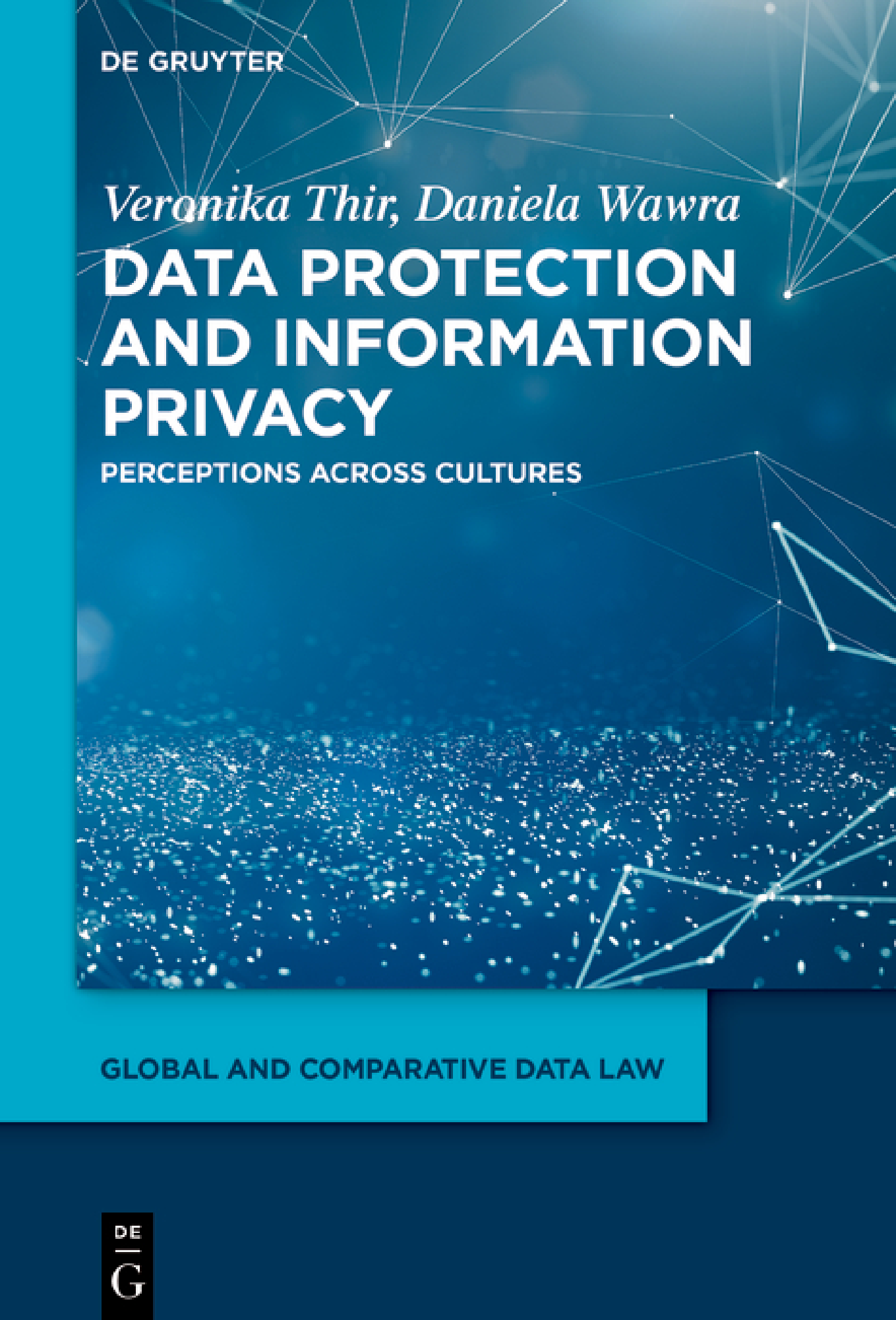
DE GRUYTER
Veronika Thir, Daniela Wawra
DATA PROTECTION AND INFORMATION PRIVACY
PERCEPTIONS ACROSS CULTURES
GLOBAL AND COMPARATIVE DATA LAW
DE
G

Veronika Thir, Daniela Wawra

Data Protection and Information Privacy

Global and Comparative Data Law

Edited by
Moritz Hennemann
Lea Katharina Kumkar
Linda Kuschel
Björn Steinrötter

Volume 5

Veronika Thir, Daniela Wawra

Data Protection and Information Privacy

Perceptions Across Cultures

DE GRUYTER

This research project and the publication of this volume is funded by the Bavarian Research Institute for Digital Transformation (bidt), an institute of the Bavarian Academy of Sciences and Humanities. The authors are responsible for the content of this publication.

We acknowledge support by the Open Access Publication Fund of University Library Passau.

ISBN 978-3-11-145812-0
e-ISBN (PDF) 978-3-11-145836-6
e-ISBN (EPUB) 978-3-11-146091-8
ISSN 2751-0174
DOI https://doi.org/10.1515/9783111458366

Library of Congress Control Number: 2024945032

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.dnb.de.

Cover image: peshkov / iStock / Getty Images
Typesetting: jürgen ullrich typosatz, Nördlingen
Printing and binding: CPI books GmbH, Leck

www.degruyter.com
Questions about General Product Safety Regulation:
productsafety@degruyterbrill.com

Table of Contents

I Introduction

In the digital age, "big data" has become a key factor in economic, political, and scientific innovation and decision-making. As a result, businesses, governments, and scholars around the world are more dependent than ever on the availability of large amounts of data, which have already become relatively easy to collect, store, connect, and process due to the technological advancements that have been made in recent decades. Further improvements, the expansion of automated, algorithm-based applications, and even wider use are to be expected. Such opportunities, however, are also accompanied by risks. Therefore, issues of data protection, informational privacy,[1] data security, and cybersecurity are and will continue to be important topics of political, scholarly, and public debate. The way we respond to the issues surrounding data collection and data sharing will have an impact on (the future of) our societies that should not be underestimated. Thus, scholars, such as Reidenberg (2015) are already warning that

> [n]ormatively, the information society has created a "transparent citizenry." Citizens are widely exposed to public view without an effective boundary between public and private information. The transparent citizen loses informational self-determination in his or her relationship with the state and thus loses an important bedrock of democratic civil society. Similarly, the transparent citizen's loss of informational self-determination alters his or her private relationships in society. (Reidenberg 2015, 449)

Political action is called for to regulate not only national but also transnational data flows in order to protect individuals' informational privacy. The regulation of transnational data flows in particular is all the more relevant in today's global internet economy, where consumer data from various countries and world regions is being collected and processed daily by a multitude of businesses. The development of appropriate regulatory standards is a complex task, and not just due to the various legal frameworks in place around the world that regulate data protection and informational privacy in different ways (see, e.g., Hoffmann, 2023). The impact of cultural factors on people's attitudes to privacy and how they manage their privacy adds a further dimension of complexity. Unfortunately, although they are now well documented, "most privacy studies and designs do not sufficiently take these cultural differences into account" (Li 2022, 267). This is problematic since "[i]dentifying such cross-cultural differences is important to inform the privacy design for technologies

1 We use the terms "information privacy" and "informational privacy" synonymously. We have used the term "informational privacy" throughout this book as it is the term that we used in our international survey.

https://doi.org/10.1515/9783111458366-001

that are used across countries" (Li 2022, 267)—and, one might add, to develop adequate regulations and strategies for transnational data flows.

