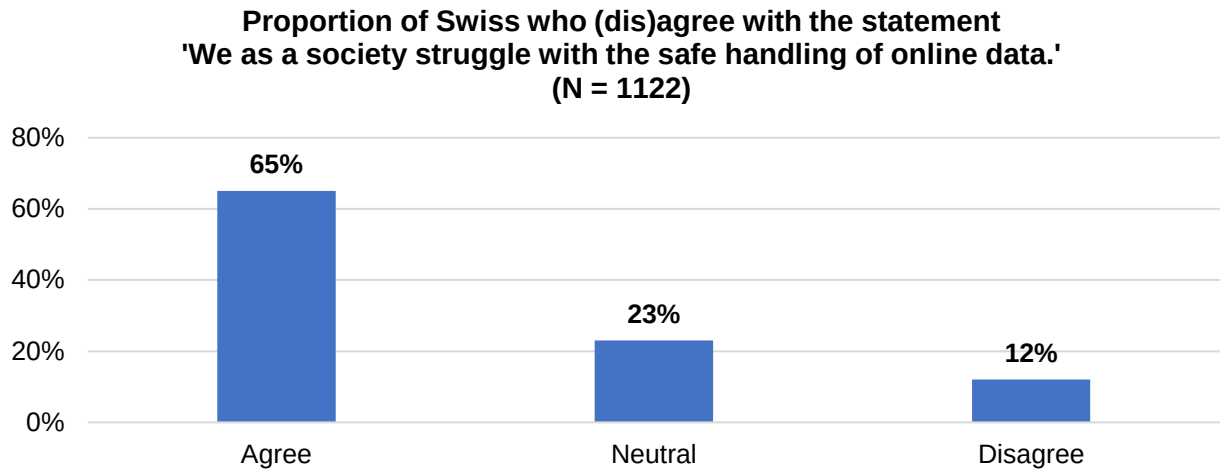

Fig. 15. Swiss respondents' views regarding the safe handling of online data (cf. Latzer et al. 2019).[24]

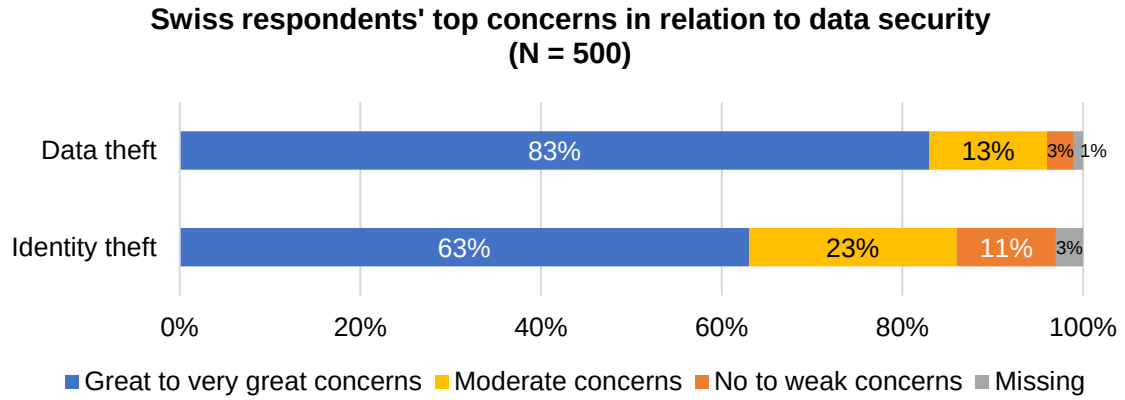

Fig. 16. Swiss respondents' top concerns in relation to data security (cf. Guirguis et al. 2021, p. 24).[25]

Such security-related concerns may be due to previous negative experiences among the Swiss. More than half of Swiss Internet users (56%) experienced one of the security-related incidents listed in Fig. 17 in 2019, which is considerably higher than the EU-27 average (37%; cf. Eurostat 2022). Almost half of respondents (47%) received 'phishing' messages, and around one in five were targeted by 'pharming', i.e., redirected to a fake website where they were asked to provide personal information. Fortunately, more serious incidents such as the hacking of one's social media or e-mail account, credit or debit card fraud, data loss due to a computer infection, misuse of online personal information resulting in some form of discrimination, harassment or bullying and online identity theft, were only experienced by a small minority of Swiss Internet users (3-6%). Notably, for all these incidents, with the exception of data loss due to computer infection, the EU-27 average was surpassed, and considerably so for phishing (47% vs. 28%).

[24] Translation according to Latzer et al. (2020, p. 27); own calculation for the entire sample, based on the percentages provided for the subsamples of Internet users (N = 1035) and non-users (N = 85) in Latzer et al. (2019, p. 15-16).

[25] Own translation. Respondents rated their concerns on a scale form 1 ('no concerns') to 5 ('very great concerns'). The original source summarized the results for values 1 and 2 and values 4 and 5 into a single category, respectively.

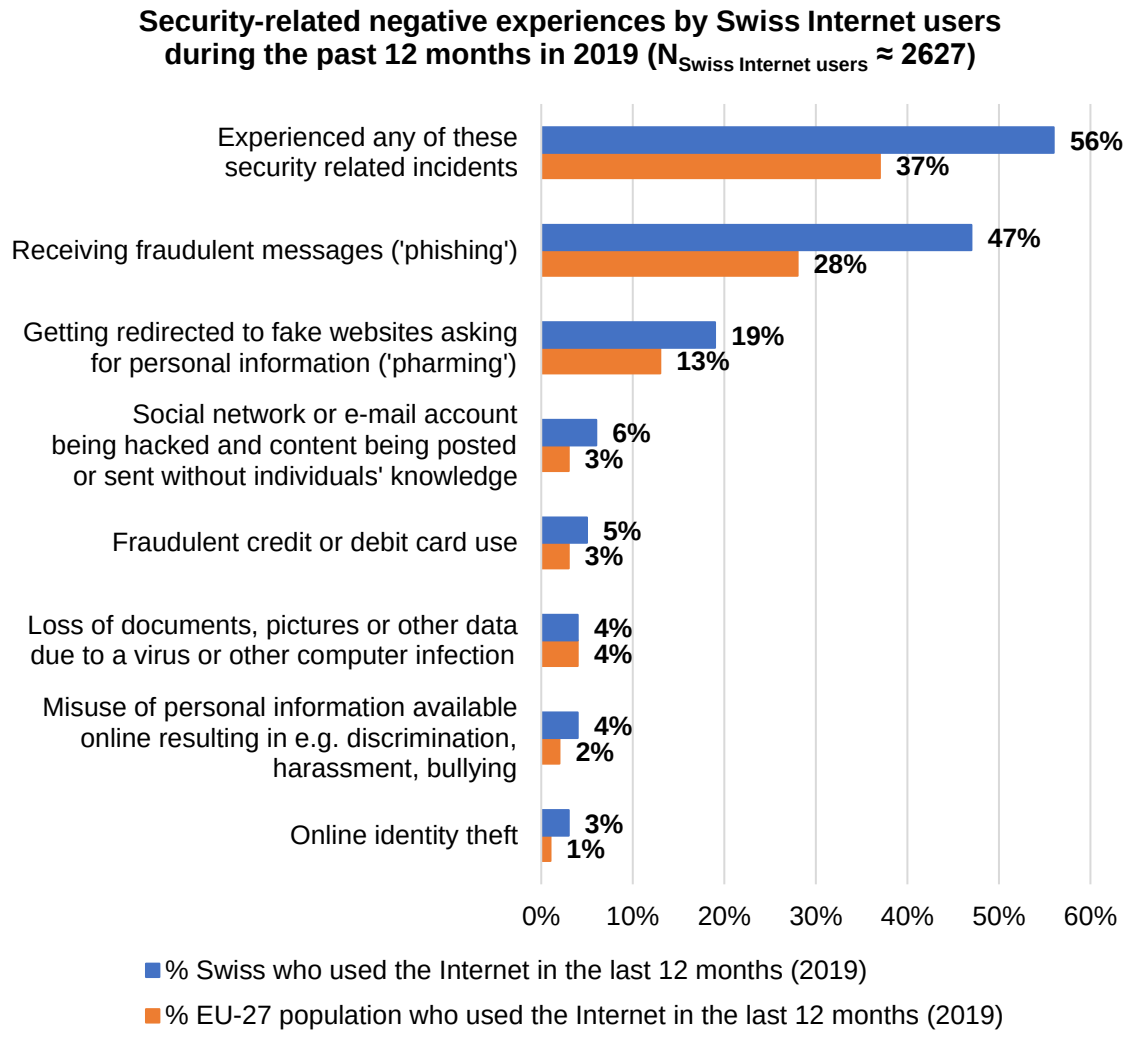

Fig. 17. Security-related negative experiences by Swiss Internet users during the past 12 months in 2019 (cf. Eurostat 2022).

Concerns about data security and data protection are an important reason why a considerable number of Swiss people would avoid using certain new e-government services. In a survey by Deloitte (2022), Swiss respondents were asked whether they would always, sometimes or never want to use certain e-government services that are not yet available. Those respondents that selected 'sometimes' or 'never' were then asked about their reasons for not (always) wanting to use a particular service, such as concerns about data protection or cyber/data security. As Fig. 18 shows, for around a third (30-34%) of respondents concerns about cyber/data security or data protection are such that they would not (always) want to use these services when using a legally binding digital signature, for the electronic exchange of all data and information with government agencies and public administration, and for the automatic collection of tax-relevant data by the state. Almost a quarter each (24%) are concerned about data security regarding e-voting and ordering a pass-port and identity card online, while about a fifth (19-20%) have concerns about data protection regarding these services. About a fifth of respondents (20-23%) stated that they are not (always) willing to file a police report online or register as unemployed online due to concerns about cyber/data security or data protection. Such concerns were the least frequent for traffic-related services, i.e. contactless payment of parking fines and digital purchase of the motorway toll sticker, which concerned 14-18% of respondents.

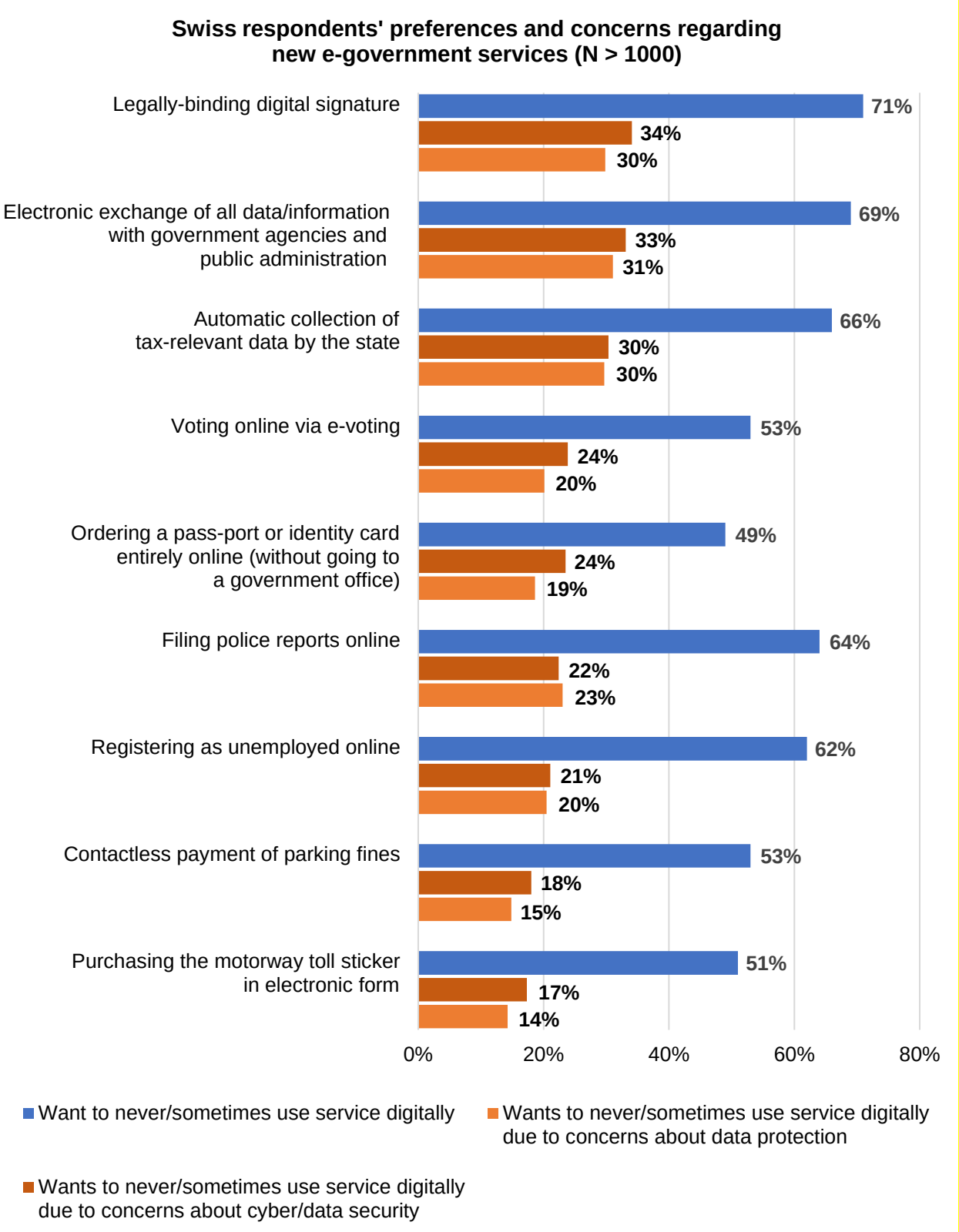

Fig. 18. Preferences and concerns of Swiss respondents regarding new e-government services (cf. Deloitte 2022, p. 8 & 12).[26]

[26] Own translation. The percentages for the orange bars were calculated based on the information and percentages provided in Deloitte (2022, p. 8 & 12).

However, the pandemic may have prompted some Swiss to put such concerns aside and use e-government services after all. As Fig. 19 shows, the proportion of Swiss people who submitted completed forms to public authorities via the Internet has increased substantially from a minority of 45% in 2019 to over two-thirds (71%) in 2021 (Eurostat 2022). This increase of 26 percentage points is considerably greater than the average of the 27 EU member states (8 percentage points), where the proportion of people submitting completed forms to public authorities via the Internet in 2021 is also considerably smaller at 44%. However, such differences may also be due to differences in the availability of e-government services and in the proportion of people who had to submit official forms at all during the surveyed period. Notably, in 2021, more people in the EU-27 countries (28%) than in Switzerland (19%) did not have to submit completed forms to public authorities (Eurostat 2022). Still, the proportion of Swiss who opted not to submit official forms online, despite being required to do so, is smaller (8%) than the EU-27 average (17%; Eurostat 2022). Of these 8%, a quarter have refrained from doing so out of concern for the protection and security of their personal data, which amounts to only 2% of the total Swiss population (Eurostat 2022).

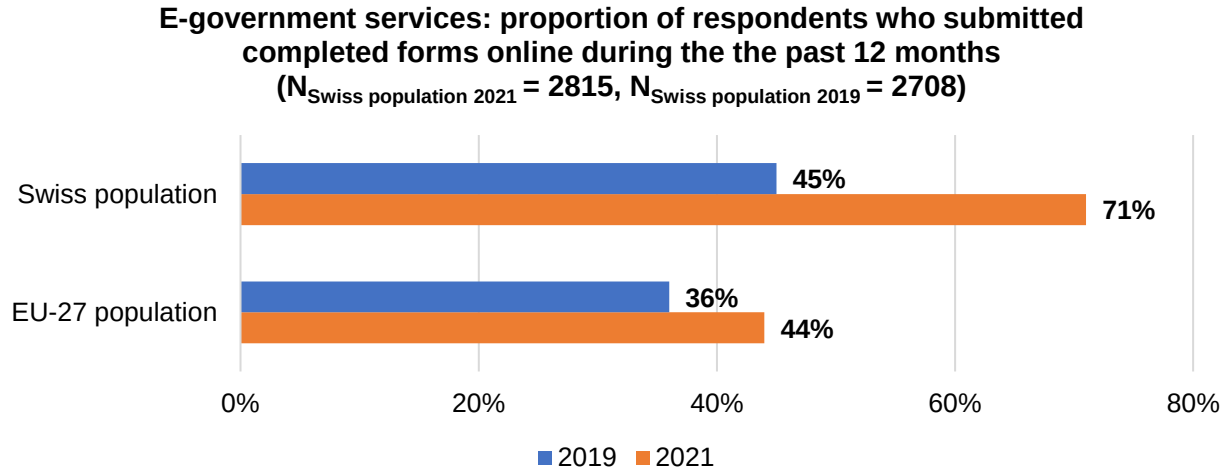

Fig. 19. E-government services: proportion of Swiss who submitted completed forms online during the past 12 months, compared to the EU-27 population (cf. Eurostat 2022).

2. Concerns and Risks related to Data Control

According to a recent survey (Guirguis et al. 2021), the majority of Swiss respondents have great to very great concerns related to various aspects of data control (Fig. 20). 87% of Swiss respondents indicated such concerns about misuse of data, 84% about the sale of personal data to third parties, 70% are very concerned about companies profiting from their data and 57% about disproportionate data collection.

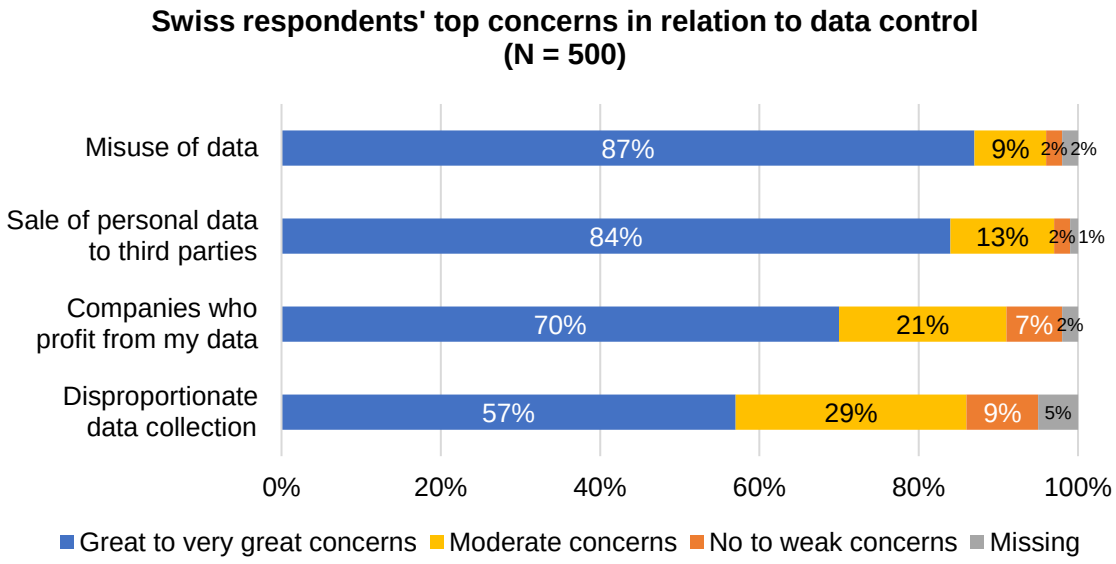

Fig. 20. Swiss respondents' top concerns in relation to data control (cf. Guirguis et al. 2021, p. 24).[27]

Furthermore, the level of concern about online data disclosure appears to be moderate to high in Switzerland. In the same survey (Guirguis et al. 2021), participants were asked to rate their concerns about disclosing personal information online on a scale of 1 to 10 (1 = no concerns at all, 10 = very strong concerns). Responses tended towards the upper half of the scale (mean = 7.05, SD = 2.11), meaning that on average participants' concerns tended to be medium-high. Notably, these concerns were found to vary according to the respondents' level of trust in government institutions regarding the right use of the personal data collected (see section IX. 1., Fig. 34), and according to their level of satisfaction with current data protection legislation (section VIII., Fig. 26). Respondents with greater trust in government institutions regarding the handling of collected personal data showed significantly lower concerns than those with lower trust ($p = 0.035$, cf. Guirguis et al. 2021, p. 24). Similarly, respondents who considered current legislation and organizational practices regarding privacy protection to be sufficient also showed significantly lower concerns about disclosing personal information online ($p = 0.001$, cf. Guirguis et al. 2021, p. 25).

CIGI-Ipsos (2019c, p. 24) does not provide any data for Switzerland regarding the question of whether people use the Internet differently because they distrust it. However, a recent survey by Latzer et al. (2021a) shows how concerns about online surveillance lead the Swiss to adapt their behavior on the Internet. They observed different types of 'chilling effects' (Fig. 21), that is, when users avoid or limit themselves in certain activities due to a fear of being monitored online. Only a small minority of 12% of Swiss respondents always or often limit themselves in their information search on sensitive topics for this reason; almost half of the respondents (49%) do so sometimes or rarely. More than twice as many – 25% – always or often limit themselves in their self-expression online, that is, when expressing opinions, interests or feelings on the Internet, out of concern about online surveillance; a third (33%) does so sometimes or rarely.

[27] Own translation. Respondents rated their concerns on a scale form 1 ('no concerns') to 5 ('very great concerns'). In the original source, the results for values 1 and 2 and values 4 and 5 were summarized into a single category, respectively.

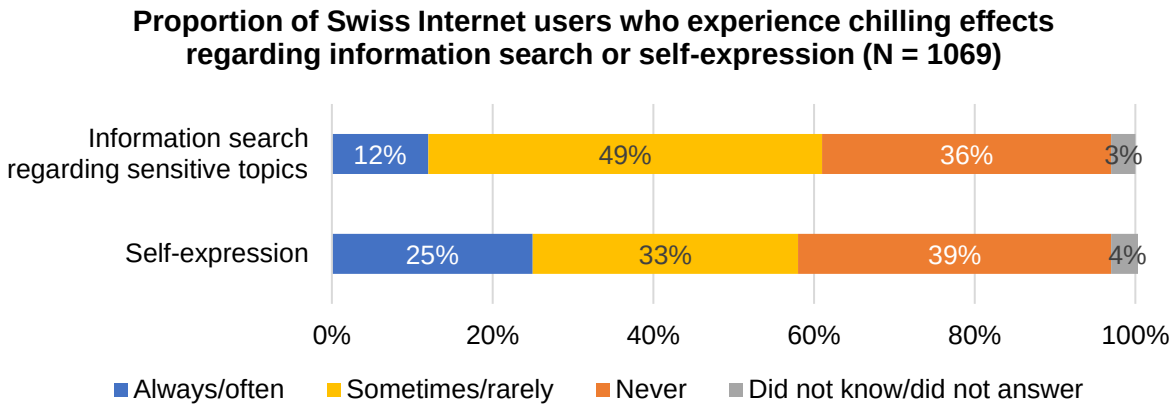

Fig. 21. Frequency of chilling effects among Swiss Internet users due to fear of online surveillance (cf. Latzer et al. 2021a, p. 17-18).[28]

Compared to the percentage of Swiss respondents who regularly limit their self-expression online, considerably fewer respondents regularly limit their online shopping behavior because of privacy concerns. In 2021, only 13% of Swiss people stated that they never or rarely shop online because they are concerned about payment security or data protection (cf. Eurostat 2022).[29]

Overall, however, Latzer et al. (2021b) found that 43% of Swiss Internet users believe concerns about online privacy are not exaggerated (Fig. 22), compared to about a quarter who do (27%) and around a quarter who take a neutral stance in this regard (28%). It is noteworthy that only a minority of about 40% believe they are able to control their online privacy (Latzer et al. 2021b, p. 22; Fig. 23). This tendency could be at least partly due to previous negative experiences among the Swiss: in 2019, over a third (37%) of Swiss Internet users had the impression that their personal data had been passed on or misused in the past year (Latzer et al. 2019, p. 27).

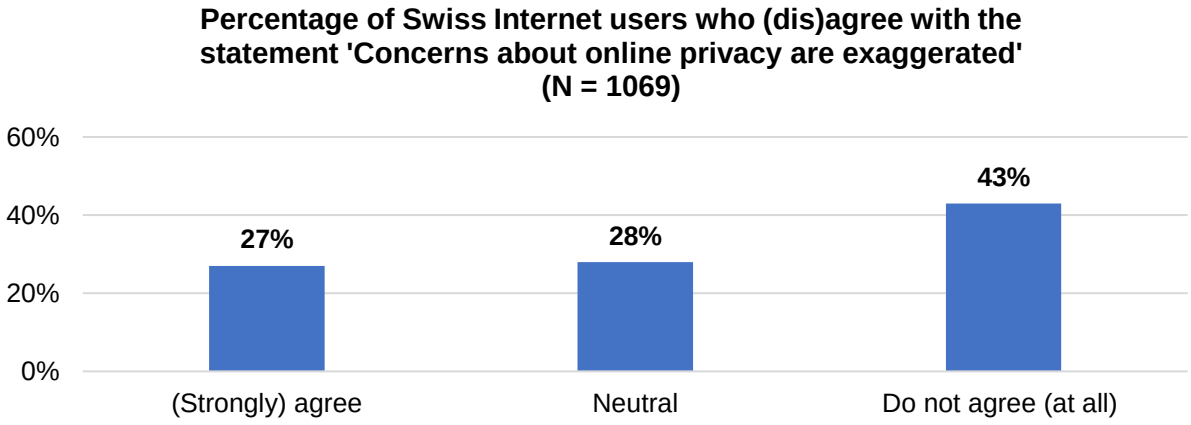

Fig. 22. Swiss Internet users' views on concerns about online privacy (cf. Latzer et al. 2021b, p. 22).[30]

[28] Translation according to Latzer et al. (2020, p. 25-26).

[29] Own translation of item in Bundesamt für Statistik (2021a, p. 20).

[30] Translation according to Latzer et al. (2020, p. 28).

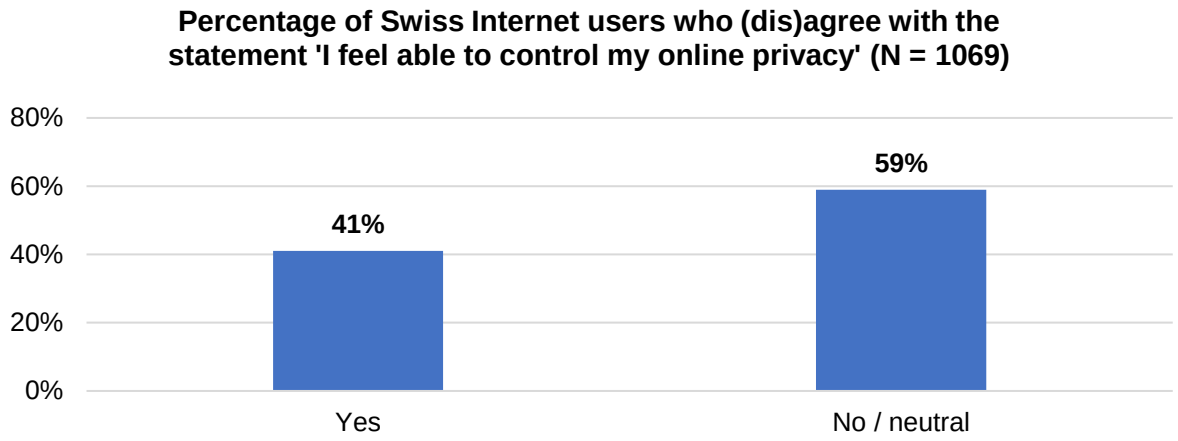

Fig. 23. Swiss Internet users' sense of control regarding their online privacy (cf. Latzer et al. 2021b, p. 22).[31]

For the special case of health-related data, it is noteworthy that four of the top five concerns of the Swiss residents regarding the hypothetical provision of their health data and/or biological samples for a research project relate to data control (Fig. 24; cf. Brall et al. 2021, p. 9). The top concern was that someone may misuse one's data to discriminate against oneself or one's family, which almost half of the respondents (46.8%) worried about. The second most common concern, selected by almost half of the respondents (46.3%), was that data may not be kept confidential. Notably, the difference in frequency to the top concern is only marginal at 0.5%. Almost half of the respondents (45.5%) worried that their data may be misused for commercial or marketing purposes. Slightly less than a third (31.2%) stated that they do not want other parties (such as private companies or researchers) to benefit financially from their data.

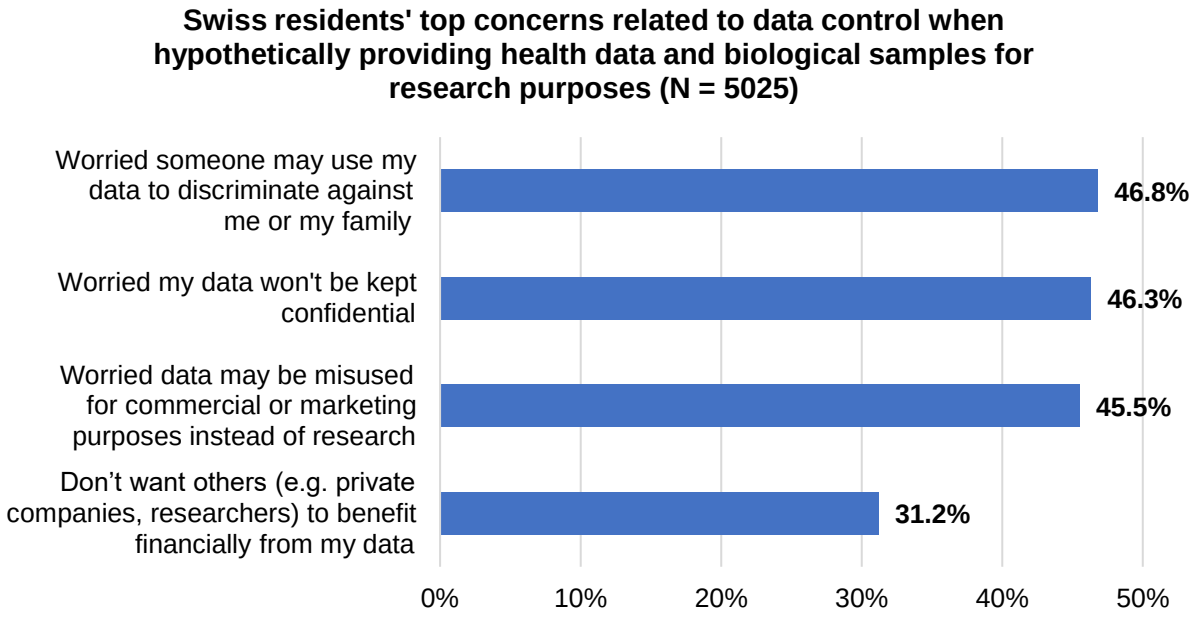

Fig. 24. Swiss residents' top concerns related to data control when hypothetically providing health data and biological samples for research purposes (cf. Brall et al. 2021, p. 9).

[31] Translation according to Latzer et al. (2020, p. 28). Since no exact percentages were provided in the original source for the options 'neutral' and 'no', these are summarized into a single category.

VIII. Data Protection Literacy

[Data Protection Literacy] captures [Swiss people's] awareness and knowledge of data protection, privacy rules and policies as well as the skills they report to have, and the measures they take to protect their personal data.[32]

As regards Swiss people's knowledge of data protection and privacy regulations, less than a third (28%) of Swiss respondents state that they are very or rather familiar with the EU General Data Protection Regulation (GDPR; Fig. 25).[33] 27% indicate they are somewhat familiar with it and 40% say they are not at all or rather not familiar with it (cf. Guirguis et al. 2021, p. 23).

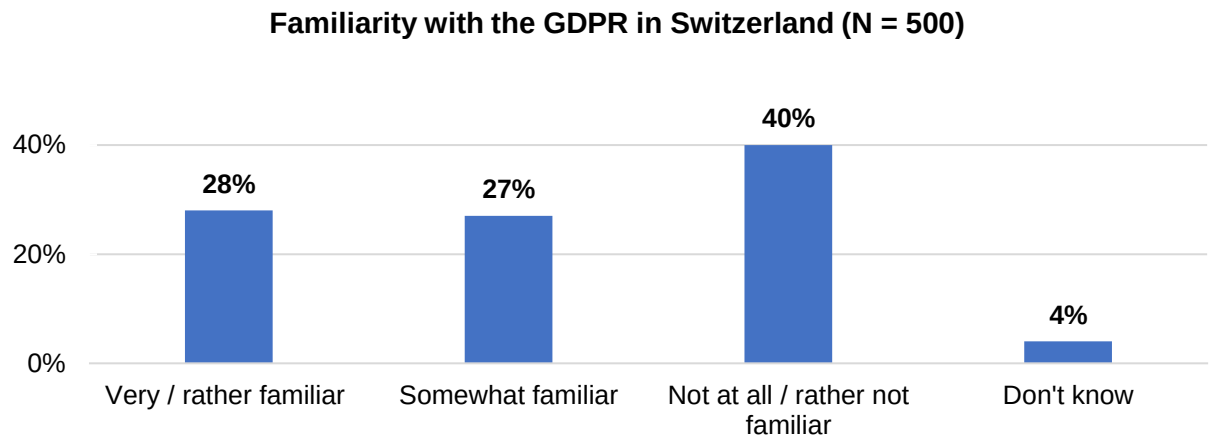

Fig. 25. Familiarity with the GDPR in Switzerland (cf. Guirguis et al. 2021, p. 23).[34]

With regard to the Swiss people's satisfaction with existing data protection laws and practices, one survey found that around half of the respondents (47%) agreed (strongly or somewhat) that "existing laws and organizational practices offer sufficient protection of people's privacy" (cf. Guirguis et al. 2021, p. 24).[35] However, the remaining, slightly larger half (52%) disagreed at least somewhat (cf. Guirguis et al. 2021, p. 24; see Fig. 26). In contrast, a recent survey found that a majority of 63.7% of Swiss people consider data protection regulation in Switzerland to be 'rather good' to 'very good' as they feel it ensures sufficient protection of personal data on the Internet (Frick 2022, p. 3, 10).

[32] Wawra (2022, IV. 2.).

[33] As the revised data security law in Switzerland had not yet come into force when the survey was conducted, the GDPR was used instead (cf. Gurguis et al. 2021, p. 23). The GDPR applies to Swiss companies when they handle the data of EU citizens and is, therefore, also relevant in Switzerland, even though the country itself is not part of the EU.

[34] Own translation.

[35] Own translation.

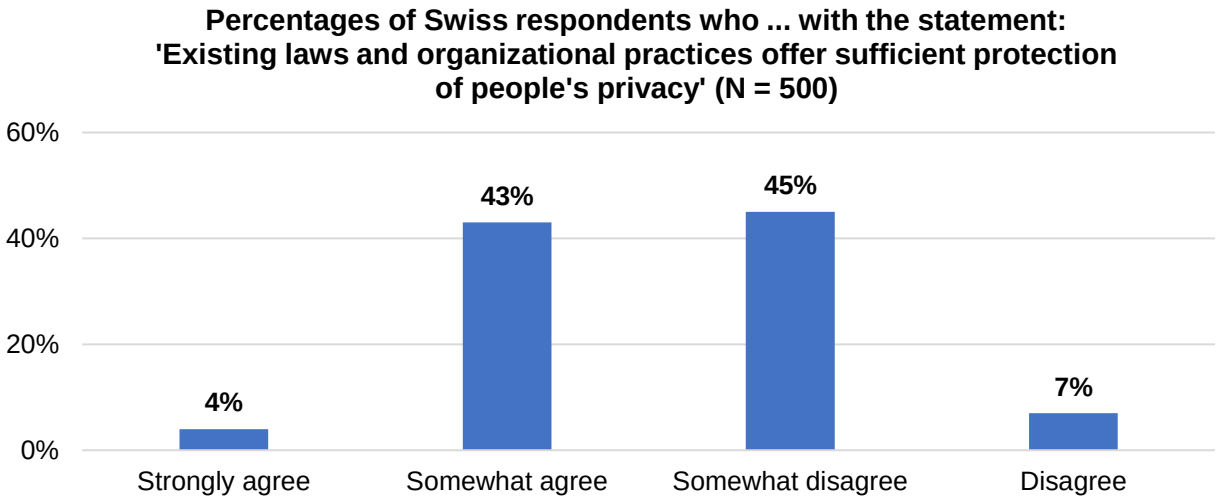

Fig. 26. Swiss respondents' satisfaction with existing data protection laws and organizational practices (cf. Guirguis et al. 2021, p. 24).[36]

CIGI-Ipsos does not provide any data for Switzerland on the question of whether respondents agree that they themselves do enough to protect their data (CIGI-Ipsos 2019b, p. 29, 2019c, p. 283). However, in a recent survey by the Swiss Federal Statistical Office (recorded in Eurostat 2022), respondents were asked which of six given measures to control their personal data on the Internet they had adopted in the past three months (see Fig. 27). For several of the measures surveyed, a majority of Swiss Internet users reported that they had adopted them during the specified time period. The most popular measure is refusing permission to use one's personal data for promotional purposes, adopted by more than two-thirds (70%), followed by restricting access to one's location (66%). More than half of respondents stated that they have restricted access to their profile and/or contents on social media or shared online storage spaces (56%) or checked the security of websites asking for their personal information (54%). However, a minority of 44% read the privacy policy before providing their personal data, and only about a quarter (24%) requested access to their personal data in order to update or delete them. Overall, four out of five respondents (87%) have adopted at least one of the listed measures, which is considerably more than the European average (73%), which the Swiss also surpass (sometimes considerably) in all six categories individually. This could be due to the fact that more Swiss people may have disclosed their personal data on the Internet than on average in the EU-27 countries. The more people disclose their personal data online, the higher the proportion of people who have reason to and therefore adopt measures to manage access to their personal data online (cf. Bundesamt für Statistik 2018, p. 10). Data from 2016-2017 show that substantially more Swiss individuals disclosed their personal data online than in the EU-27 countries (87% vs. 56%), a tendency that generally applies to the digitally most developed countries (cf. Bundesamt für Statistik 2018, p. 7). Unfortunately, no data on this is available in the Eurostat dataset for 2018-2021.

[36] Own translation.