This is where our interdisciplinary project *Vectors of Data Disclosure*[2] comes in, combining legal, information systems, and cultural perspectives on the study of privacy regulations, privacy management, and attitudes toward privacy. The overall purpose of the cultural part of the project has been to identify cultural differences but also common, cross-cultural trends that may influence data disclosure. We therefore initially set out to determine the key parameters of the cultural context of data disclosure and researched consumer views on relevant issues pertaining to privacy and data protection in the following eight countries: Brazil, China, Germany, Ghana, Japan, Russia, Switzerland, and the United States (for an introduction to our project, see Wawra 2022). We continued by compiling cultural country reports for each of those countries (see Howe 2022; Kessel 2022; Thir et al. 2023; Wawra et al. 2022a; 2022b; 2022c; 2022d), surveying Ghanaian consumers ourselves due to a lack of substantial data (see Thir & Wawra 2023). On the basis of our research for the country reports, we then conducted comparative cultural studies along key cultural data disclosure parameters (see Wawra 2023a; 2023b).

Another central goal of our interdisciplinary project has been to capture professionals' views on selected issues related to data disclosure in order to identify areas where they are either satisfied or dissatisfied with current practices and regulations in their countries and to compare the results cross-culturally. This book presents the relevant findings from our own surveys on data protection professionals from seven countries—Brazil, China, Germany, Ghana, Japan, Switzerland, and the United States (details are given in the following section)—which have allowed us to fill this research gap. We have focused on the following key data protection issues: (1) data autonomy, (2) data sensitivity, (3) the data power of companies and governments, and, finally, (4) the impact of data protection and informational privacy regulations on companies, consumers, and the state.

In the following, we will begin by introducing the methodology of our study (see Part II), before presenting our survey results in detail and comparing them cross-culturally (see Part III). The first chapter of this third part (III.1) will deal with the topic of data autonomy, that is, with professionals' assessments of

– consumers' ability to control the disclosure of their personal data (III.1.1),

2 This project was funded by the Bavarian Research Institute for Digital Transformation (bidt) from 2021–2024. The principal investigators were Moritz Hennemann (law), Kai von Lewinski (law), Daniela Wawra (cultural studies), and Thomas Widjaja (information systems). Urs Gasser (law) was the project's external advisor.

- any potentially necessary adjustments to the regulation of data protection (III.1.2), and
- consumer data protection literacy (III.1.3).

The subsequent chapter (see III.2) will present findings on how the professionals in our seven countries perceived the sensitivity of various data categories. We will then explore the perceived data power of companies and governments (see III.3). This includes

- professionals' perceptions of corporate responsibilities when collecting consumer data (III.3.1),
- their trust in various industries as well as in national and foreign governments regarding the correct use of consumer data (III.3.2), and
- their assessments of
  - the compliance of various industries with data protection and informational privacy regulations (III.3.3);
  - the levels of consumer data protection provided by various industries (III.3.4);
  - the enforcement of consumer data protection by the government, by private parties, and within companies (III.3.5); and
  - the sufficiency of their countries' current regulations to prevent the corporate misuse of consumer data (III.3.6).

Finally, the last chapter in this part (III.4) will outline our survey findings on the perceived impact of data protection and informational privacy regulations on

- customer orientation, innovation, and cooperation (III.4.1);
- bureaucracy, privacy management, and information overload (III.4.2); and
- individuals' fundamental rights as well as digitalization (III.4.3). This last section (III.4.3) also includes professionals' assessments of the overall impact of data protection and informational privacy regulation in their countries.

We will then summarize the main insights from Part III and compare them with consumer views in Part IV, thereby identifying cross-cultural trends and cultural differences. Part V contains a discussion of factors that can influence data disclosure. After an introductory contextualization (V.1), we will present a Data Disclosure Model (V.2) based on the insights gained from our studies. We will then primarily take a historical perspective, outlining the different privacy orientations that have developed in the cultures we have studied. In particular, we will discuss the related values and norms as well as a selection of other factors of our Data Disclosure Model specifically relevant to our findings (V.3). In the final part (VI), we will reflect on our study and the relevance of looking at data protection and informational privacy through a cross-cultural lens.

II Method

In order to capture professionals' views on the current data protection and informational privacy practices and regulations in their countries, we conducted online surveys on Brazil, China, Germany, Ghana, Japan, Switzerland, and the United States in January and February of 2023.[3] The survey participants were data protection professionals, mostly from the IT sector and/or working in leadership positions (for further details and the demographic data of our sample, see Appendix I). This allowed us to ensure that those surveyed had more insight into data protection and informational privacy issues than the average citizen, as they regularly deal with these issues, think about them, and are responsible for making decisions for their organizations in this regard. The total *N* was 727, while the sample size for each country was over 100 (for details, see Table 1), with the exception of Ghana (n = 87), where it proved to be very difficult to obtain adequate participants.

Table 1: Sample sizes for each country.

Country	***n***
Brazil	105
China	105
Germany	107
Ghana	87
Japan	104
Switzerland	104
US	115
N	**727**

The survey mostly consisted of closed questions but also contained several open questions.[4] The English version of the questionnaire can be found in Appendix II.[5] Several of these questions were adapted from existing survey items from previous

3 We would like to thank the Schlesinger Group for distributing the online surveys in our seven survey countries and for their help in the data collection process.
4 We would like to extend our thanks to our colleagues Moritz Hennemann, Timo Hoffmann, Sebastian Kasper, Kai von Lewinski, Martin Richthammer, Peer Sonnenberg, and Thomas Widjaja for their helpful comments and their valuable input during the development of the questionnaire items.
5 We translated this version, which was distributed to US and Ghanaian respondents, into German ourselves for the German and Swiss respondents. The Chinese, Japanese, and Portuguese translations were supplied by the Schlesinger Group.

https://doi.org/10.1515/9783111458366-002

large-scale international studies that we had already drawn on for our country reports (see Part I). For details, see the complete list of questions in Appendix II.

For the ordinal variables in the data (e.g., five-point agreement scales ranging from *strongly agree* to *strongly disagree* and five-point sufficiency scales ranging from *sufficient* to *insufficient*), we conducted a Kruskal-Wallis test in *R* to test for significant differences between the seven countries. If the test was significant ($p < 0.05$), pairwise comparisons were conducted using multiple Wilcoxon rank-sum tests. The *p* values for each set of comparisons (21 per variable) were adjusted using Holm's (1979) method. Effect sizes for significant differences were computed using the *wilcox_effsize()* function from the *rstatix* package.

When comparing differences between paired observations measured on an ordinal scale (e.g., respondents' trust in different industries to use consumer's personal data correctly), we conducted a Friedman's ANOVA to test for significant differences, followed by pairwise Wilcoxon signed rank tests. Again, the *p* values for each set of comparisons were adjusted using Holm's (1979) method (21 per variable when comparing the seven industries). Effect sizes were computed on the basis of the Wilcoxon signed rank test using the *rFromWilcox()* function given in Field et al. (2012).

When comparing a binary response variable (e.g., *yes*/*no*) across the seven countries, we computed a generalized logistic model using the *glm() function* from the *glm2* package (Marschner 2011).

Throughout the study, statistical significance is assumed at $p < 0.05$. Whenever we use the term "significant" in this book, we are referring to a statistically significant result at this level or lower.

III Results

In this part, we present the results of our survey of data protection professionals from Brazil, China, Germany, Ghana, Japan, Switzerland, and the United States. In the following chapters (III.1–4), we will focus on the percentage distributions of respondents' answers and their statistical analysis. We will compare these results with consumers' views and provide a summary of cross-cultural trends and cultural differences in the following chapter (IV), before interpreting the results in Chapter V.

1 Data autonomy

This section presents and discusses the results of our survey of local professionals' attitudes toward data autonomy, their assessments of the state of data autonomy in their countries, and consumers' ability to exercise data autonomy. The survey items addressed the following key questions:

- To what extent should and can individuals have control over the disclosure of their own data?
- Does the legal framework ensure consumer data autonomy?
- How aware are consumers of the relevant legislation in their country, and do they themselves do enough to protect their data?
- Should data protection be strengthened/relaxed (e.g., for some data categories or for certain data recipients)?