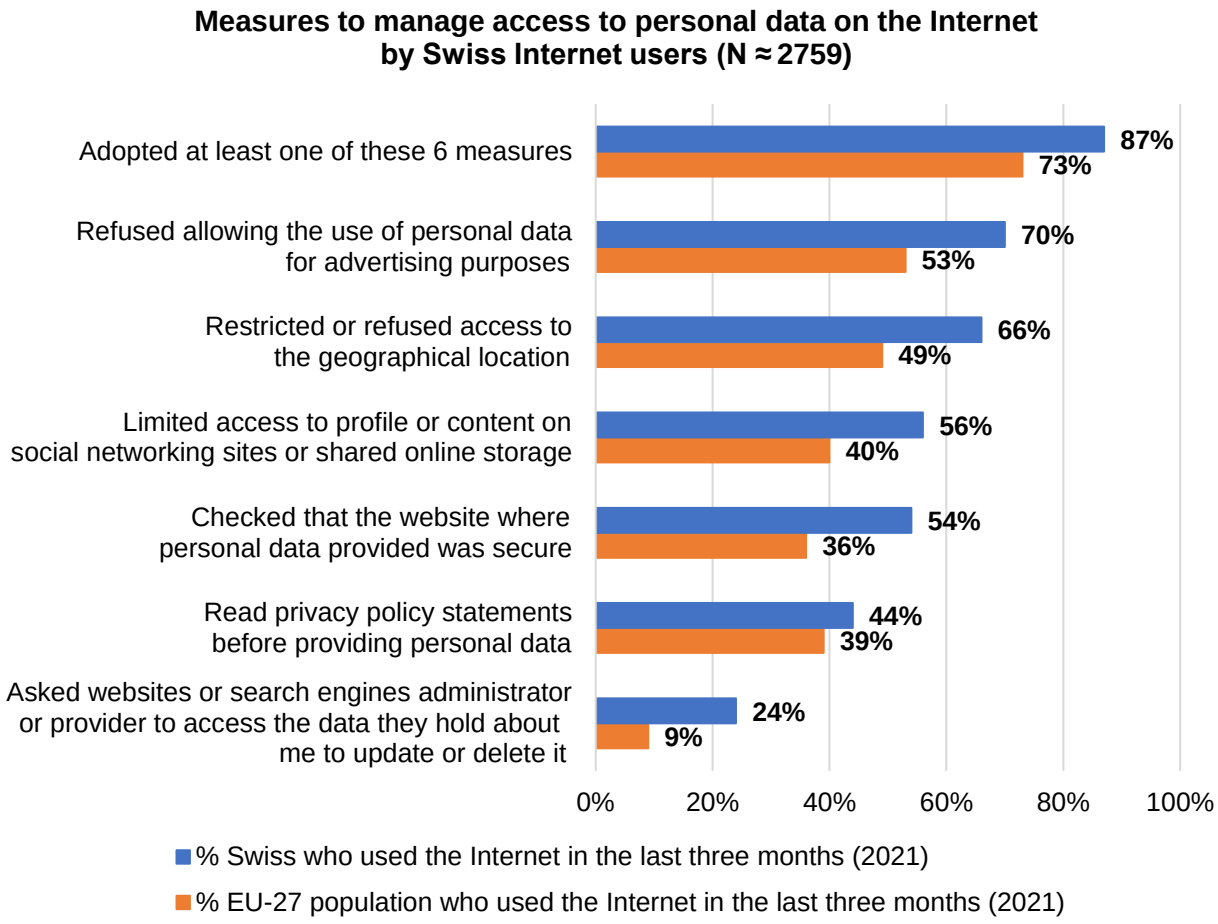

Fig. 27. Measures to manage access to personal data on the Internet by Swiss Internet users (cf. Eurostat 2022).

A more detailed picture concerning some of these measures is provided by Latzer et al. (2019, 29-30; Fig. 28). They found that only 16% of Swiss Internet users often read the privacy policy when using online services. Almost half of Swiss Internet users (49%) do so sometimes or rarely, and 35% never read the privacy policy. Thus, overall, the measure is adopted by almost two-thirds of Swiss Internet users at least on rare occasions. Similar to the results presented above, requesting the deletion of one's personal data is done less frequently. More than half of Swiss Internet users (54%) never adopt this measure, and only 13% do so often. The remaining third does so sometimes or rarely.

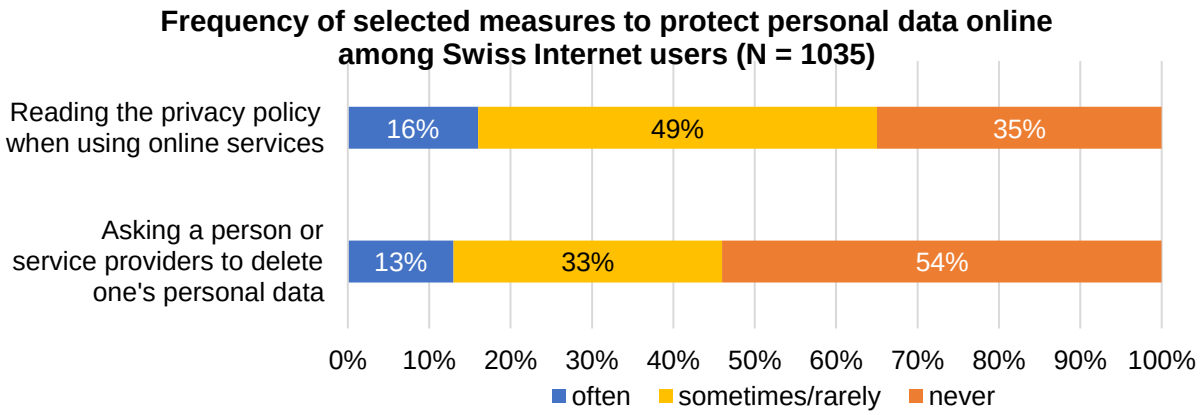

Fig. 28. Frequency of selected measures to protect personal data online among Swiss Internet users (cf. Latzer et al. 2019, p. 29-30).[37]

In the survey conducted by Eurostat (2022), respondents were also asked about their knowledge and preventative measures regarding the tracking of online activities (Fig. 29). Three-quarters (75%) of Swiss Internet users stated they know that cookies can be used to trace movements of people on the Internet, which is slightly less than the EU-27 average (80%). However, only a minority of them take action to counteract such tracking of their online activities: just over a third (37%) of Swiss Internet users stated that they have ever changed the settings of their Internet browser to prevent or limit cookies, and only one in five (21%) use software that limits the tracking of their activities on the Internet. In this lack of action, Swiss Internet users are very similar to the EU-27 average (cf. Fig. 29).

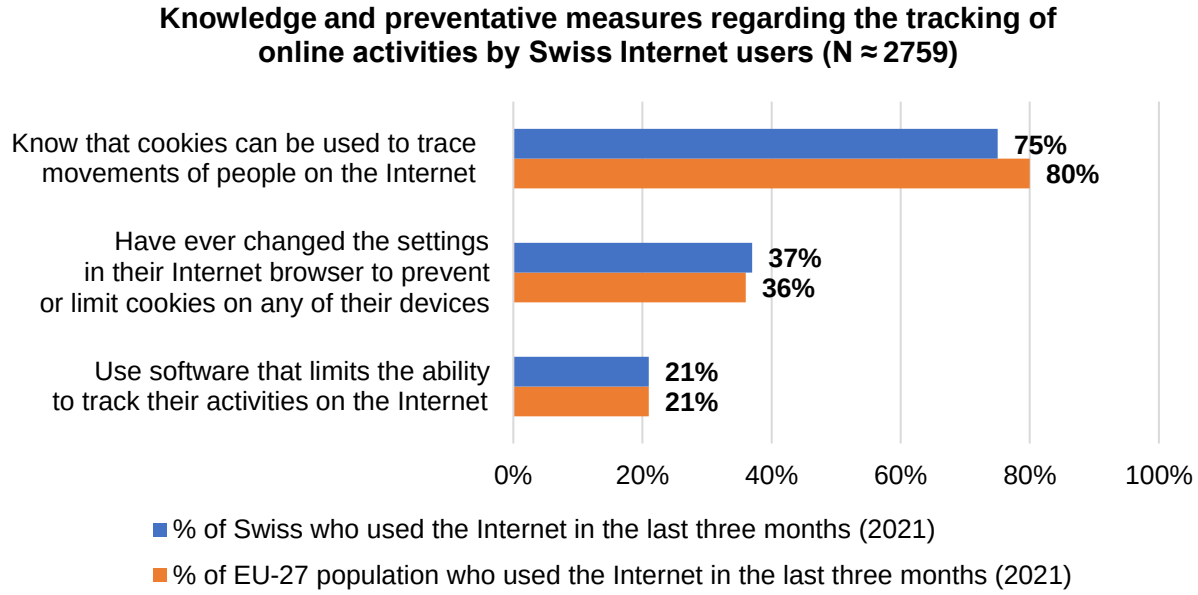

Fig. 29. Knowledge and preventative measures regarding the tracking of online activities by Swiss Internet users in 2021, compared to the EU-27 average (cf. Eurostat 2022).

Finally, the majority of Swiss PC and smartphone users have security software on their devices (Fig. 30, cf. Bundesamt für Statistik, 2021b). However, it is notable that these majorities have

[37] Own translation.

decreased slightly in recent years: while almost two-thirds (65%) of Swiss Internet users used security software to protect their PC in 2019, it was only 60% in 2021. Likewise, the proportion of smartphone users with security software on their device decreased slightly from 60% in 2019 to 57% in 2021.

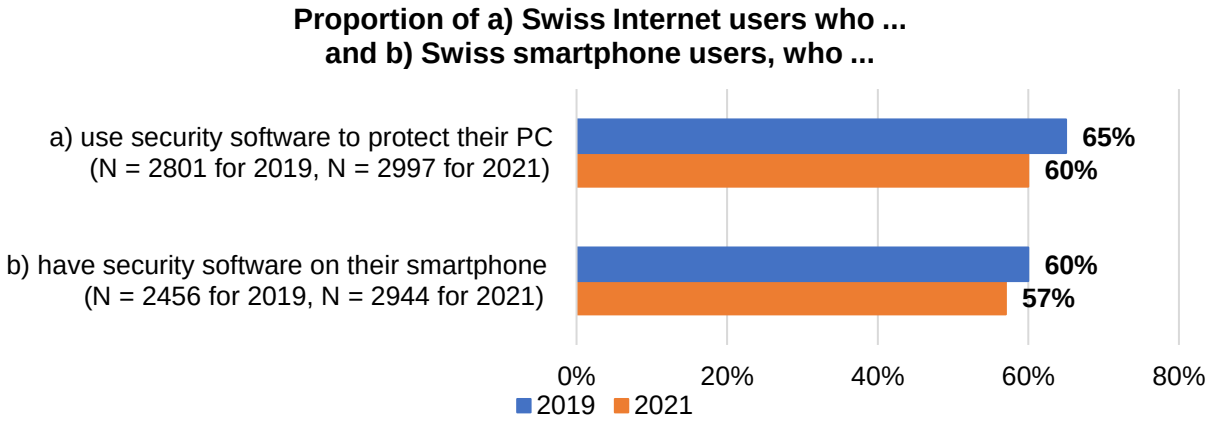

Fig. 30. Use of security software among Swiss Internet and Swiss smartphone users (cf. Bundesamt für Statistik 2021b, p. 2, 6).[38]

IX. Attitudes Towards Data Receiver

[This] parameter […] refers to [Swiss people's] attitudes towards institutions to which they disclose their data. These comprise above all their trust in national and foreign governments and (different kinds of) companies pertaining to the protection and correct use of their data.[39]

A majority (58.5%) of respondents from Switzerland feel that most people can be trusted (cf. EVS/WVS 2021c, p. 175) (Fig. 31). This general trust towards others (or lack thereof) could influence Swiss people's decisions on data disclosure. The following chapters provide more detailed insights into respondents' attitudes towards governments (IX. 1.) and companies (IX. 2.). In IX. 2., a comparison of these two sets of attitudes will be attempted whenever relevant data are available.

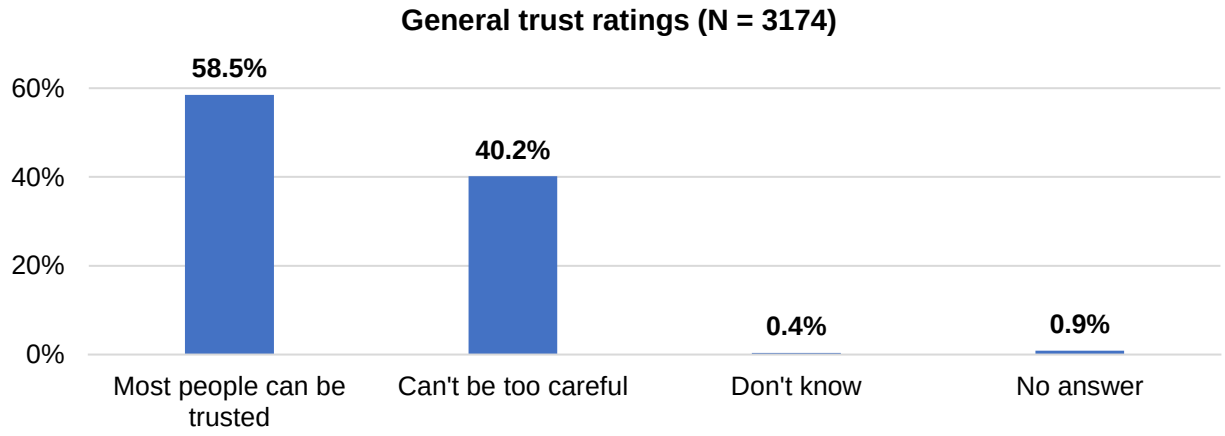

Fig. 31. Trust towards others in Switzerland (cf. EVS/WVS 2021c, p. 174).

[38] Own translation. The information on the respective N of the subsamples was obtained through personal communication.

[39] Wawra (2022, IV. 2.).

1. Attitudes Towards Governments

The majority of Swiss respondents report that they trust their government (66.3%) and parliament (57.6%), while trust in political parties is fairly low (25.1%) (cf. EVS/WVS 2021c, pp. 267, 274, 276) (Fig. 32).

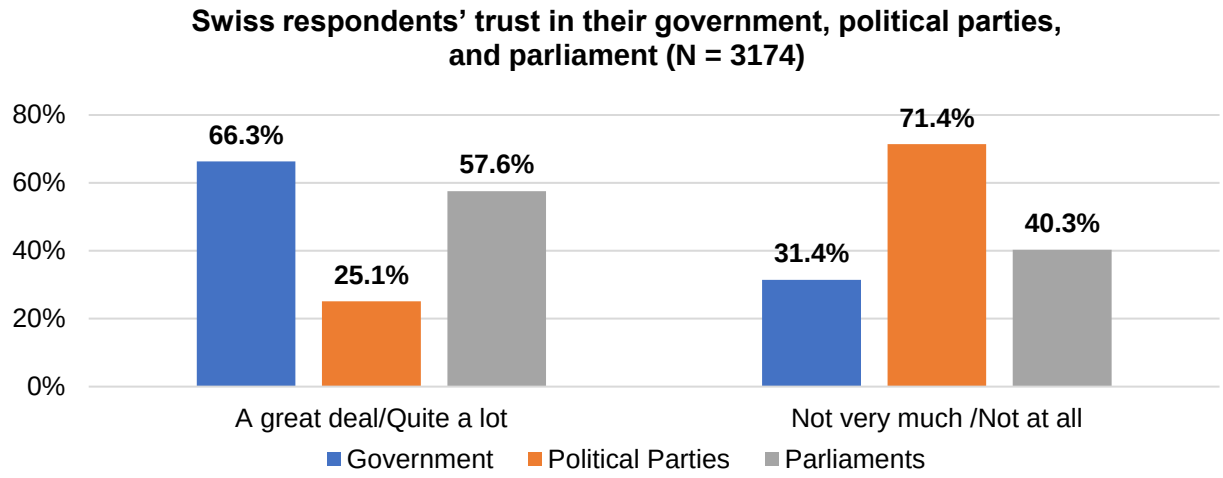

Fig. 32. Swiss respondents' trust in their government, political parties, and parliament (EVS/WVS 2021c, pp. 267, 274, 276).

Similar results were obtained in another survey (von Wyl et al. 2021), which found that more than two-thirds of the Swiss (68.7%) have high trust in their government or health authorities (Fig. 33). Notably, these levels of trust were found to influence Swiss people's data disclosure behavior, as higher levels of trust were positively related to the use of a COVID-tracing app (von Wyl et al. 2021, p. 6).

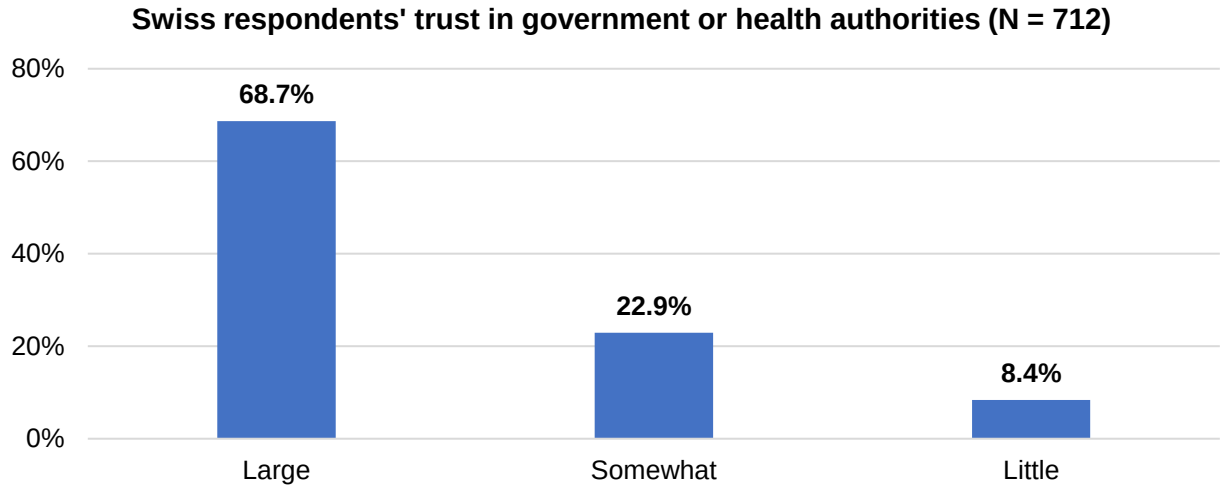

Fig. 33. Swiss respondents' trust in government or health authorities (cf. von Wyl et al. 2021, p. 6).

Ipsos (2019, p. 20) does not provide any data for Switzerland on people's trust in their own government or foreign governments with regard to the correct use of personal data. However, Guirguis et al.'s (2021) survey findings suggest that Swiss peoples' confidence in the correct use of their personal data by their government is rather strong. A clear majority (74%) of respondents fully or

rather agreed with the statement that "most government institutions treat the personal data they collect about users properly and confidentially" (Fig. 34), while only about a quarter (26%) rather disagreed or disagreed (cf. Guirguis et al. 2021, p. 24).

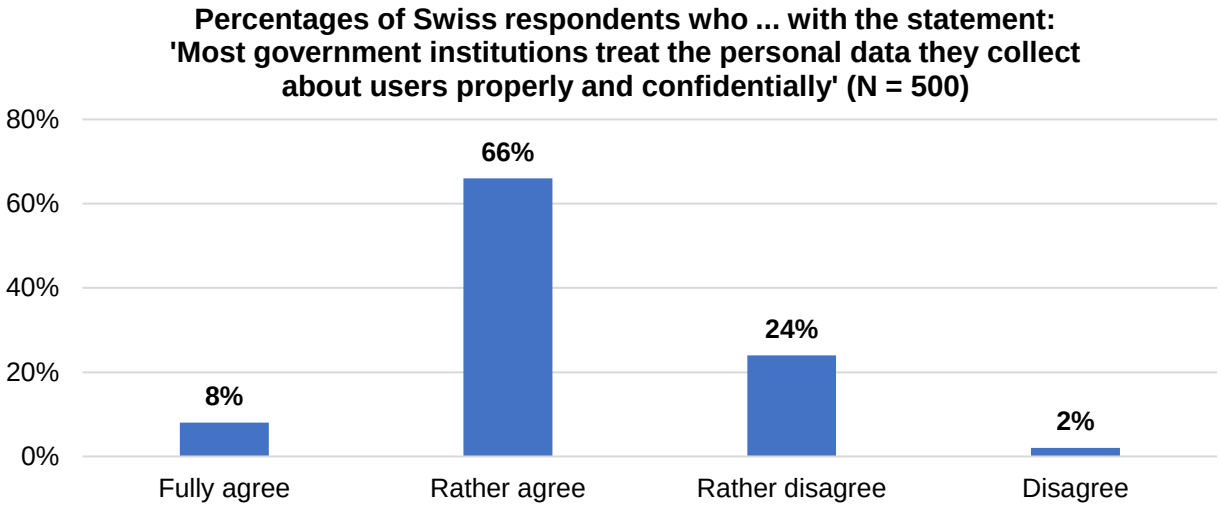

Fig. 34. Swiss respondents' trust in the correct handling of personal data by government institutions (cf. Guirguis et al. 2021, p. 24).[40]

However, a survey by Oliver Wyman (2021a, b) found that a considerably smaller number, but still a majority of Swiss people (52%) trust the government and government agencies in matters of personal data disclosure, while a minority of about a third (32%) have no trust in this regard (Fig. 35). Frick (2022) found that government agencies are trusted by the Swiss to a medium-strong degree, with an average score of 7.0 on a 10-point scale (1 = no trust at all, 10 = very strong trust) regarding the handling of consumer data.

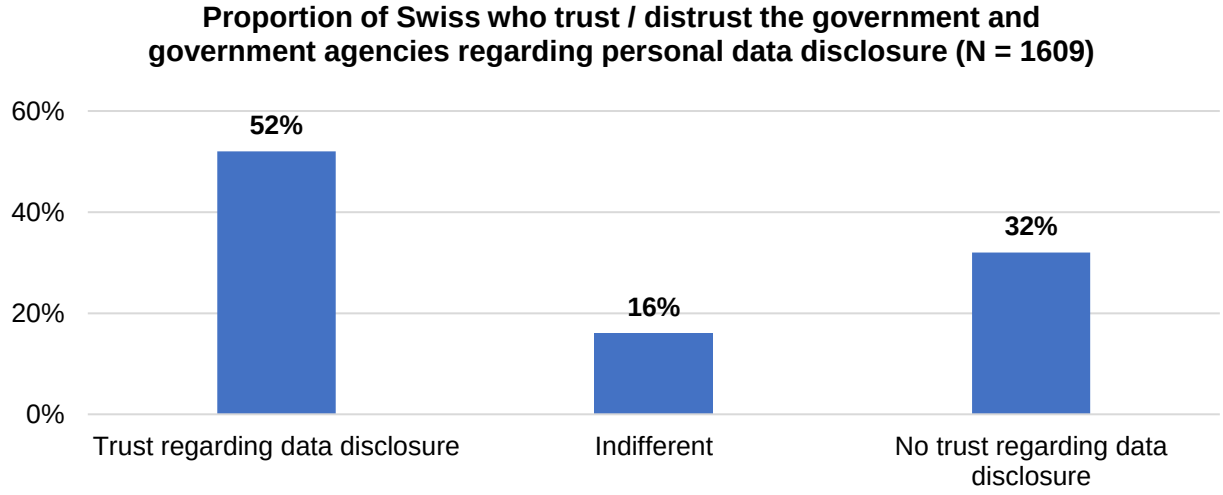

Fig. 35. Swiss respondents' trust in government and government agencies regarding personal data disclosure (cf. Oliver Wyman 2021b, p. 3).[41]

It is noteworthy that people in Switzerland trust their government far less with regard to health-related data, at least under certain conditions. In the hypothetical scenario that their health-related

[40] Own translation.

[41] Own translation.

data and samples would be stored in a biobank, less than a third of Swiss residents (29.1%) have strong trust that their government would keep them confidential and protected if it had access to them, while a majority of 71.0% have low trust (Brall et al. 2022, p. 7). In comparison, other actors such as doctors (in particular one's own doctor) and researchers at universities are trusted considerably more in this regard (Fig. 36).

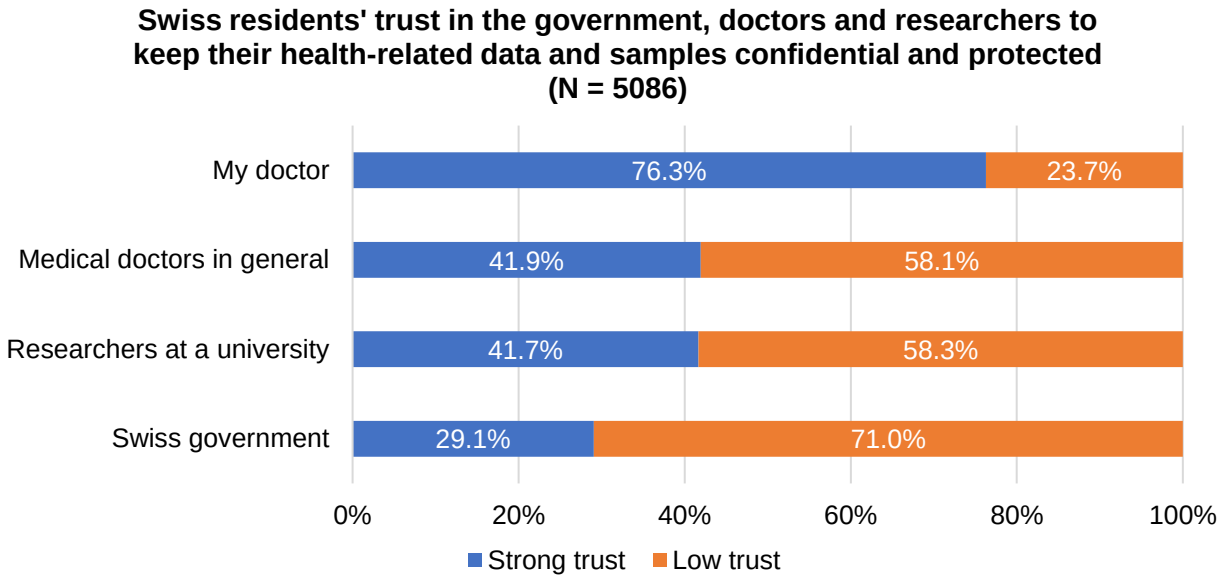

Fig. 36. Swiss residents' trust in the government, doctors and researchers to keep their health-related data and samples confidential and protected (cf. Brall et al. 2022, p. 7).[42]

CIGI-Ipsos (2019a, p. 117, 119, 2019c, p. 20) did not survey Swiss people on whether their government or foreign governments contribute to their distrust of the Internet. However, a recent survey showed that around a quarter (27%) of Swiss Internet users are concerned that the government may violate their privacy online (Latzer et al. 2021b, p. 19). In addition, 89% of Swiss believe that both governmental and commercial websites collect too much data overall (cf. Statista 2018).

According to a survey by Deloitte (2022), the majority of Swiss people are willing to use e-government services (61%, Fig. 37) and would be willing to use a number of new e-government services at least sometimes (74-88% depending on the service). This speaks for relatively widespread trust in the government in this regard.

[42] As in the original source, answers to a 5-point Likert scale (1= no trust, 5 = strong trust) are categorized here into 'low trust' (1-3) and 'strong trust (4-5).

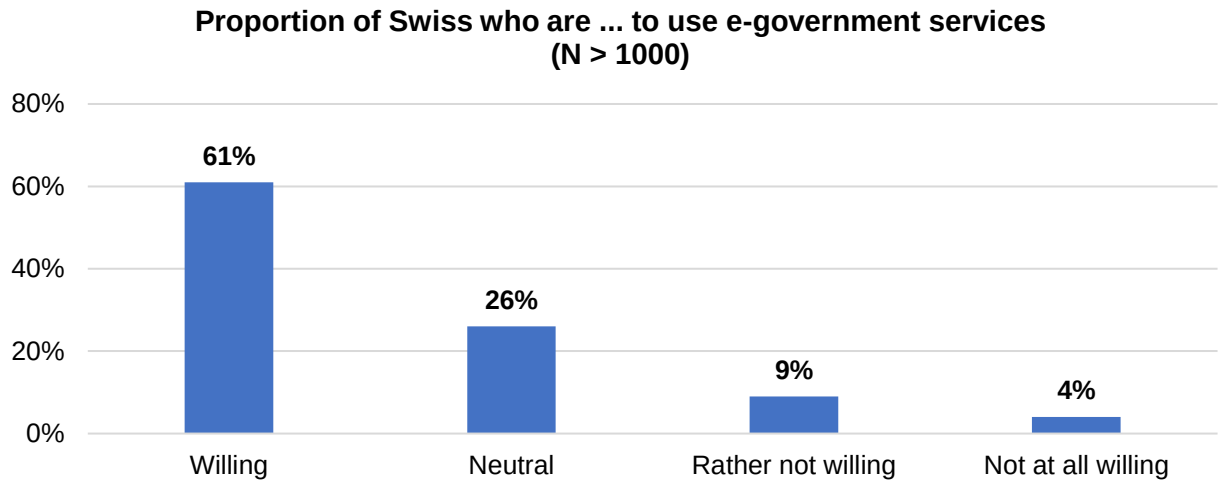

Fig. 37. Swiss respondents' willingness to use e-government services (cf. Deloitte 2022, p. 6, 9).[43]

CIGI-Ipsos (2019b, p. 45) does not provide any data for Switzerland on the question of whether people consider their government's efforts to protect their data to be sufficient. In this context, it is noteworthy that 63% of Swiss respondents view the state as primarily responsible for ensuring data security and data protection (cf. Guirguis et al. 2021, p. 25).

2. Attitudes Towards Companies

CIGI-Ipsos (2019c, p. 283) does not provide any data for Switzerland regarding the question of how much trust people have in companies to do enough to protect their data.

While the Ipsos survey (2019, p. 20), which examined people's confidence in the correct use of their data by different types of companies, did not include Switzerland, a recent survey (Frick 2022) with a similar question provides insights into Swiss people's trust in different types of companies and organizations regarding the handling of consumer data (Fig. 38). Banks enjoy the highest level of trust (mean rating of 7.1 on a 10-point scale), followed by insurance companies (6.3), booking portals (6.1) and e-mail providers (6.0). All these companies are above the center of the scale (5.5), meaning that, on average, the Swiss tend to trust these companies. Directly below the center are online shops, comparison portals and smartphone manufacturers (5.4 each), followed by business networks (5.2), chats/messenger providers (4.8) and search engines (4.7), which means that the Swiss tend not to trust these companies (or at least only show little trust). Social-media platforms and dating portals received the lowest trust ratings (3.9 and 3.7, respectively). It is noteworthy that the respondents showed higher levels of trust towards government agencies than almost all types of companies included in this study. Only banks received a minimally higher level of trust than government agencies (0.1 on a 10-point scale).

[43] Own translation.

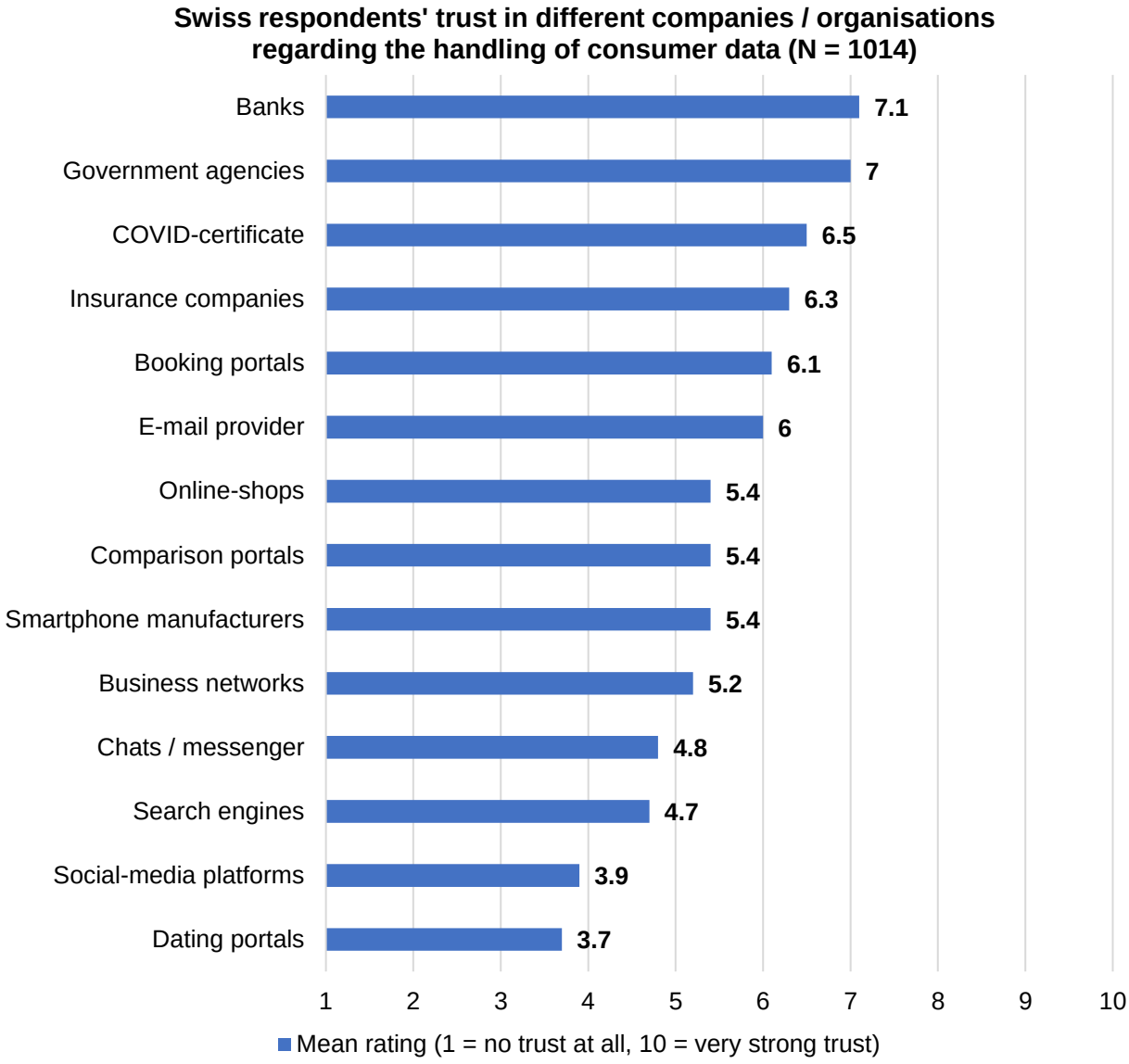

Fig. 38. Swiss respondents' trust in different companies and organizations regarding the handling of consumer data (cf. Frick 2022, p. 9).[44]

The high levels of trust that the Swiss have in banks with regard to data-related matters is corroborated by another study (Oliver Wyman 2021a, b). Fig. 39 shows that a majority of 61% of Swiss trust banks regarding the disclosure of their personal data. Only hospitals, doctors or health insurance companies are trusted by a higher proportion of Swiss in this matter, namely by over two-thirds (69%). Universities, higher education institutions and research institutions are trusted to a similar degree as banks (namely by 60% of the Swiss). Just over half of respondents trust car and household insurance companies (53%). However, a minority of Swiss trust retailers, cell phone companies and airlines and travel companies with regard to personal data disclosure (41-42%). Online shops such as *Amazon* and tech companies such as *Google* come in last, with less than one in four respondents (24% each) trusting them with regard to personal data disclosure. Comparing these results with those for the government and government agencies, one notices that the latter are trusted by a higher proportion of Swiss (52%) in this context than most of the company types

[44] Own translation.

examined (retailers, cell phone companies, airlines and travel companies, online shows and tech companies). Again, banks surpass the government in terms of trust, as do health insurance companies, which is probably due to the fact that they were grouped together with doctors and hospitals in this survey. Car and household insurance companies are trusted by about the same proportion of Swiss as the government and government agencies.

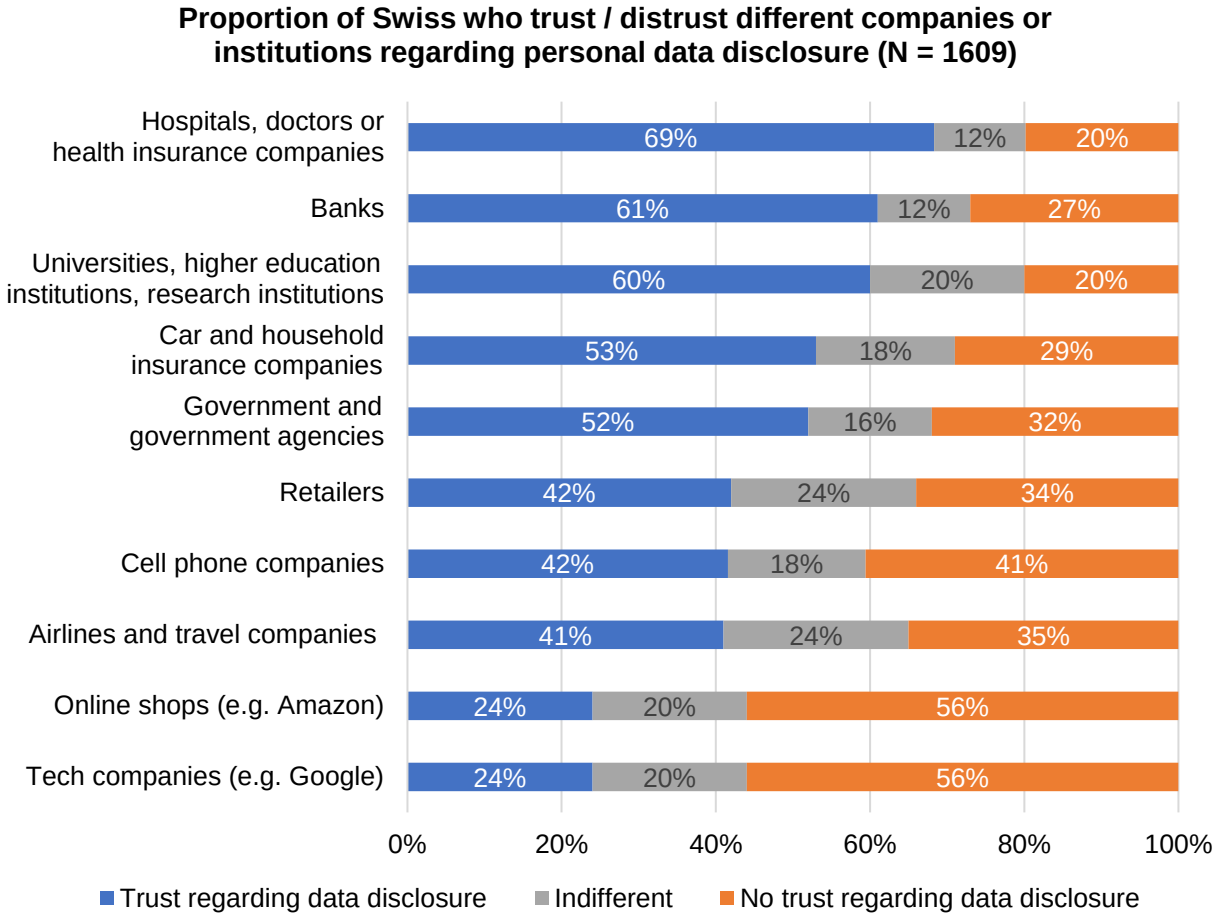

Fig. 39. Swiss respondents' trust in different companies and organizations regarding personal data disclosure (cf. Oliver Wyman 2021b, p. 3).[45]

With regard to health-related data, Brall et al. (2022) also found varying levels of trust among the Swiss towards different types of companies. In this survey, Swiss residents were asked about the extent to which they trust various actors to keep their health-related data and samples confidential and protected if they had access to them in a biobank. As Fig. 40 shows, people in Switzerland trust companies very little in this respect: all types of companies listed received low ratings of trust from at least 90% of respondents – even health insurance companies, which contrasts with the findings by Oliver Wyman (2021b, p. 3). This is probably due to the fact that in Oliver Wyman's study, health insurance companies were grouped together with hospitals and doctors, the latter of which seem to be trusted considerably more by the Swiss (cf. Fig. 40). However, health insurance companies are trusted slightly more than pharma companies (being trusted strongly by 8.4% and 6.4%, respectively), whereas other private, for-profit companies clearly received the lowest amount of trust (being trusted strongly by 3.4 % and 2.0%, respectively, depending on whether they are Swiss or international). In contrast, the Swiss government is trusted substantially more in this

[45] Own translation.

context than all these types of companies: more than a quarter (29.1%) of respondents showed strong levels of trust towards their government to keep their health-related data and samples confidential and protected.