1.1 Consumer control over data disclosure

The survey results show that, across all selected countries, an overwhelming majority (≥ 79 %) agreed strongly or somewhat that consumers should have the possibility to make self-determined decisions about disclosing their personal data. The majority of professionals in the following countries even indicated their strong agreement in this respect: Ghana (85 %), Brazil (81 %), the United States (76 %), Germany (65 %), and Switzerland (54 %). What is striking in comparison to the other countries is that only a minority of respondents from Japan (46 %) and China (34 %) agreed strongly with the statement. Similarly remarkable was the high percentage of *somewhat agree* answers (61 %) given by Chinese professionals as well as the 18 % of neutral responses provided by Japanese respondents (see Fig. 1 below).

https://doi.org/10.1515/9783111458366-003

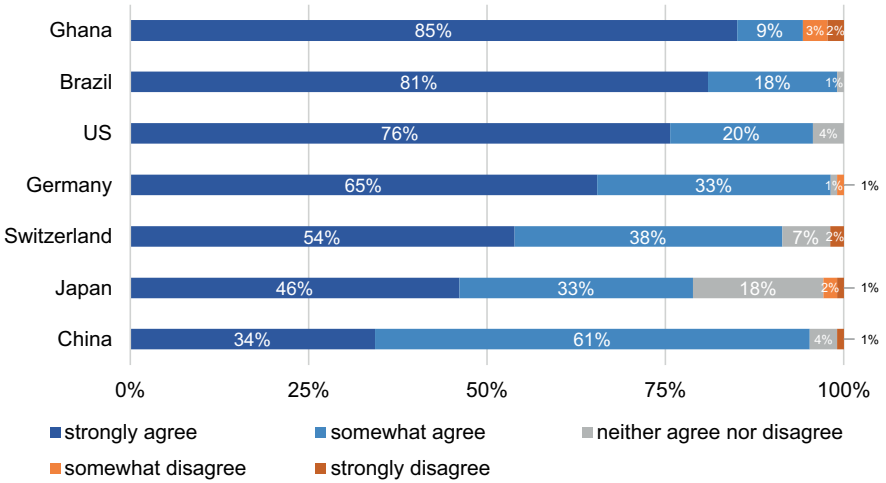

Fig. 1: Q1r1. In general, consumers should have the possibility to make self-determined decisions about the disclosure of their personal data.

Despite this general trend, it is still noteworthy that respondents' agreement with this item differed significantly across the examined countries, $H(6) = 91.26$, $p < 0.0005$. Japanese respondents exhibited significantly lower agreement with the statement than those in Brazil, Germany, Ghana, and the United States ($p < 0.0005$ and $p = 0.004$). The same four countries demonstrated significantly higher agreement than China ($p < 0.0005$ each), and three of them (Brazil, Ghana, and the United States) showed significantly greater agreement than Switzerland ($p < 0.0005$ and $p = 0.009$). However, Japan, China, and Switzerland did not differ significantly from each other ($p > 0.05$; see Table 2).

Chinese respondents in particular stood out as the comparisons between China and Brazil ($r = 0.47$) and China and Ghana approached a large effect size ($r = 0.47$; see also Table 3). A medium effect was found when examining the comparisons China-Germany ($r = 0.31$) and China-United States ($r = 0.39$) as well as Japan-Brazil ($r = 0.39$), Japan-Ghana ($r = 0.38$), Japan-United States ($r = 0.32$), Switzerland-Brazil ($r = 0.30$), and Switzerland-Ghana ($r = 0.31$). The remaining two comparisons, Japan-Germany ($r = 0.25$) and Switzerland-United States ($r = 0.23$), represented small-to-medium effects.

Table 2: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' agreement with the statement that consumers should have the possibility to make self-determined decisions about the disclosure of their personal data.

	China	Japan	Switzerland	Germany	US	Brazil
Japan	1.000					
Switzerland	0.196	0.510				
Germany	< 0.0005***	0.004**	0.327			
US	< 0.0005***	< 0.0005***	0.009*	0.674		
Brazil	< 0.0005***	< 0.0005***	< 0.0005***	0.099	0.881	
Ghana	< 0.0005***	< 0.0005***	< 0.0005***	0.051	0.674	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 3: Effect sizes for significant differences in respondents' agreement with the statement that consumers should have the possibility to make self-determined decisions about the disclosure of their personal data.

Contrast		*r*
China	Brazil	0.47
	Germany	0.31
	Ghana	0.47
	US	0.39
Japan	Brazil	0.39
	Germany	0.25
	Ghana	0.38
	US	0.32
Switzerland	Brazil	0.30
	Ghana	0.31
	US	0.23

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

While the view that consumers should be able to decide for themselves whether to disclose their data clearly dominated in all the countries surveyed, did this reflect the reality in the seven countries according to the local professionals? While no majority of professionals in any country strongly agreed that this was the case, a major-

ity in all countries at least strongly or somewhat agreed that consumers could make self-determined decisions in their country. Of all the professionals, the Japanese were the least likely to agree (55 %), showing the highest disagreement (21 % *somewhat disagree* or *strongly disagree*) (see Fig. 2 below).

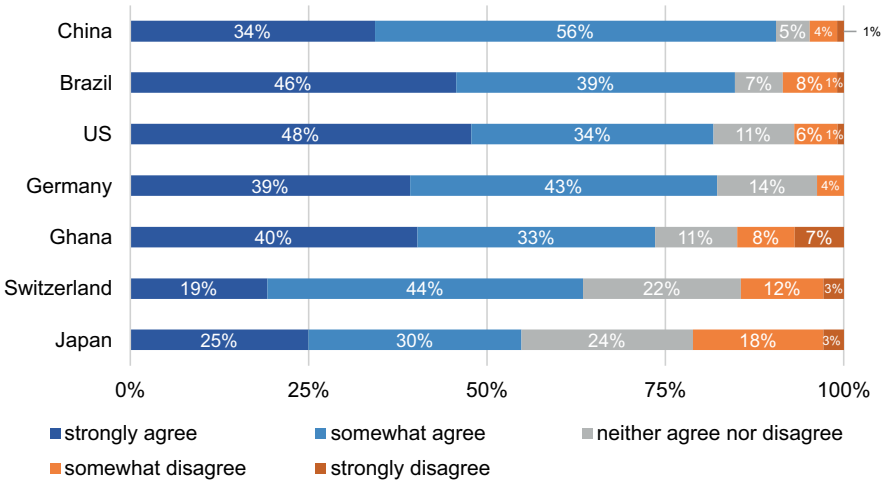

Fig. 2: Q1r2. In general, consumers in my country can make self-determined decisions about the disclosure of their personal data.

Again, respondents' agreement differed significantly across the countries examined, $H(6) = 48.26$, $p < 0.0005$. Both Japanese and Swiss respondents agreed significantly less with the statement than respondents in Brazil, China, Germany, and the United States (p ranging from < 0.0005 to 0.001; see Table 4). All these differences either amounted to or approached medium effect sizes (with r ranging from 0.27 to 0.30; see Table 5).

Table 4: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' agreement with the statement that consumers in their country can make self-determined decisions about the disclosure of their personal data.

	Japan	Switzerland	Ghana	Germany	US	Brazil
Switzerland	1.000					
Ghana	0.164	0.196				
Germany	0.001**	0.001**	1.000			
US	< 0.0005***	< 0.0005***	1.000	1.000		
Brazil	< 0.0005***	< 0.0005***	1.000	1.000	1.000	
China	0.0005**	0.0005**	1.000	1.000	1.000	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 5: Effect sizes for significant differences in respondents' agreement with the statement that consumers in their country can make self-determined decisions about the disclosure of their personal data.