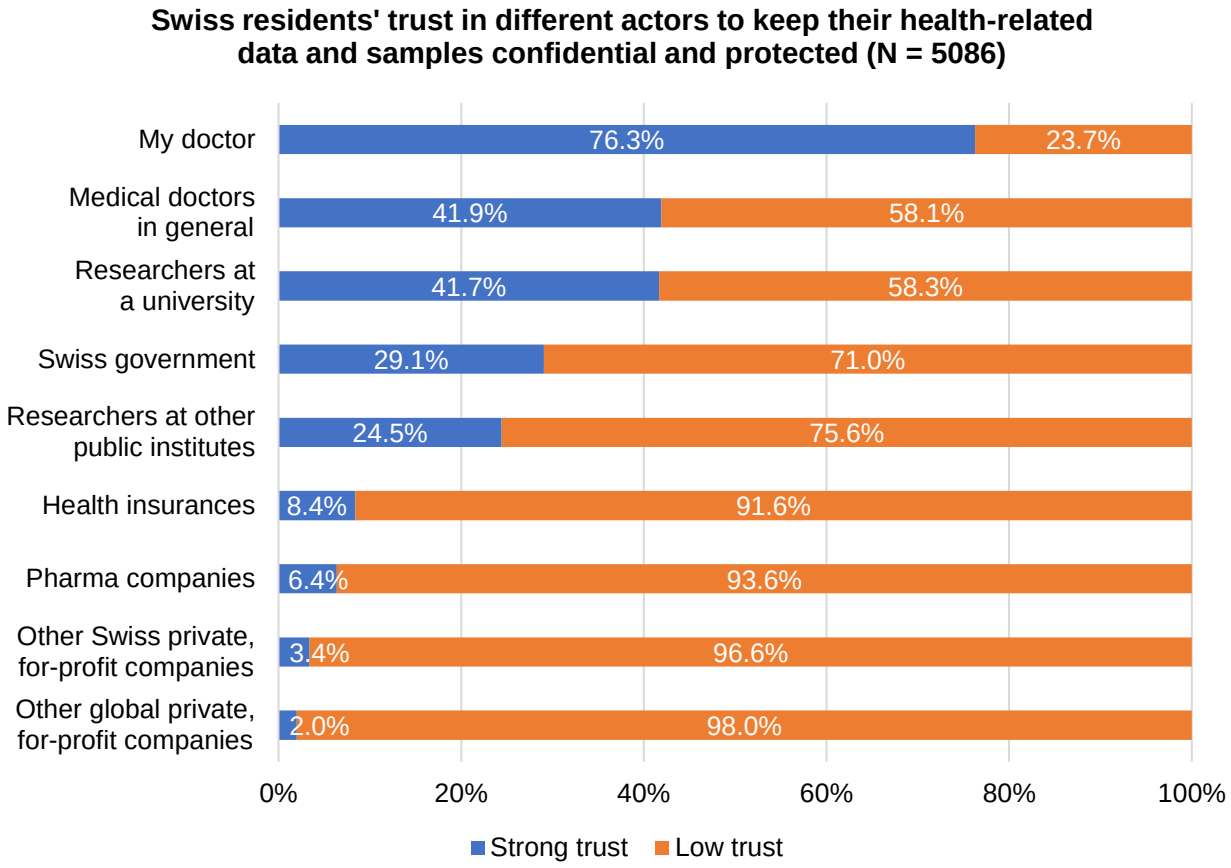

Fig. 40. Swiss residents' trust in different actors to keep their health-related data and samples confidential and protected (cf. Brall et al. 2022, p. 7).[46]

CIGI-Ipsos (2019c, p. 20) does not provide any data for Switzerland with regard to the question of the extent to which different types of companies contribute to distrust of the Internet. However, almost half (47%) of Swiss Internet users are rather or strongly concerned about companies violating their privacy online (Fig. 41, cf. Latzer et al. 2021b, p. 19). In comparison, only slightly more than a quarter (27%) have this concern with regard to their government. The category 'other people' occupies the middle ground: around four out of ten Swiss Internet users (39%) are concerned about violations of privacy on the Internet by this party.

[46] As in the original source, answers to a 5-point Likert scale (1= no trust, 5 = strong trust) are categorized here into 'low trust' (1-3) and 'strong trust (4-5).

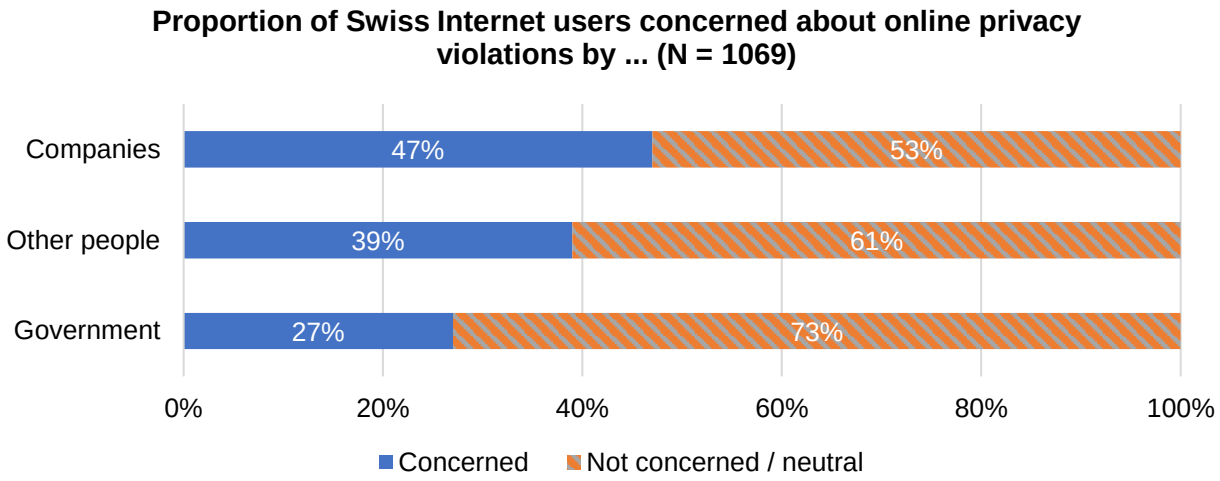

Fig. 41. Proportion of Swiss Internet users concerned about online privacy violations by companies, the government and other people (cf. Latzer et al. 2021b, p. 19).[47]

In addition, the majority (63%) of Swiss see the government as the main actor for ensuring data security and protection, while only 32% see this responsibility lying primarily with privately owned companies (cf. Guirguis et al. 2021, p. 25) (Fig. 42).

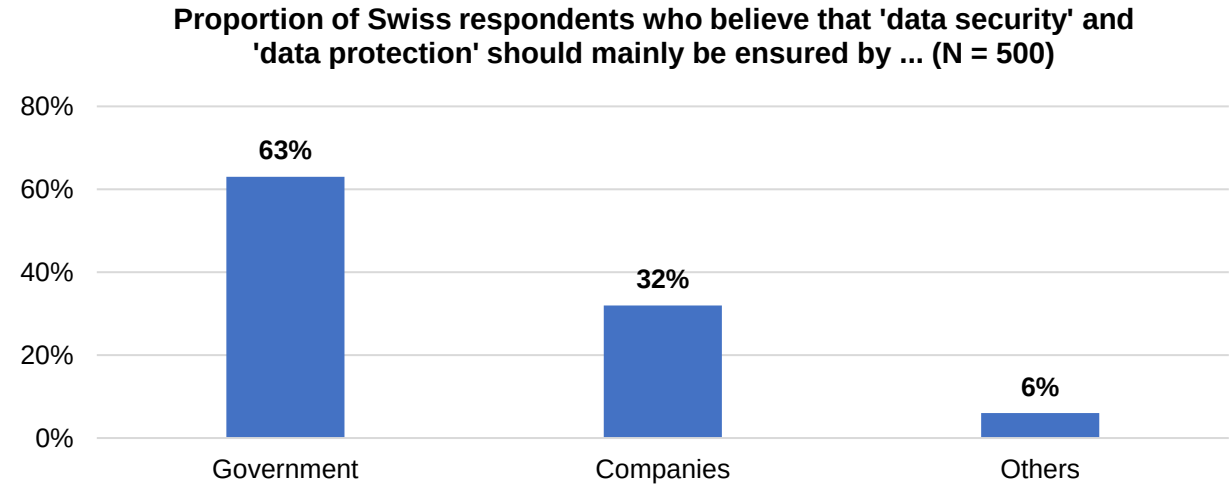

Fig. 42. Swiss respondents' views on who should mainly ensure 'data security' and 'data protection' (cf. Guirguis et al. 2021, p. 25).[48]

Moreover, majorities of over 80 % of Swiss respondents prefer that various e-government services be provided by a government agency rather than by the private sector (Deloitte 2022; see Fig. 43). Notably, the Swiss people's distrust of private companies regarding e-government services seems to have resulted in a clear majority voting against the introduction of an electronic identity (E-ID) in March 2021, mostly because the government had planned to outsource its issuing to private actors, which caused suspicion among Swiss citizens (Deloitte 2022, p. 16).

[47] Translation according to Latzer et al. (2020, p. 28). In the original source, responses to the statement 'I'm concerned that … may violate my privacy online' on a 5-point scale (1 = do not agree at all, 5 = strongly agree) were summarized to 'no' (1 and 2), 'neutral' (3) and 'yes' (4 and 5**;** own translation). Exact percentages were only provided for 'yes'.

[48] Own translation.

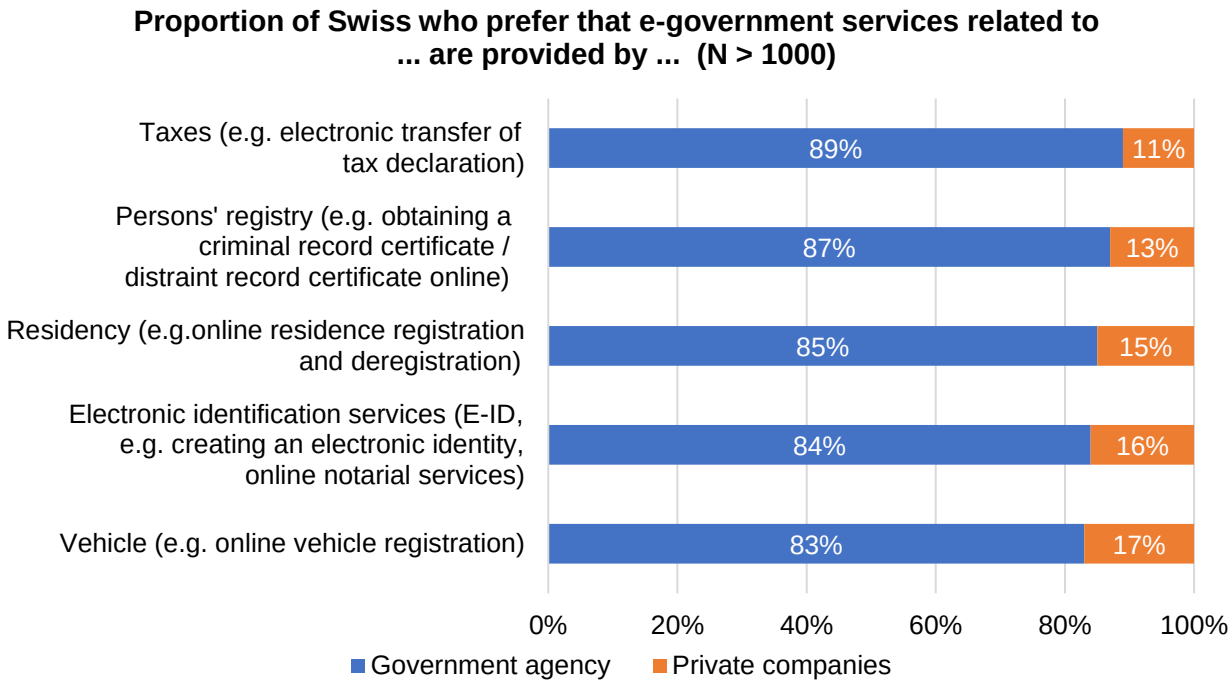

Fig. 43. Swiss respondents' preferences regarding the provision of e-government services (cf. Deloitte 2022, p. 16).[49]

X. Communication on Data Use

[This] parameter […] relates to the importance [Swiss respondents] attribute to communication on how their personal data are used.[50]

Ipsos (2019, p. 14) does not provide any data for Switzerland regarding the questions of whether people would be more likely to provide their data to companies that transparently communicate what the data will be used for and whether they would be most likely to share their data with companies or government institutions that clearly communicate potential risks (cf. Ipsos 2019, p. 17).

With regard to health-related data and samples in particular, two studies offer insights into Swiss people's preferences regarding communication on data use. Pletscher et al. (2022) found that almost two-thirds of Swiss (64%) think they would be more likely to share their anonymized health data if they knew the exact research purpose for which it was collected (Fig. 44).

[49] Own translation.

[50] Wawra (2022, IV. 2.).

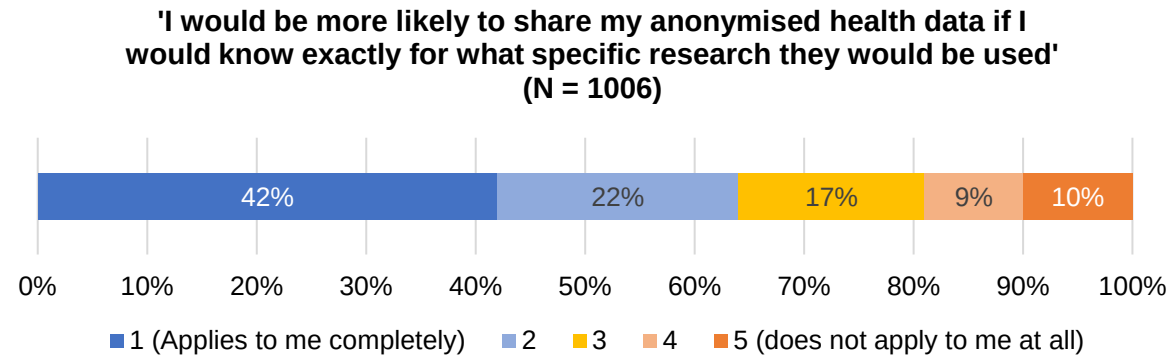

Fig. 44. Relevance of knowing the exact research purpose when sharing anonymized health data for Swiss respondents (cf. Pletscher et al. 2022, p. 6).

Brall et al. (2022) asked respondents how often a biobank should ask them for their consent to use their health-related data and samples in research projects (Fig. 45). Most respondents (39.0%) wanted to be asked again for every new research project, so clear communication about when and for which research purposes their data and samples would be used seems important to them. More than a quarter (29.4%) said that this would depend on the type of project being considered. Thus, it seems that a majority of Swiss residents (68.4%) value having at least some information about which research projects their health-related data and samples would be used for. Only for less than one in five residents (17.7%) was it sufficient to be asked for their consent once. The remaining 13.8% were not sure.

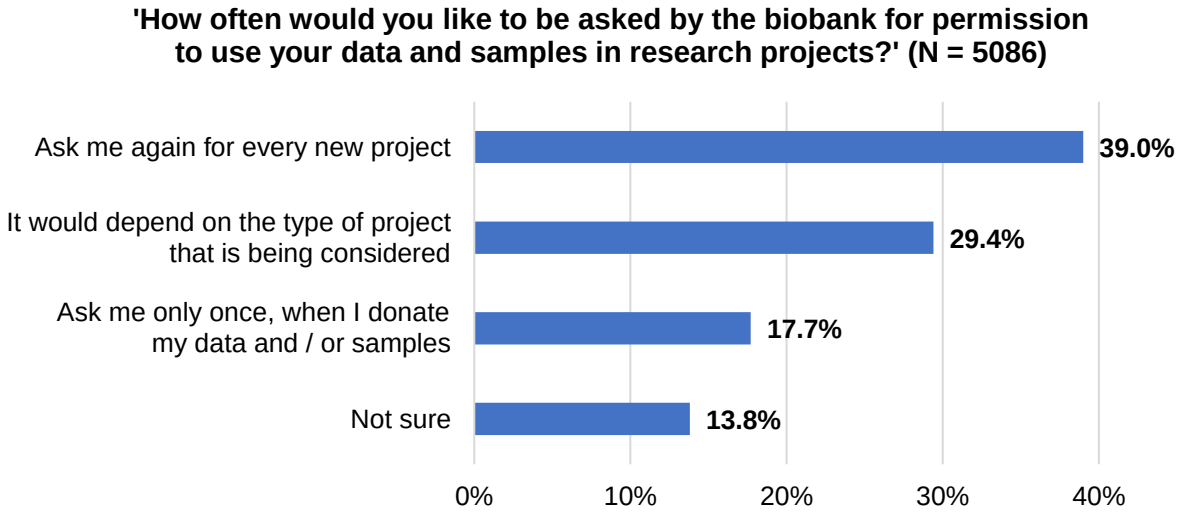

Fig. 45. Preferences of Swiss residents regarding the frequency of being asked for consent to use their health-related data and samples in research projects (cf. Brall et al. 2022, p. 6).

XI. Key Findings

This section summarizes and interprets the main findings of the studies presented above to provide a quick overview of the major outcomes of the analysis and to facilitate cross-cultural comparison. Furthermore, research gaps are identified. As far as possible, the general direction of the influence of the various factors cited below on the WTS personal data is indicated, i.e. positive (increasing) or negative (decreasing) (cf. also Wawra 2022, II. 9. and IV. 2.). It should be noted that we focus on each parameter's influence on the WTS data from a macro perspective. Their individual

intensity, reaching from a potentially significant to no influence at all, depends on the interplay with other cultural-contextual as well as socio-demographic (e.g. age, education, gender, income) and personality parameters in concrete situational contexts (cf. Wawra 2022, II. 9., III., IV. 3.). This needs to be researched with a micro-level approach. Socio-demographic factors and personality traits in particular are still under-researched in relation to Swiss people's WTS data (cf. Wawra 2022, IV. 3.).

1. Digital Competitiveness

For its overall performance, Switzerland is in 6th place out of 64 evaluated countries in the IMD (2021) ranking for digital competitiveness. It is thus in the top 10 as well as in the top 10% of all countries. Furthermore, it is at least among the top three in two of the three main categories that indicate a country's digital competitiveness in the ranking: It occupies rank 1 for knowledge and rank 3 for future readiness for digitalization. In the last of the three main categories, technology, it places among the top fifth (rank 11).

Switzerland ranks at least among the top 8 of all countries in all three subfactors for knowledge (talent, training and education and scientific concentration). In the category future readiness, it achieved 4th place for the subfactors of business agility and IT integration and 10th place for adaptive attitudes. For all subfactors of technology (regulatory framework, capital and technological framework, it ranks at least among the top 20% of all countries. For the items of these subfactors, the country is mostly among the top 20 to 30%. For the remaining items, Switzerland is still mostly in the midfield. The effect (of the individual components) of this parameter on people's WTS personal data has yet to be studied in detail (cf. Wawra 2022, IV. 2.).

2. General Value of Informational Privacy

It depends on the situational context whether Swiss respondents consider governmental surveillance acceptable or not. Only a minority of the Swiss approve of governmental email and Internet monitoring (25.7%) as well as secret data collection by the government in general (17.7%). In fact, Swiss people seem critical of online surveillance in general: Almost half (44%) believe that online surveillance is harmful to society (as opposed to 24% who do not; Latzer et al. 2019). Almost three-quarters (74%) of Swiss Internet users claim to be vigilant about protecting their privacy on the Internet (Latzer et al. 2021b). Thus, a majority of Swiss people place high value on their online privacy. This stands in contrast to informational privacy in the public sphere, where government surveillance is accepted by a majority of Swiss (62%).

Regarding Swiss perceptions of employer monitoring, several questions remain unanswered due to a lack of survey data, and further research is necessary to allow for firm conclusions regarding the value the Swiss place on informational privacy in professional contexts.

Regarding the value of informational privacy vis-à-vis companies in the Swiss context, there is a partial lack of survey data: no data could be found regarding the questions of whether Swiss people believe that consumers should be able to refuse the use of collected data by companies or that they should be paid or rewarded for allowing it. However, one study (Jarchow and Estermann 2015) found that less than a tenth (9%) of Swiss expert respondents think that people receive a fair compensation for disclosing their data online, suggesting that Swiss consumers' online privacy should be valued more highly through fair compensation by companies for data disclosure.