Contrast		*r*
Japan	Brazil	0.30
	China	0.29
	Germany	0.28
	US	0.30
Switzerland	Brazil	0.30
	China	0.29
	Germany	0.27
	US	0.30

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

When asked more specifically whether consumers in their country are sometimes restricted in their data autonomy, a majority of Brazilian professionals (59 %) answered in the affirmative (see Fig. 3 below). They gave the following reasons:

- secret data collection by companies
- insufficient information on the part of companies
- data being transferred to third parties without the users' consent
- digital data theft
- data leaks
- a lack of options to not disclose

– consumers not taking enough time to inform themselves about what happens to their data and not being aware of the consequences of data disclosure

US professionals were undecided: 50 % thought they were restricted, and 50 % thought they were not. In all the other countries surveyed, the majority saw no restrictions on consumers in this regard. China stood out in that as many as 79 % of the professionals surveyed expressed the view that there were no restrictions on consumer data autonomy in their country.

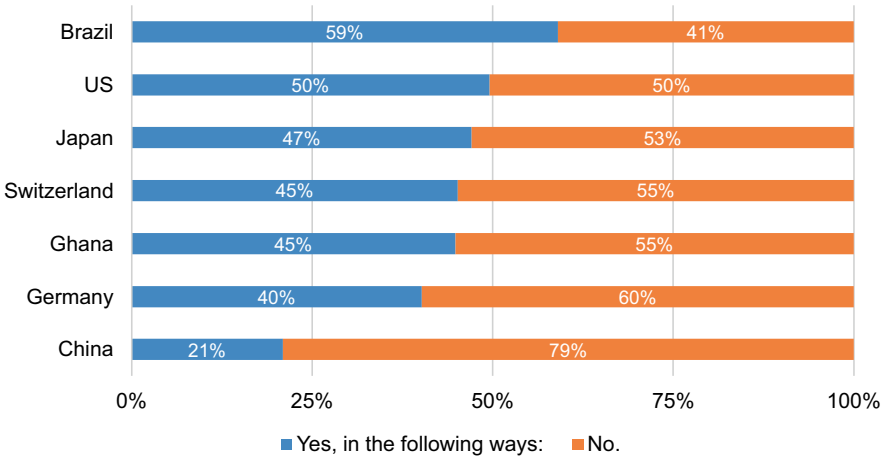

Fig. 3: Q2. In your expert opinion, are consumers in your country sometimes restricted in their data autonomy (i.e., they cannot always make self-determined decisions about the disclosure of their personal data)?

Brazil's and, in particular, China's special status was also evident when looking at the results of a generalized logistic model, which we used to evaluate the effect of the variable *country* on the binary response variable. The model summary in Table 6 shows that Brazilian professionals' response behavior differed significantly from that of professionals in China ($p < 0.0005$), Germany ($p = 0.006$), and Switzerland ($p = 0.046$). Chinese respondents were 82 % less likely to select *yes* for this item than Brazilian respondents ($OR = 0.18$), whereas German respondents were 53 % less likely ($OR = 0.47$) and Swiss respondents 43 % less likely ($OR = 0.57$). In fact, we found significant differences between China and all other countries (with p ranging from < 0.0005 to 0.030; see Table 7). Chinese respondents were 73 % less likely to select *yes* than US respondents ($OR = 0.27$), 70 % less likely than Japanese respondents ($OR = 0.30$), 68 % less likely than Swiss respondents ($OR = 0.32$), 67 % less likely than Ghanaian respondents ($OR = 0.33$), and 61 % less likely than German respondents

(*OR* = 0.39). Thus, even more so than Brazil, China stood out here in that the view that consumers are not restricted in their data autonomy was exceptionally widespread among Chinese professionals.

Table 6: Summary of logistic regression model regarding respondents' views on consumers being restricted in their data autonomy.

Fixed effects	***Estimate***	***SE***	***z value***	***p* value**
Intercept	0.366	0.198	1.844	0.065
US	-0.383	0.272	-1.408	0.159
Japan	-0.481	0.279	-1.724	0.085
Switzerland	-0.559	0.280	-1.998	0.046*
Ghana	-0.574	0.293	-1.957	0.050
Germany	-0.764	0.280	-2.730	0.006*
China	-1.694	0.311	-5.441	< 0.0005***

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Brazilian respondents were set as the reference category (intercept). Significant effects are shaded grey.

Table 7: *P* values of further significant differences regarding respondents' views on consumers being restricted in their data autonomy.[6]

Contrast		***p***
China	Germany	0.030*
	Ghana	0.006*
	Japan	0.001**
	Switzerland	0.003**
	US	< 0.0005***

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05.

Moving on to professionals' assessments of the sufficiency of legislation in their countries to ensure consumer data autonomy, we found that most Chinese professionals (76 %) considered their country's legislation to be *sufficient* or *rather sufficient* in this respect, as did 69 % of German, 66 % of US, 63 % of Brazilian, and 55 % of

6 Any *p* values not contained in Table 6 were obtained by running the model again after adjusting the reference category for "country" and then applying Holm's (1979) method to correct for multiple comparisons. This table only contains statistically significant contrasts ($p < 0.05$), i.e., insignificant contrasts are not included.

Swiss respondents. However, only 35 % of Ghanaian and 30 % of Japanese professionals held this opinion for their countries. Almost as many took a neutral stance (30 % of Ghanaian and 28 % of Japanese respondents), so there was no majority in either country that rated its legislation as *rather insufficient* or *insufficient* in this respect either (see Fig. 4 below).

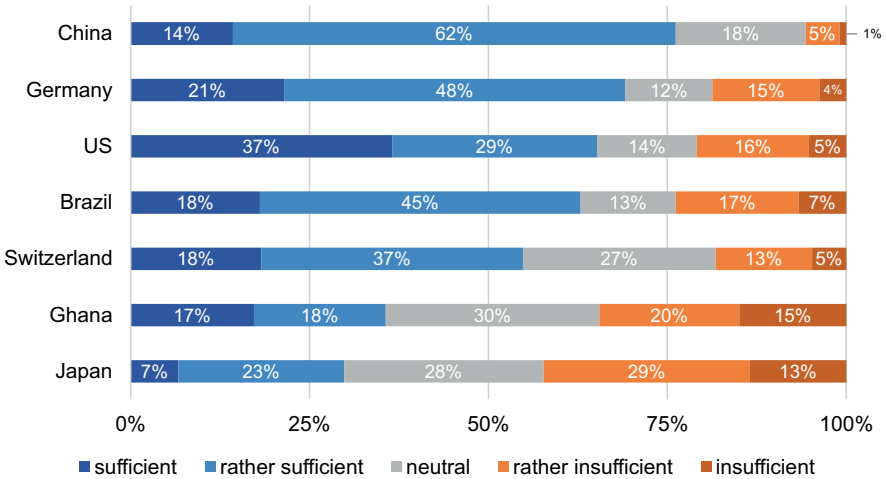

Fig. 4: Q3. Legislation in my country is … to ensure consumers' self-determined decisions about the disclosure of their personal data.

Japan's and Ghana's special status regarding this item was also confirmed on the basis of statistical tests. Respondents' assessments of the sufficiency of their country's legislation to ensure consumer data autonomy differed significantly across the examined countries, $H(6) = 65.42$, $p < 0.0005$. Japanese respondents regarded their country's legislation as significantly less sufficient in this respect than respondents in all other countries except for Ghana ($p < 0.0005$ for all contrasts except Japan-Ghana). These differences amounted to medium effects ($r = 0.30$ or $r = 0.38$; see Table 9), apart from the difference between Japan and China, which approached a large effect size ($r = 0.47$). Moreover, the sufficiency ratings given by Ghanaian respondents were significantly lower than those assigned by Chinese, German, and US respondents (p ranging from < 0.0005 to 0.004; see Table 8), with medium ($r = 0.34$ for Ghana-China) or small-to-medium effect sizes ($r = 0.26$ for Ghana-Germany and $r = 0.27$ for Ghana-United States).

Table 8: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' assessments of the sufficiency of their country's legislation to ensure that consumers can make self-determined decisions about the disclosure of their personal data.

	Japan	Ghana	Switzerland	Brazil	China	Germany
Ghana	1.000					
Switzerland	< 0.0005***	0.117				
Brazil	< 0.0005***	0.106	1.000			
China	< 0.0005***	< 0.0005***	0.233	0.759		
Germany	< 0.0005***	0.004**	1.000	1.000	1.000	
US	< 0.0005***	0.001**	0.407	0.529	1.000	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 9: Effect sizes for significant differences in respondents' assessments of the sufficiency of their country's legislation to ensure that consumers can make self-determined decisions about the disclosure of their personal data.

Contrast		*r*
Japan	Brazil	0.30
	China	0.47
	Germany	0.38
	Switzerland	0.30
	US	0.38
Ghana	China	0.34
	Germany	0.26
	US	0.27

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

1.2 The necessity of adjustments to data protection and information privacy regulations

Next, we were interested in whether professionals thought that the regulation of data protection and informational privacy in their country should be reformed in any way. We therefore asked respondents whether there were certain

(a) types of data
(b) contexts of data disclosure

(c) purposes of data collection or
(d) industries

for which they thought that the regulation of data protection and informational privacy needed adjusting. For each of these four items, they could either list points in an open text response in the fields *stricter:* and/or *weaker:* or select the answer option *No adjustments are necessary*. If respondents entered answers such as "no" or "none" in both fields, this was taken to indicate that they believed no adjustments were necessary, and their response was recoded as such. If respondents' entries indicated that they did not know (e.g., "not sure") or that they did not want to give an answer (e.g., by entering a random number), this was counted as an empty text field. Respondents who had given such an answer in both of an item's open text fields (which enabled them to essentially skip the question) were removed from the statistical analysis for this item. The proportion of these respondents is given in grey in Fig. 5 (section 1.2.1), Fig. 10 (section 1.2.2), Fig. 13 (section 1.2.3), and Fig. 17 (section 1.2.4) below.

It should be noted that each of the four items contained examples in order to facilitate respondents' understanding of the question, e.g., "Are there certain types of data (e.g., health data, financial data, personal identification numbers, etc.) … ." During our qualitative analysis, we noticed that this may have primed participants to primarily name these categories. This must be taken into account when interpreting the results of the open-ended responses presented below.

1.2.1 Types of data

Let us first consider (a) types of data. Fig. 5 shows that it was only in China, Switzerland, and Japan that a majority of respondents believed that no adjustments to the regulation of data protection and informational privacy were necessary in this regard, though in Switzerland and Japan, this amounted to just over half of respondents (51 % and 52 %). German respondents were undecided, with half (50 %) believing that no adjustments were necessary. By contrast, in Ghana, the United States, and Brazil, only a minority of professionals saw no need for adjustment (40 % for Ghana, 34 % for the United States, and 19 % for Brazil).

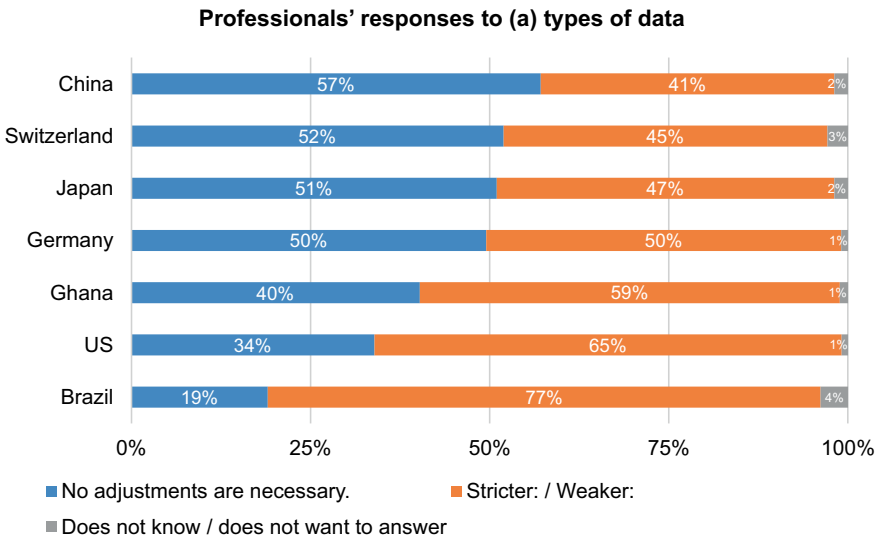

Fig. 5: Q4. Are there certain types of data (e.g., health data, financial data, personal identification numbers, etc.) for which you think the regulation of data protection and informational privacy should be ...

To test whether these differences were significant, we treated the variable as a binary response variable (comparing participants who had opted for *No adjustments are necessary* with those who had not) and computed a generalized logistic model. Respondents who had indicated that they did not have an answer or did not want to give one were removed from the dataset. The adjusted *n* values of the seven subsamples on which the following model is based are given in Table 10.

Table 10: Adjusted sample sizes for each country.

Country	***n***
Brazil	101
China	103
Germany	106
Ghana	86
Japan	102
Switzerland	101
US	114
N	**713**

The model summary in Table 11 shows that Chinese professionals' response behavior differed significantly to that of respondents in Brazil ($p < 0.0005$), the United States ($p < 0.0005$) and Ghana ($p = 0.017$). Brazilian respondents were 82 % less likely to select *No adjustments are necessary* than Chinese respondents ($OR = 0.18$), whereas US respondents were 63 % less likely ($OR = 0.37$) and Ghanaian respondents 51 % less likely ($OR = 0.49$). In addition, Brazilian professionals were significantly more likely to see a need for adjustment than respondents from four other countries ($p < 0.0005$, $p = 0.025$; see Table 12): They were 79 % less likely to believe that no adjustments were necessary than Swiss respondents ($OR = 0.21$), 77 % less likely than Japanese respondents ($OR = 0.23$), 75 % less likely than German respondents ($OR = 0.25$), and 64 % less likely than Ghanaian respondents ($OR = 0.36$).

Table 11: Summary of logistic regression model regarding respondents' views on whether the regulation of data protection and informational privacy needs adjusting for certain types of data.

Fixed effects	***Estimate***	***SE***	***z value***	***p* value**
Intercept	0.333	0.200	1.667	0.095
Switzerland	-0.194	0.282	-0.688	0.491
Japan	-0.255	0.281	-0.905	0.365
Germany	-0.333	0.279	-1.195	0.232
Ghana	-0.71	0.297	-2.391	0.017*
US	-0.987	0.281	-3.514	< 0.0005***
Brazil	-1.732	0.320	-5.416	< 0.0005***

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Chinese respondents were set as the reference category (intercept). Significant effects are shaded grey.

Table 12: *P* values of further significant differences regarding respondents' views on whether the regulation of data protection and informational privacy needs adjusting for certain types of data.[7]

Contrast		*p*
Brazil	Germany	< 0.0005***
	Ghana	0.025*
	Japan	< 0.0005***
	Switzerland	< 0.0005***

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05.

Thus, even more so than China and Switzerland, Brazil stood out here in that Brazilian professionals were significantly more likely to see a need for adjustments to the regulation of data protection and informational privacy for certain data types than respondents in *all* other countries except for the United States. By contrast, Chinese respondents were significantly less likely to hold such views than respondents from three out of the six countries (Brazil, the United States, and Ghana).

Let us therefore take a closer look at Brazilian professionals' responses to this item. Fig. 6 shows that the vast majority of Brazilian respondents (72 %) advocated to increase the regulation of data protection and informational privacy for certain data types by entering something in the field *Stricter:*. By far the most frequent type of data named by Brazilian respondents in this respect was various types of financial data (or financial data in general), which were mentioned by 42 % of all Brazilian respondents. In contrast, only 31 % of Brazilian professionals believed that regulation should be weaker for certain types of data. The most common data type named in this respect was health data (13 %).

7 Any *p* values not contained in Table 11 were obtained by running the model again after adjusting the reference category for "country" and then applying Holm's (1979) method to correct for multiple comparisons. This table only contains statistically significant contrasts ($p < 0.05$), i.e., insignificant contrasts are not included.