3. Degree of Privacy of Data

Personal data are legally classified as sensitive in Switzerland if they reveal information about

- religious, ideological, political or trade union views or activities

or are related to

- health
- the intimate sphere
- racial or ethnic origin
- social security measures, or
- administrative or criminal proceedings and sanctions.

Sensitive data furthermore includes

- genetic and biometric data that unequivocally identifies a natural person.

Due to a lack of survey data, no conclusions can be drawn about how these and other more general categories of personal data are perceived by Swiss respondents. Further research in this area is needed to close this research gap.

Regarding certain more specific categories of data, such as different types of health-related data, no direct evidence in the form of sensitivity ratings by Swiss respondents could be found. In one study (Latzer et al. 2015), Swiss respondents were asked how important it was for them that only they or people authorized by them know certain types of personal online data. The findings indicated that respondents perceived the contents of e-mails and other correspondences as particularly sensitive, which is reflected in the high proportion of respondents (76%) who regarded it as (very) important that this data remain confidential. This was followed by the category of online contacts, which 67% considered (very) important to remain confidential. Further evidence regarding the perceived sensitivity of different types of online data may be derived from a study that showed which types of personal data were shared on the Internet by Swiss respondents in 2021 (Bundesamt für Statistik 2021a, b). The findings show that, for example, one's current location or personal details (such as name, date of birth, or ID number) were shared by smaller proportions of people (50% and 56%) than payment information (68%) and contact information (72%). Other information (e.g. health status, employment status, photos) was shared by the least amount of people (20%). These findings may be indicative of perceptions of sensitivity of these data categories by Swiss people, although they cannot be seen as directly reflecting them, since they are clearly also influenced by practical constraints, such as which types of information need to be shared frequently when using various online services.

Health-related data appear to be perceived as fairly sensitive in the Swiss context, which is reflected in the fact that almost half (45.6%) of Swiss residents stated that they would be unwilling to disclose their health-related data and biological samples for research purposes in a survey by Brall et al. (2021). Of those 53.6% of respondents who were willing to provide this type of data, comparatively high proportions stated that they would be willing to disclose data in questionnaires about their health status, blood samples or self-collected biological samples (> 80% of respondents in each case). A majority of about 60% each were willing to provide biological samples taken by medical staff or medical records about themselves, and half of the respondents (50.1%) were willing to share their family's medical history. These unexpectedly high levels of willingness to disclose these

types of health-related data may be explained by the research context, namely the opportunity to improve treatments in the future. In contrast, comparatively small proportions were willing to provide data collected via apps (36.2%) and social media data (14.2%). However, this finding may be due to respondents' considerations of the time and continued effort necessary when providing these types of data or a lack of trust in the security of data storage in apps and on social media platforms, rather than the perceived sensitivity of these categories of data. Overall, the results based on data from Brall et al.'s (2021) show that people's willingness to share personal data – including data that is typically considered rather sensitive, such as health-related data – is influenced by the context, purpose, and type of data collection. However, as stated above, more research is needed to provide direct evidence for the perceived sensitivity of different types of data, such as health-related data, by Swiss respondents before any firm conclusions can be drawn in this regard.

4. Benefits Associated with Data Disclosure

Further research is needed regarding the benefits which the Swiss associate with data disclosure in general and regarding their willingness to share personal data in exchange for benefits. Survey findings on this are available only for certain contexts of data disclosure. With regard to the use of e-government services, i.e. the disclosure of data to the government via the Internet, a majority of Swiss respondents highlight each of the following potential benefits (Deloitte 2022):

- temporal flexibility, i.e. access to the services offered at any time (75%)
- spatial flexibility, i.e. access to the services offered from anywhere (72%)
- saving time (72%)
- simplicity and convenience of the services (68%)
- user autonomy (68%)
- saving money in the form of discounts (64%)
- freedom of choice (60%).

Thus, a clear majority of Swiss regard all of these factors as benefits for disclosing their data to the government via the Internet.

With regard to the sharing of health-related data in particular, two studies suggest that financial compensation is not a relevant benefit for most Swiss people: more than half (56.9%) of Swiss respondents consider money or any other material compensation to be (rather) unimportant for providing their health data and samples to a Swiss publicly funded biobank (Brall et al. 2022). Moreover, more than three-quarters (78%) of Swiss respondents deny that financial compensation would increase the likelihood of them sharing their anonymized health data (Pletscher et al. 2022). Instead, altruistic motives seem to be a relevant factor in this regard: a majority of Swiss people stated that they would be more likely to share anonymized health data if this would result in better treatment for others (86%) and if this would reduce Swiss healthcare costs and thus health insurance premiums in the long run (67%; Pletscher et al. 2022). Moreover, another study found perceived societal benefits to be a relevant factor in Swiss people's readiness to install a COVID-19 contact tracing app (Brüesch et al. 2020). However, one's perceived personal (health) benefit was also found to be a relevant factor in this context. This was also identified as a relevant factor in Pletscher et al. (2022), who found that a majority of Swiss would rather not share their anonymized

health data if they had no direct personal health benefit from it (60%). Thus, personal health benefits are also an important variable for a majority of Swiss when providing health-related data.

The limited relevance attributed by the Swiss to financial compensation regarding the disclosure of health-related data may be due to its sensitivity (according to the Swiss legal framework and as suggested by indirect evidence – see section XI. 3.): For Ackermann et al. (2021) conclude that the higher the perceived sensitivity of data, the less other variables (such as benefits of disclosure) affect people's WTS data:

"In other words, consumers will be very unlikely to share private data that they perceive as very sensitive, irrespective of what type of compensation they are offered in return or the degree of anonymity that is granted to them" (Ackermann et al. 2021).

If, however, data are

"not perceived as very sensitive, other factors, such as what compensation is offered and whether the data allow for personal identification […], will likely have a considerable impact on individual decisions to share these data" (Ackermann et al. 2021).

Further studies that distinguish between more and less sensitive types of data are needed to determine whether this also applies to Swiss data disclosure culture. Moreover, they should systematically differentiate between different kinds of benefits, as there might be cultural differences with regard to the value attributed to specific benefits, and this could influence people's WTS data accordingly. Previous research has, for example, differentiated between three categories of benefits: (1) "financial rewards", (2) "personalization benefits", and (3) "social adjustment benefits" (Buchwald et al. 2017). The latter have been defined as "the establishment of social identity by integrating into desired social groups" (Lu et al. 2004, p. 572), which allows individuals to "fulfil their need for affiliation" (Buchwald et al. 2017).

5. Privacy Concerns and Risks

a. Data Security

Survey data for Switzerland are still missing with regard to the question of whether people feel more comfortable with sharing their data with companies that have "never been subject to any breach, leak, or fraudulent usage of data" (cf. Ipsos 2019, p. 14). Neither was the question surveyed in Switzerland if people want their "online data & personal information" to be "stored on a secure server", preferably "in their own economy" (CIGI-Ipsos 2019b, pp. 13, 15) or abroad, and whether they care if their data left Switzerland (cf. CIGI-Ipsos 2019b, pp. 17, 19).

However, Swiss people seem very much aware of certain risks concerning data security. Four in five Swiss respondents (83%) have great or very great concerns regarding data theft, and a majority of 63% have such concerns regarding identity theft (Guirguis et al. 2021). Given these concerns, it is perhaps unsurprising that most Swiss believe that the safe handling of online data constitutes a challenge for society (65%; Latzer et al. 2019). This tendency is not without reason, since negative experiences regarding online security are widespread among the Swiss: the majority of Swiss Internet users (56%) experienced at least one of seven security-related incidents in 2019 (Eurostat 2022). While serious incidents such has fraudulent credit or debit card use were only experienced by a small minority (<6%), almost half of Swiss Internet users (47%) had been affected by receiving 'phishing' messages, substantially exceeding the EU-27 average (28%). Similarly, more Swiss people fell victim to 'pharming' (i.e., being redirected to a fake website in order to provide personal information) than the average of the EU-27 countries in the period studied (19% vs. 13%). The same applied to all remaining security-related incidents except for data loss due to computer infection.

Notably, concerns of the Swiss regarding data theft may be less pronounced in certain data disclosure contexts. In the hypothetical scenario that they would be asked to provide health data and/or biological samples for a research project, only less than a third (31.9.%) of Swiss residents indicated that they would be worried about their data being hacked and stolen (Brall et al. 2021). This comparatively low percentage may partly be due to the fact that some respondents, although worried about data theft, may have prioritized other concerns when answering this question (they were only allowed to select up to three concerns from a given list). However, it may also be due to greater levels of trust in research institutions to keep respondents' data safe from security breaches and cyber-attacks.

Concerns about data security may also lead Swiss people to avoid using certain new e-government services. In a recent survey (Deloitte 2022), about one in three respondents (30-34%) cited concerns about data/cyber security or about data protection as reasons for not (always) wanting to use a legally-binding digital signature, the electronic exchange of all data and information with government agencies and public administration and the automatic collection of tax-relevant data by the state, if they were available. Such concerns are far less widespread for traffic-related e-government services (contactless payment of parking fines, digital purchase of the motorway toll sticker), being cited by about half as many people (14-18%) as reasons for avoiding these services. About one in four respondents (24%) said they would not (always) want to use e-voting or order a pass-port or identity card online because they are worried about data/cyber security, while about a fifth (19-20%) would not (always) want to do so due to concerns about data protection. About a fifth (20-23%) said they would not (always) want to file a police report online or register themselves as unemployed online because of concerns about data/cyber security or about data protection. Such concerns are not unfounded, as recent incidents involving cyber risks to Swiss governmental databases have shown (Deloitte 2022, p. 9). The implementation of appropriate measures against cyber-attacks is crucial in order to avoid such incidents which understandably weaken the confidence of the Swiss population in the security of e-government services, and thus to increase the willingness of Swiss people to use new e-government services more frequently.

Notably, concerns about data security and data protection may lose some of their impact if external circumstances make it difficult to use traditional government services. The proportion of Swiss who submitted completed forms to public authorities via the Internet increased dramatically during the COVID-19 pandemic (45% in 2019 vs. 71% in 2021), and at a considerably higher rate than the EU-27 countries average (Eurostat 2022). In 2021, only a small fraction of Swiss (2%) did not submit official forms online due to concerns about the protection and security of their personal data (Eurostat 2022). Whether this trend will continue beyond the peak of the pandemic is a question for further research.

b. Data Control

Concerns about data control are relatively widespread in Switzerland. A large majority (> 80% each) of Swiss respondents have great or very great concerns about the misuse of data and the sale of personal data to third parties, about companies profiting from their data (70%) and disproportionate data collection (57%; Guirguis et al. 2021).

Concerns about disclosing personal information on the Internet are medium-high among the Swiss (7.05 on a 10-point scale), but were found to decrease with greater trust in government institutions regarding the right use of collected personal data and with greater satisfaction with current legislation and organizational practices regarding privacy protection (Guirguis et al. 2021).

Survey data for Switzerland are still missing on the question of whether people use the Internet differently because they distrust it. However, the available data show that online surveillance is a major concern among Swiss Internet users. The majority of respondents have experienced chilling effects online, i.e., they avoid or limit themselves in certain activities out of fear of being watched, for example when researching sensitive topics online (61%) or when expressing opinions, interests, or feelings on the Internet (58%; Latzer et al. 2021a). However, chilling effects regarding online self-expression are more frequent among Swiss Internet users than those related to information search, in that the former are always or often experienced by twice as many users (25%) than the latter (12%; Latzer et al. 2021a). Only a relatively small proportion of Swiss (13%) limit their online shopping behavior in that they never or rarely shop online due to concerns about payment security or privacy (Eurostat 2022).

Furthermore, a large proportion of Swiss Internet users take concerns about online privacy seriously: 43% do not believe that concerns about online privacy are exaggerated, compared to 27% who do and 28% who take a neutral stance in this regard (Latzer et al. 2021b). Although vigilance regarding online privacy protection is prevalent among Swiss Internet users (see XI. 2.), only a minority (40%) feel in control of their online privacy (Latzer et al. 2021b). This trend may be due to previous negative experiences among the Swiss: more than a third of Swiss Internet users believe that their personal data has been passed on or misused in the previous year (Latzer et al. 2019).

A considerable number of Swiss residents have concerns about data control regarding the special case of health-related data. When hypothetically providing their health data and/or biological samples for a research project, almost half of respondents, in each case, would worry that someone may misuse their data to discriminate against them or their family (46.8%), that their data may not be kept confidential (46.3%) or that their data may be misused for commercial or marketing purposes (45.5%; Brall et al. 2021). A less frequent concern, exhibited by only about a third (31.2%), is that private companies or researchers may benefit financially from one's data (Brall et al. 2021).

Clearly, such privacy concerns may reduce the WTS data among Swiss respondents. According to previous research (cf. e.g. Hoffmann et al. 1999, Roeber et al. 2015, and Ackermann et al. 2021), people's feeling of control over their personal data can be improved by providing a delete option for data and/or by guaranteeing anonymity. Ackermann et al. (2021) even identified the granting of anonymity as "the most effective single factor for evoking WTS". However, this does not seem to apply to very sensitive data (cf. Ackermann et al. 2021, see above). Surveys and further empirical studies on this aspect of data disclosure are needed, particularly with Swiss respondents.

6. Data Protection Literacy

No survey data could be found on Swiss people's factual knowledge of the revised data security law in Switzerland, and further research is necessary to close this research gap. Swiss people's factual knowledge of the GDPR, which applies when Swiss companies process the data of EU citizens, varies greatly: 28% of Swiss respondents state that they are very/rather familiar with the regulations and 27% report being somewhat familiar, while 40% are not at all or rather not familiar with it (Guirguis et al. 2021, p. 23). Thus, a majority of more than half of the Swiss population report to have at least some knowledge of the GDPR. However, the findings regarding Swiss people's satisfaction with data protection regulation in their country are somewhat inconsistent.[51] One study (Guirguis et al. 2021) suggests that the Swiss are divided in this respect: while just under half of respondents (47%) tended to agree that existing laws and organizational practices are sufficient

[51] CIGI-Ipsos (2019b, p. 45) does not provide data for Switzerland on the question of whether people consider their government's efforts to protect their data to be sufficient.

to protect people's privacy, a very slight majority of 52% tended to disagree on this point. In contrast, another survey (Frick 2022) suggests that a majority of Swiss are rather satisfied with data protection regulation in Switzerland: 63.7% believe that data protection regulation in Switzerland is 'rather good' or 'very good' and provides sufficient protection of personal data on the Internet.

Data for Switzerland are still lacking concerning the question of whether citizens agree that they are doing enough to protect their data (cf. CIGI-Ipsos 2019b, p. 29, 2019c, p. 283). However, data provided by Eurostat (2022) show that the majority of Swiss Internet users report having adopted various measures to control their personal data on the Internet within a three-month period. These include:

1) refusing permission to use one's personal data for promotional purposes (70%)
2) restricting access to one's location (66%)
3) restricting access to one's profile and/or contents on social media or shared online storage spaces (56%)
4) checking the security of websites that asked for personal information (54%).

Measures adopted only by a minority of Swiss Internet users in the specified time-period include:

5) reading the privacy policy before providing one's personal data (44%)
6) requesting access to ones' personal data to update or delete them (24%).

Notably, Swiss Internet users surpass the European average on each of these six measures, and also on the adoption of at least one of these measures (87% of Swiss Internet users vs. 73% for the EU-27 countries). However, this could be due to the fact that more Swiss people may have shared personal data online than on average in the EU-27 countries. Survey findings by Latzer et al. (2019) paint a more positive picture regarding measure 5 and 6: they found that a clear majority of almost two-thirds of Swiss Internet users read the privacy policy when using online services at least on rare occasions, with 16% doing so often and almost half (49%) doing so sometimes or rarely. They also found that almost half (46%) of Swiss Internet users request the deletion of their personal data at least on rare occasions, with 13% doing so often and 33% doing so sometimes or rarely. This difference in findings may be explained by the specified time frame given in the Eurostat data (the past three months), which implies a certain frequency of taking this action.

Regarding online tracking, a majority (75%) of Swiss Internet users claim to know that cookies can be used to trace people's movements on the Internet, but only a minority report to have taken actions to prevent online tracking in one form or another, e.g. by changing browser settings to prevent or limit cookies (37%) or by using anti-tracking software (21%; Eurostat 2022). This lack of action, in which Swiss Internet users are very similar to the EU-27 average, may be due to a difference between their declarative and their procedural data protection literacy in this respect (cf. Trepte et al. 2015). That is, although they may be aware of online tracking through cookies, they may not know *how* to prevent it.

The use of security software is relatively widespread (albeit declining) in Switzerland, with the majority of Swiss Internet and smartphone users (60% and 57%, respectively) having security software on their PC or smartphone, according to the most recent survey data available (Bundesamt für Statistik 2021b).

In further studies, a systematic distinction should be made between different aspects of data protection literacy, such as between declarative and procedural knowledge, in order to (better) determine the effect (of the individual components) on Swiss people's WTS personal data (cf. Baruh et al. 2017, Wawra 2022, II. 2.).

7. Attitudes Towards Data Receiver

a. Attitudes Towards Governments

Overall, a majority of Swiss respondents (58.5%) express trust towards others.

The Swiss' attitude toward their government reflects this general tendency of trust toward others in Switzerland: a majority expressed trust in the government (66.3%) and the parliament (57.6%) in the EVS/WVS study (2021c). Similar high trust scores were found in another study (von Wyl et al. 2021) for 'government or health authorities': 68.7% of respondents expressed great trust in them. The same study found that this type of trust is positively related to the uptake of a COVID-tracing app, thus providing evidence for its positive effect on data disclosure. In contrast, political parties are trusted only by a small minority of Swiss (25.1%), according to the EVS/WVS data (2021c).

Findings on how much the Swiss trust their government with regard to the correct handling of personal data are somewhat inconsistent.[52] The results of one study suggest that Swiss people's trust in government institutions concerning the correct use of personal data exceeds their general trust in the government by 7.7%. 74% of respondents trust government institutions in this particular respect (Guirguis et al. 2021), compared to 66.3% of respondents that trust the government in general (EVS/WVS 2021c). Notably, Guirguis et al. (2021) also found that people who trust government institutions more have fewer concerns about disclosing personal information online, demonstrating the positive impact of this factor on data disclosure. In contrast, another survey (Oliver Wyman 2021a, b) found that only slightly more than half of the Swiss (52%) trust the government and government agencies in matters of personal data disclosure (however, the remaining 48% did not all distrust the government in this respect – in fact, 16% were indifferent). A third study (Frick 2022) found medium-high levels of trust among the Swiss (7.0 on a 10-point scale, whereby 1= no trust at all, 10 = very strong trust) towards government agencies regarding the handling of consumer data. Thus, although the findings vary to some extent, overall the Swiss tend to trust their government regarding the handling of personal data. Therefore, a majority of the Swiss might generally be willing to disclose data to their own government. However, this may not be the case in contexts of personal data disclosure where Swiss people's trust of the government regarding the handling of personal data is, for some reason, diminished. An example of this is the storage of health-related data in a biobank: when asked whether they would trust their government to keep their health-related data and samples in a biobank confidential and protected, the vast majority of Swiss respondents (71.0%) had low trust (Brall et al. 2022).

Data for Switzerland are still lacking on the questions of whether people trust foreign governments regarding the correct use of personal data, and whether the government or foreign governments contribute to people's distrust of the Internet (cf. CIGI-Ipsos 2019a, p. 117, 119, 2019c, p. 20, Ipsos 2019, p. 20). Only about a quarter (27%) of Swiss Internet users worry that the government may violate their privacy online (Latzer et al. 2021b). However, almost nine in ten Swiss respondents (89%) believe that governmental and commercial websites collect too much data overall (Statista 2018).

[52] Ipsos (2019, p. 20) does not provide any data for Switzerland in this regard.

The tendency of the Swiss to trust their government regarding the handling of personal data is also mirrored in their willingness to use e-government services. According to a recent survey (Deloitte 2022), a majority of the Swiss (61%) are prepared to use such services, and an even greater majority would be willing to at least occasionally use new e-government services (74%-88%, depending on the service).

Finally, a majority of Swiss people (63%) believe that the state is primarily responsible for ensuring data security and data protection (Guirguis et al. 2021).

b. Attitudes Towards Companies

Survey data are lacking regarding the question of how much trust the Swiss have in companies to do enough to protect their data (cf. CIGI-Ipsos 2019c, p. 283). One study on people's trust in different industries regarding the handling of consumer data (Frick 2022) shows that the Swiss tend to trust banks the most in this respect, followed by insurance companies, booking portals and e-mail providers. Online shops, comparison portals and smartphone manufacturers are distrusted slightly in this respect, followed by business networks, chat/messenger providers and search engines. Social-media platforms and dating portals are trusted the least. The fact that the Swiss tend to trust banks in data-related matters is confirmed by another study (Oliver Wyman 2021b, p. 3), which found that a majority of 61% trust banks with regard to the disclosure of personal data. Health insurance companies were trusted by more than two-thirds of respondents (69%), while car and household insurance companies were trusted by just over half (53%). This study is thus also in line with Frick's (2022) finding that the Swiss tend to trust insurance companies in data-related matters, although it should be noted that the high value for health insurance companies found by Oliver Wyman (2021b) might be due to the fact that they were grouped together in one category with hospitals and doctors (the latter of which were found to enjoy strong trust by a substantially larger proportion of respondents than health insurance companies in another study – see below). It also corroborates the finding that the Swiss tend to distrust online shops and tech companies such as *Google* (cf. Frick's (2022) finding regarding search engines) in data-related matters, both of which were found to be distrusted by a majority of 56% and trusted by only 24%. Furthermore, it was found that only a minority (41%-42%) trusts retailers, cell phone companies, and airline and travel companies.

Regarding the special case of health-related data and samples stored in a biobank (Brall et al. 2022), people in Switzerland have very little trust in companies to keep this type of data confidential and protected: all types of companies investigated received low levels of trust from at least 90% of respondents – including health insurance companies. However, they were trusted more than pharmaceutical companies, which, in turn, were trusted more than other Swiss private for-profit companies, followed by other global private for profit-companies. The finding that health insurance companies are trusted very little by Swiss residents in this particular context of data disclosure contrasts with the finding by Oliver Wyman (2021a, b), according to which a vast majority of Swiss have trust in them regarding personal data disclosure. As stated above, this may be due to the fact that in Oliver Wyman's study, they were grouped together with doctors and hospitals. An additional factor could be that the Swiss may feel less comfortable with health insurance companies having access to medical data and samples that they originally provided for research purposes, as opposed to data they provided to insurance companies themselves for reimbursement purposes, for example. The number one concern expressed by Swiss residents when hypothetically proving medical data and samples for research purposes is that someone may use their data to discriminate against them or their family (Brall et al. 2021). It is possible that most Swiss have a low level of trust towards health insurance companies regarding the handling of data stored in a biobank because

they fear that these data might be misused in the financial interest of the company (e.g. to identify high risk-patients and increase premiums).

In sum, a majority of Swiss respondents trust banks and insurance companies with regard to the disclosure of personal data in general, and there seems to be at least a tendency among the Swiss to trust booking portals and e-mail providers with regard to the handling of consumer data. This is likely to have a positive effect on Swiss people's WTS data with these types of companies. However, a majority of Swiss respondents are skeptical about online shops and tech companies in terms of disclosing personal data, and there is a tendency to distrust comparison portals, smartphone manufacturers, business networks, chat/messenger providers, search engines, and, in particular, social media platforms and dating portals regarding the handling of consumer data. Moreover, the vast majority of Swiss people distrust companies to keep their health-related data and samples stored in a biobank confidential and protected, and almost half of Swiss Internet users are concerned that companies violate their privacy on the Internet. A basic negative impact on most Swiss people's WTS data is therefore to be expected in such data disclosure situations.

There is a lack of data on the extent to which different types of companies contribute to Swiss people's distrust of the Internet (cf. CIGI-Ipsos 2019c, p. 20). A recent survey found that around half (47%) of Swiss Internet users are rather or strongly concerned about online privacy violations by companies, while only about a quarter (27%) have such concerns about the government (Latzer et al. 2021b). The Swiss thus trust companies considerably less than the government with regard to their online privacy.

The findings from several surveys further confirm the trend that people in Switzerland tend to have more trust in their government than in various types of companies when it comes to data-related matters. One study (Frick 2022) found that, with the exception of banks (which were trusted to virtually the same extent), the Swiss trust government agencies more than all types of companies examined regarding the handling of consumer data. Another study (Oliver Wyman 2021a, b) found that a greater or about equal proportion of Swiss trust the government and government agencies regarding matters of personal data disclosure than most of the companies examined, with the exception of banks and health insurance companies, although, as stated above, the results regarding the latter are somewhat uncertain as they were grouped together with doctors and hospitals in one category. A third study (Brall et al. 2022) found that people in Switzerland also trust their government considerably more than various types of companies with regard to the confidentiality and protection of their health-related data and samples stored in a biobank, although both the government and companies are only trusted by a minority in this respect (29.1% vs. max. 8.4%). Allowing companies in particular to access such data may thus negatively affect Swiss residents' willingness to provide their health-related information and samples to a biobank. Moreover, a clear majority (63%) of Swiss see the government and not privately-owned companies as the main actor for ensuring data security and protection (Guirguis et al. 2021).

The Swiss people's distrust of companies is also reflected in the fact that a large majority (>80%) want various e-government services to be provided by a government agency rather than private companies (Deloitte 2022). This may have been the reason for the failure of the introduction of an E-ID failed in 2021, which the Swiss government had planned to outsource to private actors (Deloitte 2022). This is a concrete example of how a lack of trust in the data recipient can lead people to oppose the disclosure of data (in this case, by voting against the introduction of the E-ID). New e-government services are thus more likely to be accepted by the Swiss if they are provided by a government agency.

8. Communication on Data Use

As of yet, there are no data available for Switzerland concerning the questions of whether people would be more comfortable disclosing their data to companies that communicate transparently what the data will be used for (Ipsos 2019, p. 14) and whether they would be most willing to share their data with companies or government institutions that clearly communicate potential risks (cf. Ipsos 2019, p. 17). However, there are some findings on Swiss people's preferences for communication on data use regarding health-related data and samples collected for research purposes: a majority of Swiss people (64%) believe they would be more likely to share their anonymized health data if they knew the exact research purpose for which they were being collected (Pletscher et al. 2022). Moreover, in the hypothetical scenario that they would provide health-related data and samples for a biobank (Brall et al. 2022), a majority of Swiss residents (68.4%) seem to want at least some information about the research projects for which their health-related data and samples would be used before giving permission to use them. Most respondents (39.0%) stated that they would like to be asked again for permission to use their data and samples for each new project, and more than a quarter (29.4%) stated that this would depend on the type of project being considered. Thus, transparent communication about the purpose of data collection may increase people's likeliness to share their health-related data and samples in the Swiss context.

Moreover, as noted in sections VI. and XI. 4., altruistic motives seem to play an important role for the Swiss regarding their decision to share health-related data. If it is clearly communicated how their health-related data may benefit other people or society as a whole, this could positively influence the data disclosure behavior of the Swiss in this context.

XII. Conclusion and Outlook

This study captures the narrower cultural context of data disclosure in Switzerland (cf. Wawra 2022, II. 8., III.). It provides an overview of Swiss respondents' perceptions of informational privacy, data protection, and data control issues pertaining to personal data disclosure from a macro perspective. It reflects the cultural preconditions of information governance in Switzerland by shedding light on the prevailing attitudes, assumptions, views, and reported behaviors of Swiss respondents that can influence their WTS personal data.

First of all, this study has shown where Switzerland stands in a global comparison with regard to digitalization. In addition, it has above all provided statistical insights on

- the value Swiss respondents place on their informational privacy in different contexts
- what types of data are defined as sensitive personal data according to Swiss law and which data may be considered more or less private or sensitive by Swiss respondents
- the benefits which people in Switzerland associate with data disclosure in certain contexts
- the value Swiss people place on data security
- reported behavior that follows from perceived privacy concerns and risks
- Swiss people's awareness and evaluation of data protection and privacy rules
- Swiss people's general levels of trust and their trust in their government and different types of companies
- whether certain communicative content would make Swiss people feel more at ease when asked to share personal data.

The less basic WTS data the surveys indicate, the more effort organizations requesting personal data potentially have to put into convincing people to disclose their data anyway. This can be achieved through communication and business or political strategies aimed primarily at increasing people's trust in the data recipient and reducing privacy concerns. It should also be noted that previous research on data disclosure suggests that the degree of privacy or sensitivity of the data, the granting or denial of anonymity, and whether or not data are requested in line with an organization's mission and responsibilities are the factors that have the greatest influence on people's data disclosure decisions (see above; cf. Ackermann et al. 2021).

This study was able to reveal general trends in Swiss respondents' views on issues closely related to data disclosure decisions. It was also able to show the general direction of influence of most of the cited parameters on people's WTS data. In actual data disclosure scenarios, the different variables can have a greater or lesser (to no) impact on people's final decision to share personal data. It must also be considered that depending on the situation in which personal data are requested, the decision to disclose may not always be made through conscious deliberation, and actual behavior may differ from reported behavior (cf. e.g. Kim et al. 2015, Ackermann et al. 2021, Wawra 2022, II. 9.). The complex interplay of the many variables that can influence the WTS data – including not only cultural-contextual, but also socio-demographic factors and personality traits – needs to be approached on a micro level and therefore further explored in concrete situational contexts.

XIII. References

Ackermann, K. A., Burkhalter, L., Mildenberger, T., Frey, M., and Bearth, A. (2021). Willingness to Share Data: Contextual Determinants of Consumers' Decisions to Share Private Data with Companies. Journal of Consumer Behaviour 2021. 1-12. DOI: 10.1002/cb.2012 (last access: 02/07/2022).

Baruh, L., Secinti, E., and Cemalcilar, Z. (2017). Online Privacy Concerns and Privacy Management: A Meta-Analytical Review: Privacy Concerns Meta-Analysis. Journal of Communication 67(1). 26-53. DOI: 10.1111/jcom.12276 (last access: 02/07/2022).

Brall, C., Berlin, C., Zwahlen, M., Ormond, K. E., Egger, M., and Vayena, E. (2021). Public Willingness to Participate in Personalized Health Research and Biobanking: A Large-Scale Swiss Survey. PloS ONE 16(4): 1-17. DOI: 10.1371/journal.pone.0249141 (last access: 11/04/2022).

Brall, C., Berlin, C., Zwahlen, M., Vayena, E., Egger, M., and Ormond, K. E. (2022). Public Preferences towards Data Management and Governance in Swiss Biobanks: Results from a Nationwide Survey. BMJ Open 12(8). 1-10. DOI: 10.1136/bmjopen-2022-060844 (last access: 11/04/2022).

Bruce, G. (2021). Convenience vs. Security: What Do Consumers Prioritize When Choosing Mobile Apps? YouGovAmerica May 22. https://today.yougov.com/topics/technology/articles-reports/2021/05/22/convenience-vs-security-what-do-consumers-prioriti (last access: 12/06/2021).

Brüesch, C., Fischer, D., and Lang, A. (2020). Bevölkerungsumfrage in der Schweiz, Deutschland und Österreich zur nationalen Contact Tracing-App: Eine Studie des Instituts für Verwaltungs-Management der ZHAW. ZHAW School of Management and Law. https://www.zhaw.ch/storage/hochschule/medien/news/2020/201119-zhaw-studie-corona-app-umfrage.pdf (last access: 11/11/2022).

Buchwald, A., Letner, A., Urbach, N., and von Entreß-Fürsteneck, M. (2017). Towards Explaining the Willingness to Disclose Personal Self-Tracking Data to Service Providers. 2017 Twenty-Fifth European Conference on Information Systems (ECIS). 1-11. https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/682/wi-682.pdf (last access: 02/07/2022).

Bundesamt für Statistik (2017). Omnibus-Erhebung 2017: Erhebung zur Internetnutzung. https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/erhebungen/omn2017.assetdetail.2348769.html (last access: 02/09/2023).

Bundesamt für Statistik (2018). Erhebung zur Internetnutzung 2017. Digitale Kompetenzen, Schutz der Privatsphäre und Online-Bildung: die Schweiz im internationalen Vergleich. https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/erhebungen/omn2017.assetdetail.5306733.html (last access: 11/03/2022).

Bundesamt für Statistik (2019). Omnibus-Erhebung 2019: Erhebung zur Internetnutzung. https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/erhebungen/omn2019.assetdetail.8126219.html (last access: 02/09/2023).

Bundesamt für Statistik (2021a). Erhebung zur Internetnutzung in der Schweiz: Omnibus IKT 2021. Fragebogen und Codebook. Neuchâtel: Bundesamt für Statistik. https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/erhebungen/omn2021.assetdetail.20125566.html (last access: 11/18/2022).

Bundesamt für Statistik (2021b). Pandemie treibt Nutzung von E-Government-Diensten voran. Neuchâtel: Bundesamt für Statistik. https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/erhebungen/omn2021.assetdetail.20004303.html (last access: 11/21/2022).

Bundesamt für Statistik (2022). Omnibus-Erhebung 2021: Erhebung zur Internetnutzung. https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/erhebungen/omn2021.assetdetail.22284438.html (last access: 02/08/2023).

CIGI-Ipsos (2019a). CIGI-Ipsos Global Survey on Internet Security and Trust. Parts I & II: Internet Security, Online Privacy & Trust. Centre for International Governance Innovation. www.cigionline.org/internet-survey-2019 (last access: 12/15/2021).

CIGI-Ipsos (2019b). CIGI-Ipsos Global Survey Internet Security & Trust. Part 6: Cross-Border Data Flows. Centre for International Governance Innovation. www.cigionline.org/internet-survey-2019 (last access: 12/15/2021).

CIGI-Ipsos (2019c). CIGI-Ipsos Global Survey on Internet Security & Trust. Detailed Results Tables. www.cigionline.org/internet-survey-2019 (last access: 12/15/2021).

Cisco (2021). Consumer Privacy Survey. Building Consumer Confidence Through Transparency and Control. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf (last access: 12/03/2021).

Deloitte (2022). Die Deloitte Studie 2021 zur digitalen Verwaltung in der Schweiz: Die Treiber und Hürden von E-Government-Diensten. https://www2.deloitte.com/ch/de/pages/public-sector/articles/digital-government-study.html (last access: 11/25/2022).

DLA Piper (2021). Data Protection Laws of the World: Switzerland – Definitions. https://www.dlapiperdataprotection.com/index.html?t=definitions&c=CH (last access: 05/20/2022).

EVS/WVS (2021a). World Values Survey Wave 7 (2017-2020). Questionnaire : WVS-7 Master Questionnaire 2017-2020. https://www.worldvaluessurvey.org/WVSDocumentationWV7.jsp (last access : 12/15/2021).

EVS/WVS (2021b). European Values Study and World Values Survey: Joint EVS/WVS 2017-2021 Dataset (Joint EVS/WVS). JD Systems Institute & WVSA. Dataset Version 1.1.0. https://www.worldvaluessurvey.org/WVSEVSjoint2017.jsp (last access: 12/15/2021).

EVS/WVS (2021c). European Values Study and World Values Survey: Joint EVS/WVS 2017-2020 Data-Set (version 2.0.0). Documentation: Frequency Tables. WVS/EVS Joint v2.0 Results by Country. https://www.worldvaluessurvey.org/WVSDocumentationWV7.jsp (last access: 12/15/2021).

Eurostat (2021). ICT Usage in Households and by Individuals (isoc_i): National Reference Metadata in Single Integrated Metadata Structure (SIMS). https://ec.europa.eu/eurostat/cache/metadata/EN/isoc_i_simsih_ch.htm (last access: 09/02/2023).

Eurostat (2022). Digital Economy and Society: Comprehensive Database. Statistics on Households and Individuals: Access database. (version 25 March 2022). https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/comprehensive-database (last access: 11/18/2022).

Federal Statistical Office (2022). Languages. https://www.bfs.admin.ch/bfs/en/home/statistics/population/languages-religions/languages.html (last access: 02/08/2023).

Frick, J. (2022). Comparis-Datenvertrauensstudie 2022. comparis.ch. https://www.comparis.ch/telecom/zuhause/internet-sicherheit/daten-vertrauen-studie (last access: 11/30/2022).

Fukuta, Y., Murata, K., Adams, A. and Orito, Y. (2017). Personal Data Sensitivity in Japan: An Exploratory Study. ORBIT Journal 1(2). DOI: 10.29297/orbit.v1i2.40. https://www.researchgate.net/publication/317413763_Personal_Data_Sensitivity_in_Japan_An_Exploratory_Study (last access: 01/08/2022).

Geber, S., and Friemel, T. N. (2021). A Typology-Based Approach to Tracing-App Adoption During the COVID-19 Pandemic: the Case of the SwissCovid App. Journal of Quantitative Description 1. 1-28. DOI: https://doi.org/10.51685/jqd.2021.007 (last access: 11/25/2022).

GfK (2017). Willingness to Share Personal Data in Exchange for Benefits or Rewards. https://cdn2.hubspot.net/hubfs/2405078/cms-pdfs/fileadmin/user_upload/country_one_pager/nl/images/global-gfk_onderzoek_-_delen_van_persoonlijke_data.pdf (last access: 01/18/2022).

Guirguis, K., Pleger L. E., Dietrich, S., Mertes, A. and 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). 16-30. DOI: https://doi.org/10.5334/ssas.153 (last access: 01/10/22)

Hoffmann, D., Novak, T., and Peralta, M. (1999). Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web. The Information Society 15(2). 129-139. DOI: 10.1080/019722499128583 (last access: 01/28/2022).

Howe, S. (2022). Cultural Influences on Personal Data Disclosure Decisions – German Perspectives. *University of Passau Institute for Law of the Digital Society Research Paper Series No. 22-14.* https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/ (last access: 09/10/2022).

IMD (2021). IMD World Digital Competitiveness Ranking 2021. https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/ (last access: 12/15/2021).

Ipsos (2019). Global Citizens & Data Privacy: An Ipsos-World Economic Forum Project. https://www.ipsos.com/sites/default/files/ct/news/documents/2019-01/ipsos-wef_-_global_consumer_views_on_data_privacy_-_2019-01-25-final.pptx_lecture_seule_0.pdf?mod=article_inline (last access: 12/15/2021).

Jarchow, Thomas, Beat Estermann. (2015). Big Data: Chancen, Risiken und Handlungsbedarf des Bundes. Ergebnisse einer Studie im Auftrag des Bundesamts für Kommunikation. https://www.egovernment.ch/files/2614/5078/6178/BFH_Big-Data-Studie_v1-0-3.pdf (last access: 05/01/2022).

Kessel, L. (2022). Cultural Influences on Personal Data Disclosure Decisions: US-American Perspectives. University of Passau Institute for Law of the Digital Society Research Paper Series 22(4). 1-29. https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4068964 (last access: 08/11/2022).

Kim, M., Ly, K., and Soman, D. (2015). A Behavioural Lens on Consumer Privacy. Behavioural Economics in Action Research Re-port Series. Toronto: Rotman School of Management, University of Toronto. https://inside.rotman.utoronto.ca/behaviouraleconomicsinaction/files/2013/09/ConsumerPrivacy-BEAR-2015-Final.pdf (last access: 02/07/2022).

Latzer, M., Büchi, M., Just, N. and Festic, N. (2015). Vertrauen und Sorgen bei der Internet-Nutzung in der Schweiz 2015. Summary Report from the World Internet Project – Switzerland 2015. Zürich: Universität Zürich. https://www.mediachange.ch/media/pdf/publications/Vertrauen_Sorgen_2015.pdf (last access: 11/15/2022).