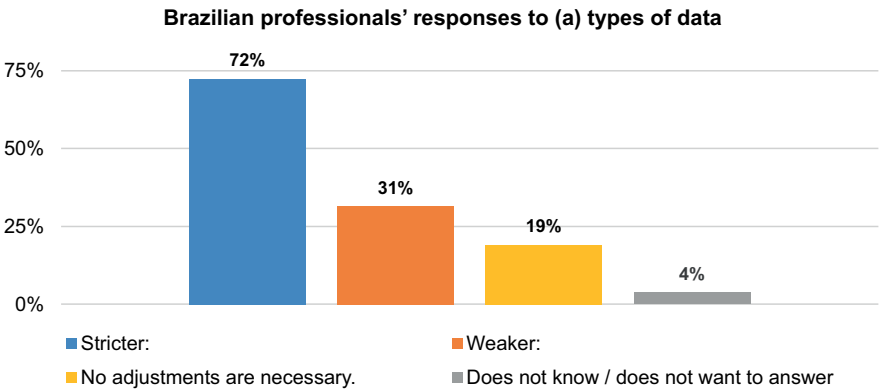

Fig. 6: Brazilian professionals' responses to Q4: Are there certain types of data (e.g., health data, financial data, personal identification numbers, etc.) for which you think the regulation of data protection and informational privacy should be …

Turning to US respondents, Fig. 7 shows that a clear majority (64 %) advocated to increase the regulation of data protection and informational privacy for certain data types. The most frequent type of data named in this respect was health-related data (16 % of all US respondents), which was followed closely by financial data (14 %). By contrast, only 25 % of US professionals believed that regulation should be weaker for certain types of data. Health data and financial data were also mentioned here, but by less than 3 % each.

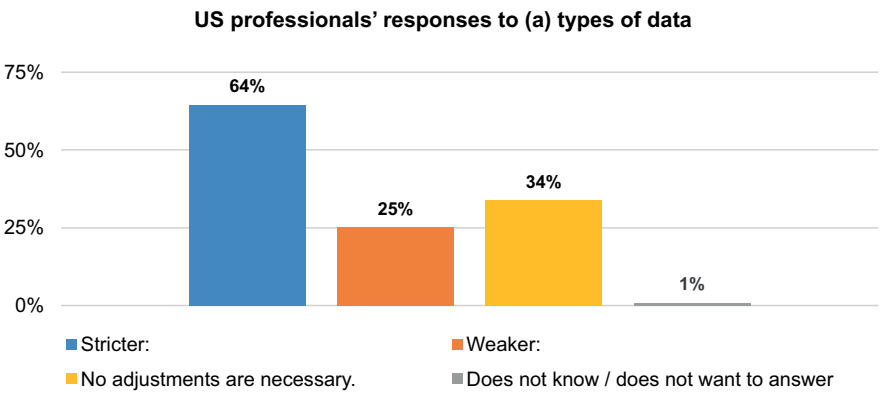

Fig. 7: US professionals' responses to Q4: Are there certain types of data (e.g., health data, financial data, personal identification numbers, etc.) for which you think the regulation of data protection and informational privacy should be …

Moving on to Ghanaian respondents (Fig. 8), we see that a majority of 54 % advocated to increase the regulation of data protection and informational privacy for certain data types. The data type most frequently named by Ghanaian respondents in this respect was financial data at 23 %, followed by personal identification information (e.g., ID numbers) at 14 % and health data at 13 %. Only 15 % of Ghanaian professionals believed that regulation should be weaker for certain types of data. Health data was the most frequent data type mentioned here, albeit by a smaller proportion of respondents (9 %) than those who advocated for stricter rules in this regard.

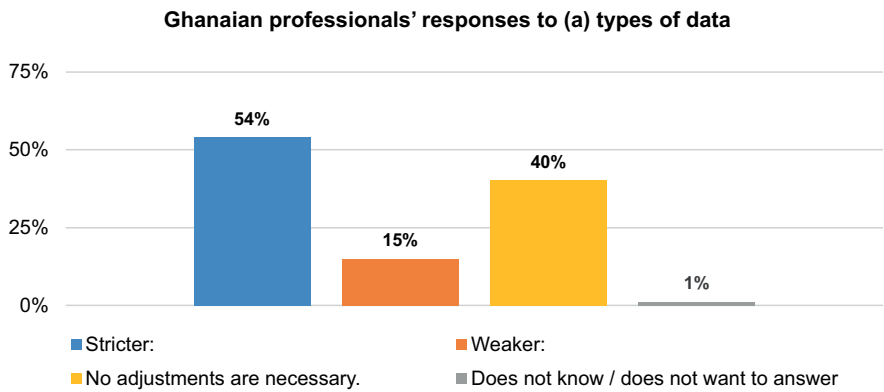

Fig. 8: Ghanaian professionals' responses to Q4: Are there certain types of data (e.g., health data, financial data, personal identification numbers, etc.) for which you think the regulation of data protection and informational privacy should be …

Regarding German respondents, Fig. 9 shows that half advocated to increase the regulation of data protection and informational privacy for certain data types. The most frequent type of data named in this respect was financial data (21 % of all German respondents), followed by health data (17 %). Only 22 % of German professionals believed that regulation should be weaker for certain types of data. Health data was the most frequent data type mentioned here, albeit by a much smaller proportion of respondents (4 %) than those who advocated for stricter rules in this regard.

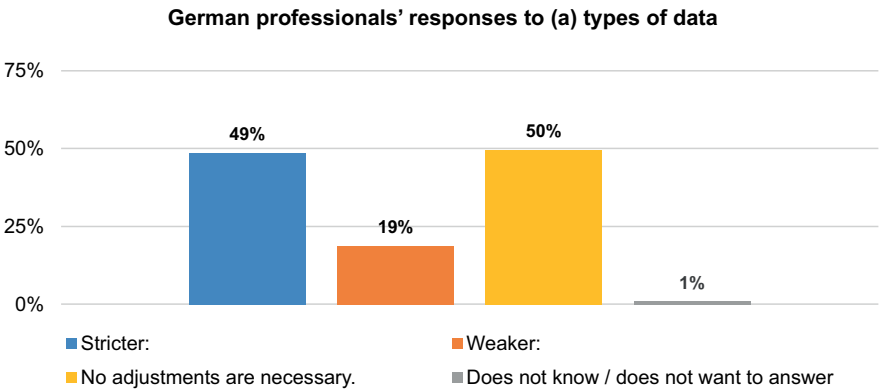

Fig. 9: German professionals' responses to Q4: Are there certain types of data (e.g., health data, financial data, personal identification numbers, etc.) for which you think the regulation of data protection and informational privacy should be …

1.2.2 Contexts of data disclosure

Let us now move on to (b) contexts of data disclosure. Fig. 10 shows that the majority of respondents in all countries except for Brazil and the United States believed that no adjustments to the regulation of data protection and informational privacy were necessary in this regard, though in Ghana, this was just over half of respondents (51 %). China was once again the country where the highest proportion of respondents (67 %) held this view. In the United States and Brazil, only a minority of professionals saw no need for adjustment (38 % in the United States and 34 % in Brazil).