Latzer, M., Büchi, M., and Festic, N. (2019). Vertrauen und Sorgen bei der Internetnutzung in der Schweiz 2019. Summary Report from the World Internet Project – Switzerland 2019. Zürich: Universität Zürich. https://mediachange.ch/media//pdf/publications/Vertrauen_Sorgen_2019.pdf (last access: 11/15/2022).

Latzer, M., Büchi, M., and Festic, N. (2020). Internet Use in Switzerland 2011-2019: Trends, Attitudes and Effects. Summary Report from the World Internet Project – Switzerland. University of Zurich. http://mediachange.ch/research/wip-ch-2019 (last access: 03/09/2023).

Latzer, M., Büchi, M., Kappeler, K., and Festic, N. (2021a). Internet und Politik in der Schweiz 2021. Summary Report from the World Internet Project – Switzerland 2021. Zürich: Universität Zürich. https://mediachange.ch/media//pdf/publications/Internet_und_Politik_2021.pdf (last access: 10/21/2022).

Latzer, M., Büchi, M., Kappeler, K., Festic, N. (2021b). Vertrauen und Sorgen bei der Internetnutzung in der Schweiz 2021. Summary Report from the World Internet Project – Switzerland 2021. Zürich: Universität Zürich. https://mediachange.ch/media//pdf/publications/Vertrauen_Sorgen_2021.pdf (last access: 10/21/2022).

Lu, Y., Tan, B., and Hui, K.-L. (2004). Inducing Consumers to Disclose Personal Information to Internet Businesses with Social Adjustment Benefits. Proceedings of the Twenty-Fifth International Conference on Information Systems. Washington DC, USA. http://repository.ust.hk/ir/Record/1783.1-57524 (last access: 02/16/2022).

Markos, E., Milne, G., Peltier, J. (2017). Information Sensitivity and Willingness to Provide Continua: A Comparative Privacy Study of the United States and Brazil. https://doi.org/10.1509/jppm.15.159 (last access: 11/24/2021).

Oliver Wyman (2021a). Switzerland's Digital DNA 2021. https://www.oliverwyman.ch/unsere-expertise/publikationen/2021/oct/switzerland-digital-dna-2021.html (last access: 02/08/2023).

Oliver Wyman (2021b). Switzerland's Digital DNA 2021 [figures]. https://www.oliverwyman.ch/content/dam/oliver-wyman/europe/switzerland/Pressemitteilungen/20160711_PM_Automotive%20Manager_CH.pdf/Oliver_Wyman_Switzerlands_digital_DNA_2021_Grafiken.pdf (last access: 03/09/2023).

Pletscher, F., Mändli Lerch, K., and Glinz, D. (2022). Willingness to Share Anonymised Routinely Collected Clinical Health Data in Switzerland: A Cross-Sectional Survey. Swiss Medical Weekly 152(2324). 1-10. https://doi.org/10.4414/SMW.2022.w30182 (last access: 01/12/2022).

PwC (2021a). Hopes and Fears 2021. Mainland China Report. https://www.pwccn.com/en/consulting/people-and-organisation/hopes-fears-2021-china-report-apr2021.pdf (last access: 12/06/2021).

PwC (2021b). Hopes and Fears 2021: Japan. https://www.pwc.com/jp/ja/knowledge/thought-leadership/2021/assets/pdf/hopes-and-fears-jp2021.pdf (last access: 01/08/2022).

Reinecke, P. (2020). Country Specific Info HH Switzerland. (version 1.3). Eurostat. https://circabc.europa.eu/ui/group/4f80b004-7f0a-4e5a-ba91-a7bb40cc0304/library/8ab148bc-b3c3-4be2-a053-43a04b16413e/details (last access: 09/02/2023).

Roeber, B., Rehse, O., Knorrek, R., and Thomsen, B. (2015). Personal Data: How Context Shapes Consumers' Data Sharing with Organizations from Various Sectors. Electronic Markets 25(2). 95-108. DOI: 10.1007/s12525-015-0183-0 (last access: 01/28/2022).

Rössler, B. (2001). Der Wert des Privaten. Frankfurt am Main: Suhrkamp.

Statista (2018). Sind Sie der Meinung, dass Staatliche und Kommerzielle Websites zu Viele Daten Sammeln? https://de.statista.com/statistik/daten/studie/505521/umfrage/umfrage-zur-datensammlung-durch-websites-in-der-schweiz/ (last access: 05/01/2022).

Thir, V., and Wawra, D. (2023). Cultural Influences on Personal Data Disclosure Decisions – Ghanaian Perspectives. University of Passau Institute for Law of the Digital Society Research Paper Series 23(4). 1-25. https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/ (last access: 20/06/2023).

Trepte, S., Masur, P. (2016). Cultural Differences in Social Media Use, Privacy, and Self-Disclosure. http://opus.uni-hohenheim.de/volltexte/2016/1218/pdf/Trepte_Masur_ResearchReport.pdf (last access: 12/07/2021).

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., and Lind, F. (2015). Do People Know about Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In S. Gutwirth, R. Leenes, and P. de Hert. Reforming European Data Protection Law. Dordrecht: Springer. 333-365. DOI: 10.1007/978-94-017-9385-8_14 (last access: 12/14/2022).

Unisys (2021). Unisys Security Index™: Global Report. https://www.unisys.com/unisys-security-index/ (last access: 01/08/2022).

Von Wyl, V., Höglinger M., Sieber, C., Kaufmann, M., Moser, A., Serra-Burriel, M., Ballouz, T., Menges, D., Frei, A., and Puhan, M. A. (2021). Drivers of Acceptance of COVID-19 Proximity Tracing Apps in Switzerland: Panel Survey Analysis. JMIR Public Health Surveillance 7(1). 1-15. https://doi.org/10.2196/25701 (last access: 11/25/2022).

Wawra, D. (2022). The Cultural Context of Personal Data Disclosure Decisions. University of Passau Institute for Law of the Digital Society Research Paper Series 22(2). 1-19. https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/ (last access: 03/03/2022).

Wawra, D. et al. (2022). Cultural Influences on Personal Data Disclosure Decisions – Japanese Perspectives. University of Passau Institute for Law of the Digital Society Research Paper Series 22(10). 1-24. https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/ (last access: 09/10/2022).

Wawra, D. (2023). Data Sensitivity and Data Protection Literacy in Cross-Cultural Comparison. In M. Hennemann, K. von Lewinski, D. Wawra, and T. Widjaja. Data Disclosure: Global Developments and Perspectives. Berlin: De Gruyter. 169-194. DOI: https://doi.org/10.1515/9783111010601 (last access: 04/24/2023).

Westin, A. (2003). Social and Political Dimensions of Privacy: Social and Political. Journal of Social Issues 59(2). 431-453. https://doi.org/10.1111/1540-4560.00072 (last access: 02/14/2022).

XIV. Appendix 1

Appendix 1. List of included surveys and survey details[53]

Study	Overview	Sample size	Demographics
Brall et al. (2021). Public Willingness to Participate in Personalized Health Research and Biobanking: A Large-Scale Swiss Survey Brall et al. (2022). Public Preferences towards Data Management and Governance in Swiss Biobanks: Results from a Nationwide Survey	A nationwide survey conducted in fall 2019/winter 2020 on "the Swiss public's willingness, attitudes, and concerns regarding personalized health research participation by providing health information and biological material" (Brall et al. 2021, abstract) and on their "preferences […] regarding data management and governance when hypothetically providing data or samples for personalized health research" (Brall et al. 2022, p. 1).	N = 5086 (total sample of complete responses) N = 5025 (subsample for the data presented in Fig. 24) N = 2726 (subsample of participants hypothetically willing to participate in a research project using their health data and/or biological samples)	Age of respondents: 18-79 years Swiss residents, mostly Swiss nationals (76.0%), mostly from a German-speaking region (70.8%, as opposed to 24.5% for French-speaking regions and 4.7% for Italian-speaking regions), mostly from urban areas (61.0%). Assuming that respondents' regional origin corresponded to their main language, German speakers were thus slightly oversampled, whereas French and Italian speakers were undersampled (cf. Federal Statistical Office 2022). "Respondent age ranged from 18 to 79 years, with fairly uniform spread across sex and age categories between 25 and 64 years." (Brall et al. 2022, abstract)
Brüesch et al. (2020). Bevölkerungsumfrage in der Schweiz, Deutschland und Österreich zur nationalen Contact Tracing-App: Eine Studie des Instituts für	A study conducted in September 2020 examining the reasons for (not) installing the national COVID-19 contact tracing app in Germany, Austria and Switzerland as well as factors influencing people's decision in this	N = 1024 (Swiss sample)	Age of respondents: >18 Comparable to the Swiss population in terms of gender ratio (49.1% male / 50.9% female) and regional distribution (Lake Geneva region: 18.9%, Espace Mittelland: 22.1%, Northwestern Switzerland: 13.6%, Canton of Zürich:

[53] Basic information on the EVS/WVS studies in the table was copied from Kessel (2022) and supplemented with specific information on respondents from Switzerland.

Study	Overview	Sample size	Demographics
Verwaltungs-Management der ZHAW	respect (such as trust or the perceived benefit of using the app).		17.7%, Eastern Switzerland: 13.9%, Central Switzerland: 9.5%, Ticino: 4.3%). Non-representative in terms of age (the age groups 40-64 and 65-79 years were over-represented, the age group 80+ was under-represented).
Bundesamt für Statistik (2018). Erhebung zur Internetnutzung 2017. Digitale Kompetenzen, Schutz der Privatsphäre und Online-Bildung: die Schweiz im internationalen Vergleich	A survey on Internet access and Internet use in the Swiss population conducted in 2017 ("Omnibus IKT 2017"), based on a European model questionnaire to enable comparison with Switzerland's neighboring countries (cf. Bundesamt für Statistik 2017).	N = 2673[54]	Age of respondents: 16-74 years Random sample (cf. Bundesamt für Statistik 2017).
Bundesamt für Statistik (2021a). Erhebung zur Internetnutzung in der Schweiz: Omnibus IKT 2021. Fragebogen und Codebook Bundesamt für Statistik (2021b). Pandemie treibt Nutzung von E-Government-Diensten voran	A survey on Internet access and Internet use in the Swiss population conducted in 2021 ("Omnibus IKT 2021"), based on a European model questionnaire to enable comparison with Switzerland's neighboring countries (cf. Bundesamt für Statistik 2022). In Bundesamt für Statistik (2021b), the results are sometimes compared to those of the "Omnibus IKT 2019 survey", an equivalent survey	N_{2019} = 3004[55] N_{2021} = 3137 $N_{\text{Swiss Internet users (last 3 months) 2019}}$ = 2801 $N_{\text{Swiss Internet users (last 3 months) 2021}}$ = 2997 $N_{\text{Swiss smartphone users 2019}}$ = 2456	Age of respondents: 15-88 years Random sample (cf. Bundesamt für Statistik 2022).

[54] The total sample was about 3000 and also included respondents aged 15 and 75-88 years. The subsample on which this report is based was also provided for the Eurostat (2022) dataset, for which the sample size N = 2673 is given in Reinecke (2020).

[55] Information on sample sizes was obtained through personal communication.

Study	Overview	Sample size	Demographics
	conducted in 2019 (cf. Bundesamt für Statistik 2019).	$N_{Swiss\ smartphone\ users\ 2021}$ = 2944	
Deloitte (2022). Die Deloitte Studie 2021 zur digitalen Verwaltung in der Schweiz: Die Treiber und Hürden von E-Government-Diensten	A survey by accounting firm *Deloitte* on Swiss people's views and preferences regarding e-government services, conducted in September 2021. The focus was on "citizens' global trust in public authorities' and administrations' current and future capability to offer digital services" (Deloitte 2022, p. 26).[56]	N > 1000	Age of respondents: 18-81 years The sample was relatively evenly distributed across all 5 five age groups (<30, 30-39, 40-49, 50-59, >60), and involved respondents from both urban (67%) and rural areas (33%), as well as from German-, French- and Italian- speaking parts of Switzerland (no information regarding exact distribution). 235 respondents were public service employees, since the survey also aimed at examining "views within authorities and administrations regarding technological obstacles and challenges associated with digital transformation" (Deloitte 2022, p. 26).[57]
European Values Study and World Values Survey (EVS/WVS 2021a, b, c)	The cooperation between the European and the World Values Survey investigates values that are most important to people from different national backgrounds, including values that relate to attitudes towards data disclosure.	N = 3174	Age of respondents: 18+ "random probability representative samples of the adult population" (EVS/WVS 2021).
Eurostat (2022)	Data for Switzerland were gathered by the Swiss Federal Statistical Office, through the "Omnibus IKT 2021" survey described above	$N_{Switzerland\ 2019}$ = 2708[58]	Age of respondents: 16-74 years

[56] Own translation.

[57] Own translation.

[58] See the documentation in Reinecke (2020).

Study	Overview	Sample size	Demographics
	(Bundesamt für Statistik 2021a, b), and the "Omnibus IKT 2019" survey (Bundesamt für Statistik 2019), though the sample for the Eurostat statistics does not include respondents over 74 and under 16.	$N_{\text{Swiss Internet users (last 12 months) 2019}} \approx 2627$[59] $N_{\text{Switzerland 2021}} = 2815$[60] $N_{\text{Swiss Internet users (last 3 months) 2021}} \approx 2759$[61]	Random sample (cf. Bundesamt für Statistik 2019, 2022).
Frick (2022). Comparis-Datenvertrauensstudie 2022	A survey by online comparison service *comparis.ch* on Swiss people's trust regarding various matters related to data disclosure, conducted in September 2022.	N = 1014	Age of respondents: at least 15-74 years (no exact details given) Conducted in all regions of Switzerland.
Guirguis et al. (2021). Datenschutz in der Schweiz: Eine Quantitative Analyse der Gesellschaftlichen Bedenken und Erwartungen an den Staat	An online survey about Swiss people's concerns regarding data protection and their expectations of the state in this respect, conducted in July 2019.	N = 500	Age of respondents: 18+ Representative of the Swiss population regarding age and sex. All respondents were from German-speaking Switzerland.
Jarchow and Estermann (2015). Big Data: Chancen, Risiken und Handlungsbedarf des Bundes. Ergebnisse einer Studie im	A study by the Bern University of Applied Sciences, commissioned by the Swiss Federal Office of Communications, which aims at "identifying the opportunities and risks afforded by 'big data' and at highlighting need for action by	N = 821	Age of respondents: exact range not given, youngest age group: ≤ 30, oldest age group: > 60 Target population: "people in Switzerland who deal with the issue of 'big data' in one way or another" (Jarchow and Estermann 2015, p. 28)[63]

[59] Own calculation (97% of total sample).

[60] See the documentation in Eurostat (2021).

[61] Own calculation (98% of total sample).

[63] Own translation.

Study	Overview	Sample size	Demographics
Auftrag des Bundesamts für Kommunikation	the Swiss Confederation in this respect" (Jarchow and Estermann 2015, p. 3).[62]		Non-representative since the demographics of the target population were unknown. Respondents were mostly male (84%) and half of them were aged 50+, with 50–59-year-olds being the largest age group in the sample (37%). The second largest age group was 40–49-year-olds (32%). 81% of respondents were German-speaking, 18% were French-speaking and 1%[64] were Italian-speaking. Thus, German-speaking respondents were over-represented (actual proportion in the permanent resident population of Switzerland: 73%) whereas French-speaking and Italian speaking respondents were under-represented (actual proportion: 23% and 6%, respectively; cf. Jarchow and Estermann 2015, p. 30).
Latzer et al. (2015). Vertrauen und Sorgen bei der Internet-Nutzung in der Schweiz 2015	A telephone survey on the Swiss population's use of and attitudes towards the Internet using the internationally standardized World Internet Project (WIP) questionnaire and additional country-specific questions, conducted in May/June 2015.	N = 981 (subsample of Internet users)	Age of respondents: 14-84 years "The total sample of 1121 people is representative of the Swiss population between 14 and 84 years by age, gender, employment status, and three language regions (German-, French- and

[62] Own translation.

[64] The proportion of Italian-speaking respondents was calculated based on what respondents who provided their contact details at the end of the survey stated to be their preferred language of communication.

Study	Overview	Sample size	Demographics
			Italian-speaking parts of Switzerland)" (Latzer et al. 2015, p. 26).[65]
Latzer et al. (2019). Vertrauen und Sorgen bei der Internetnutzung in der Schweiz 2019	A telephone survey on the Swiss population's use of and attitudes towards the Internet using the internationally standardized World Internet Project (WIP) questionnaire and additional country-specific questions, conducted in May/June/July 2019.	N = 1035 (subsample of Internet users)	Age of respondents: 14+ "The total sample of 1122 people is representative of the Swiss population over 14 years by age, gender, employment status, and the three language regions (German-, French- and Italian-speaking parts of Switzerland)" (Latzer et al. 2019, p. 33).[66]
Latzer et al. (2021a). Internet und Politik in der Schweiz 2021 Latzer et al. (2021b). Vertrauen und Sorgen bei der Internetnutzung in der Schweiz 2021	A telephone survey on the Swiss population's use of and attitudes towards the Internet using the internationally standardized World Internet Project (WIP) questionnaire and additional country-specific questions, conducted in May/June 2021.	N = 1069 (subsample of Internet users)	Age of respondents: 14+ "The total sample of 1120 people is representative of the Swiss population over 14 years by age, gender, employment status, and the three language regions (German-, French- and Italian-speaking parts of Switzerland)" (Latzer et al. 2021a, p. 21).[67]
Oliver Wyman (2021a). Switzerland's Digital DNA 2021	A survey on various issues related to digitalization conducted in Switzerland by international strategy consulting firm *Oliver Wyman*.	N = 1609[68]	Age of respondents: 14+ Representative in terms of age, gender, and two language regions of the Swiss population; 75% of respondents were from German-speaking parts

[65] Translation adapted from Latzer et al. (2020, p. 34).

[66] Translation adapted from Latzer et al. (2020, p. 34).

[67] Translation adapted from Latzer et al. (2020, p. 34).

[68] Information on sample size was obtained through personal communication.

Study	Overview	Sample size	Demographics
Oliver Wyman (2021b). Switzerland's Digital DNA 2021 [figures]			of Switzerland, 25% from French-speaking parts of Switzerland.[69]
Pletscher et al. (2022). Willingness to Share Anonymised Routinely Collected Clinical Health Data in Switzerland: A Cross-Sectional Survey	A survey examining Swiss people's views on sharing anonymized health data for research purposes, with a focus "on the re-use (secondary use) of hospital-derived health data in anonymised form" (Pletscher et al. 2022, summary), conducted in fall 2020.	N = 1006	Age of respondents: 18+ "The general population interviewed was representative of the French and German-speaking Swiss population, that is, structurally identical or with a very similar distribution of age groups, gender and regional distribution" (Pletscher et al., 2022 p. 4).
Statista (2018). Sind Sie der Meinung, dass Staatliche und Kommerzielle Websites zu Viele Daten Sammeln?	Panel survey on data collection by websites in Switzerland.	N = 1026 (for 2018)	Age of respondents: 15-74 Participants came from German- and French speaking parts of Switzerland (exact distribution unknown).
Von Wyl et al. (2021). Drivers of Acceptance of COVID-19 Proximity Tracing Apps in Switzerland: Panel Survey Analysis	A study on "the coverage of the SwissCovid app and the reasons for its nonuse in Switzerland during a period of increasing incidence of COVID-19 cases" (von Wyl et al. 2021, abstract). Data was collected "via a nationwide online panel survey" in fall 2020 (von Wyl et al. 2021, abstract).	N = 712 (for the results reported here)	This subsample was a "randomly selected split-sample, including 47.1% (712/1511) of the full study population" (von Wyl et al. 2021, p. 6). The total sample was "stratified based on age, gender, and language region, […] in order to make the sample representative of the Swiss population" (von Wyl et al. 2021, p. 2). The language regions considered included German- French-, and Italian-speaking parts of Switzerland.

[69] Information on sample demographics was obtained through personal communication.