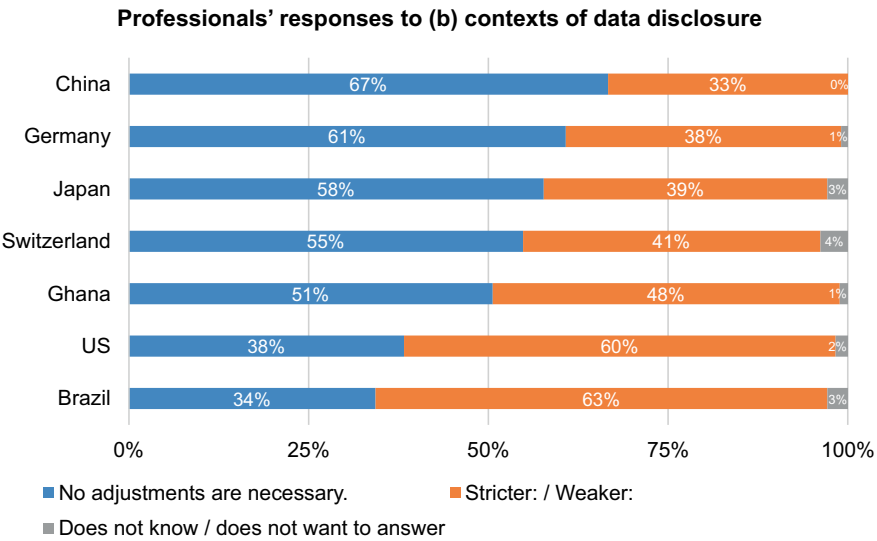

Fig. 10: Q5. Are there certain contexts of data disclosure (e.g., when using smartphone apps, when disclosing data to foreign governments, etc.), for which you think the regulation of data protection and informational privacy should be ...

Like with the previous variable, we treated this one as a binary response variable (comparing participants who had opted for *No adjustments are necessary* to those who had not) to test for significant differences between the countries with the help of a generalized logistic model. Again, respondents who had indicated that they did not have an answer or did not want to give one were removed from the dataset. The adjusted *n* values of the seven subsamples on which the following model is based are given in Table 13. This time, we set Brazil as the reference category, as a visual inspection of Fig. 10 suggested its special status in terms of this variable, alongside the United States.

Table 13: Adjusted sample sizes for each country.

Country	*n*
Brazil	102
China	105
Germany	106
Ghana	86
Japan	101
Switzerland	100
US	113
N	**713**

The model summary in Table 14 confirms this first impression: Brazilian respondents were significantly less likely to believe that no adjustments to the regulation of data protection and informational privacy were necessary in certain contexts of data disclosure than respondents in almost all other countries (with p varying between < 0.0005 and 0.029), the exception being the US. Brazilian respondents were 73 % less likely than Chinese respondents (OR = 0.27), 66 % less likely than German respondents (OR = 0.34), 63 % less likely than Japanese respondents (OR = 0.37), 59 % less likely than Swiss respondents (OR = 0.41), and 48 % less likely than Ghanaian respondents (OR = 0.52) to hold this view. In addition, US respondents were also significantly less likely to choose the option *No adjustments are necessary* than respondents in China (p = 0.001; see also Table 15), Germany (p = 0.014), and Japan (p = 0.039), with a decrease in probability of 68 % relative to Chinese respondents (OR = 0.32), 60 % relative to German respondents (OR = 0.4), and 56 % relative to Japanese respondents (OR = 0.44).

Thus, Brazilian professionals were, again, significantly more likely to see a need for adjustment than professionals from almost all other countries, the exception again being the United States. Moreover, US respondents were significantly more likely to hold such a view than respondents from three out of six countries (China, Germany, and Japan).

Table 14: Summary of logistic regression model regarding respondents' views on whether the regulation of data protection and informational privacy needs adjusting in certain contexts of data disclosure.

Fixed effects	***Estimate***	***SE***	***z value***	***p* value**
Intercept	-0.606	0.207	-2.925	0.003
China	1.299	0.293	4.436	< 0.0005***
Germany	1.067	0.288	3.71	< 0.0005***
Japan	0.987	0.29	3.405	0.001**
Switzerland	0.888	0.289	3.069	0.002**
Ghana	0.653	0.299	2.182	0.029*
US	0.156	0.283	0.552	0.581

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Brazilian respondents were set as the reference category (intercept). Significant effects are shaded grey.

Table 15: *P* values of further significant differences regarding respondents' views on whether the regulation of data protection and informational privacy needs adjusting in certain contexts of data disclosure.[8]

Contrast		***p***
US	China	0.001**
	Germany	0.014*
	Japan	0.039*

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05.

Let us therefore examine Brazilian professionals' responses to this item more closely. Fig. 11 shows that the majority of Brazilian respondents (58 %) advocated to increase the regulation of data protection and informational privacy in certain contexts of data disclosure. At 14 %, the context most frequently named by Brazilian respondents in this respect was various smartphone applications and phone-related disclosure contexts/data in general. Slightly more respondents (15 %) did not mention any particular context of data disclosure, referring to various kinds of financial or banking-related data instead. By contrast, only 22 % of Brazilian professionals be-

8 Any *p* values not contained in Table 14 were obtained by running the model again after adjusting the reference category for "country" and then applying Holm's (1979) method to correct for multiple comparisons. This table only contains statistically significant contrasts ($p < 0.05$), i.e., insignificant contrasts are not included.

lieved that regulation should be weaker in certain contexts of data disclosure. Here, too, smartphone applications and phone-related contexts were mentioned most often (5 % of all Brazilian respondents).

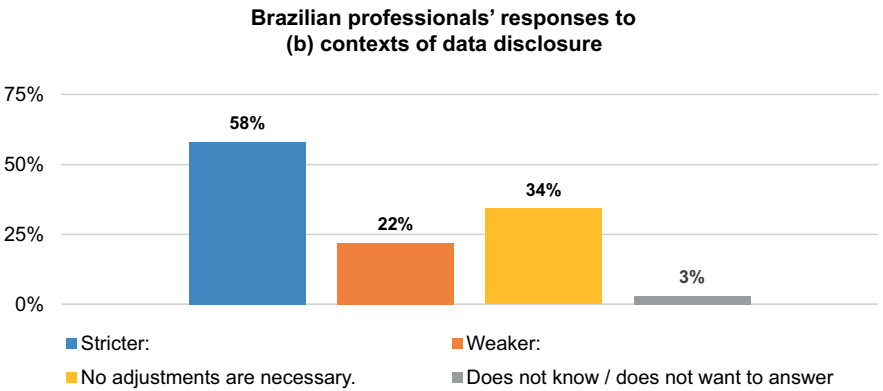

Fig. 11: Brazilian professionals' responses to Q5: Are there certain contexts of data disclosure (e.g., when using smartphone apps, when disclosing data to foreign governments, etc.), for which you think the regulation of data protection and informational privacy should be …

Taking a closer look at US professionals' responses (Fig. 12), we see that here, too, a majority of 58 % advocated to increase the regulation of data protection and informational privacy in certain contexts of data disclosure. The most frequent context named by US respondents in this respect was smartphone applications and phone-related disclosure contexts, though these were only mentioned by 8 % of all respondents.

Like Brazilian respondents, only 22 % of US professionals believed that regulation should be weaker in certain contexts of data disclosure. None of the contexts mentioned by US respondents, however, were named by more than 3 % of respondents.

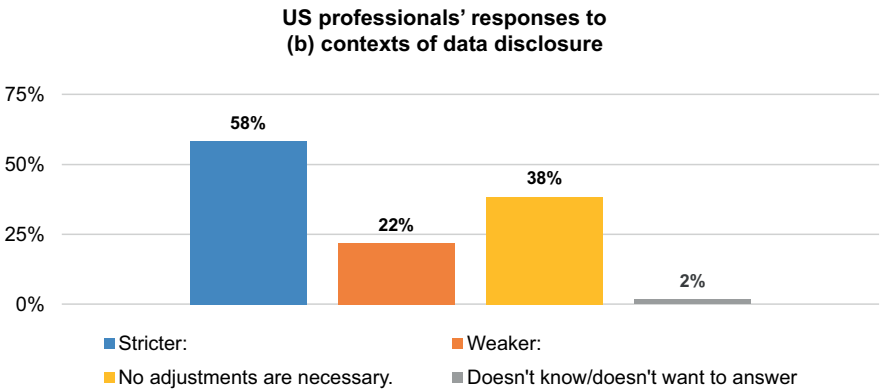

Fig. 12: US professionals' responses to Q5: Are there certain contexts of data disclosure (e.g., when using smartphone apps, when disclosing data to foreign governments, etc.), for which you think the regulation of data protection and informational privacy should be ...

1.2.3 Purposes of data collection

The next point to consider is (c) purposes of data collection. Fig. 13 shows that a majority of respondents in China, Japan, Germany, and Switzerland believed that no adjustments to the regulation of data protection and informational privacy were necessary in this respect. China was again the country where the highest proportion of respondents (69 %) held this view. In the United States, Ghana, and Brazil, however, only a minority of professionals saw no need for adjustment (42 % in the United States, 41 % in Ghana, and 37 % in Brazil; the latter was once again the country with the smallest proportion of respondents holding this view).

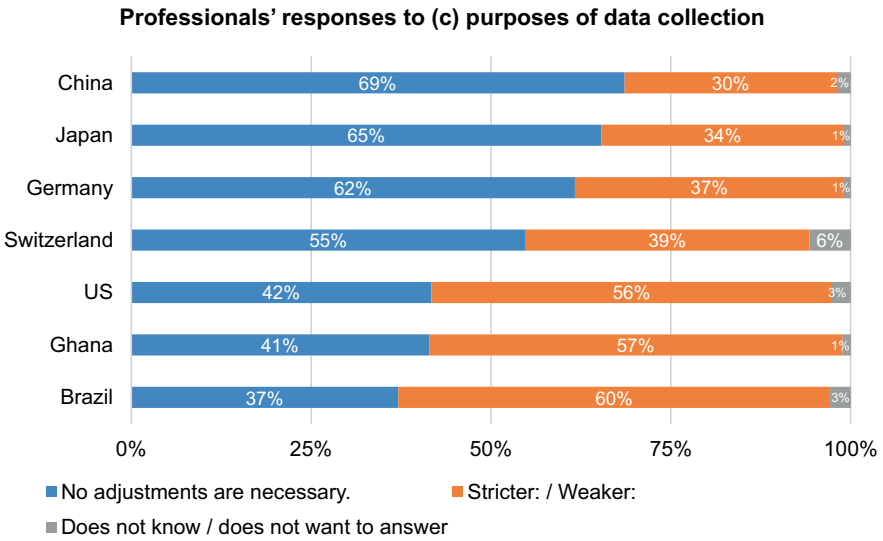

Fig. 13: Q6. Are there certain purposes of data collection (e.g., law enforcement, medical research, marketing, etc.) for which you think the regulation of data protection and informational privacy should be ...

We again computed a generalized logistic model, setting Brazil as the reference category (see the model summary in Table 17). Once more, respondents who had indicated that they did not have an answer or did not want to give one were removed from the dataset (see Table 16 for the adjusted *n* values of the seven subsamples).

Table 16: Adjusted sample sizes for each country.

Country	***n***
Brazil	102
China	103
Germany	106
Ghana	86
Japan	103
Switzerland	98
US	112
N	**710**

Brazilian respondents were significantly less likely to believe that no adjustments to the regulation of data protection and informational privacy were necessary for cer-

tain purposes of data collection than respondents in most other countries (with p varying between < 0.0005 and 0.005), the exceptions being the United States and Ghana. They were 73 % less likely than Chinese respondents (OR = 0.27), 68 % less likely than Japanese respondents (OR = 0.32), 62 % less likely than German respondents (OR = 0.38), and 55 % less likely than Swiss respondents (OR = 0.45) to hold this view.

US respondents were also significantly less likely to see no need for adjustment than respondents in China (p = 0.001; see also Table 18), Japan (p = 0.010), and Germany (p = 0.048), with a decrease in probability of 68 % relative to Chinese respondents (OR = 0.32), 61 % relative to Japanese respondents (OR = 0.39), and 55 % relative to German respondents (OR = 0.45). Alongside US and Brazilian respondents, Ghanaian respondents were also significantly less likely to opt for *No adjustments are necessary* than Chinese respondents (p = 0.002)—with a decrease in probability of 69 % (OR = 0.31)—and Japanese respondents (p = 0.012)—with a decrease in probability of 63 % (OR = 0.37).

The pattern already observed for (a) and (b) was thus also evident for (c): Brazilian professionals were significantly more likely to see a need for adjustment than professionals in most other countries, the exception being the United States and, this time, Ghana as well. US professionals were significantly more likely to hold such a view than respondents from three out of six countries (China, Japan, and Germany). By contrast, Chinese and Japanese respondents were less likely to hold such a view than respondents from three out of six countries (Brazil, the United States, and Ghana).

Table 17: Summary of logistic regression model regarding respondents' views on whether the regulation of data protection and informational privacy needs adjusting for certain purposes of data collection.

Fixed effects	***Estimate***	***SE***	***z value***	***p* value**
Intercept	-0.480	0.204	-2.354	0.019
China	1.322	0.296	4.466	< 0.0005***
Japan	1.144	0.291	3.928	< 0.0005***
Germany	0.98	0.286	3.431	0.001**
Switzerland	0.809	0.289	2.801	0.005*
US	0.192	0.279	0.687	0.492
Ghana	0.151	0.299	0.506	0.613

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Brazilian respondents were set as the reference category (intercept). Significant effects are shaded grey.

Table 18: *P* values of further significant differences regarding respondents' views on whether the regulation of data protection and informational privacy needs adjusting for certain purposes of data collection.[9]

Contrast		*p*
US	China	0.001**
	Germany	0.048*
	Japan	0.010*
Ghana	China	0.002**
	Japan	0.012*

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05.

Let us now examine Brazilian professionals' responses to this item more closely. Fig. 14 shows that a majority of Brazilian respondents (53 %) advocated to increase the regulation of data protection and informational privacy for certain purposes of data collection. The most frequent purpose named by Brazilian respondents in this respect was law enforcement. This was, however, mentioned by only 8 % of all Brazilian respondents and was closely followed by medical research/data and financial data (6 % each). By contrast, only 22 % of Brazilian professionals believed that regulation should be weaker for certain purposes of data collection. The most common purposes named in this regard were marketing and medical-research-/health-data-related purposes, though each of these were named by only 4 % of respondents.

9 Any *p* values not contained in Table 17 were obtained by running the model again after adjusting the reference category for "country" and then applying Holm's (1979) method to correct for multiple comparisons. This table only contains statistically significant contrasts ($p < 0.05$), i.e., insignificant contrasts are not included.

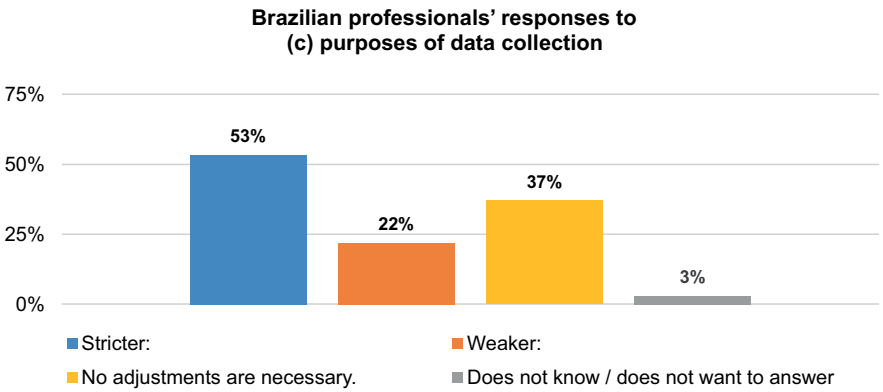

Fig. 14: Brazilian professionals' responses to Q6: Are there certain purposes of data collection (e.g., law enforcement, medical research, marketing, etc.) for which you think the regulation of data protection and informational privacy should be ...

As for US respondents (Fig. 15), a majority (53 %) advocated to increase the regulation of data protection and informational privacy for certain purposes of data collection. The most frequent purpose named by US respondents in this respect was law enforcement (including related datatypes) (11 %). This was closely followed by medical research (and related data types) (10 %). In contrast, only 22 % of US professionals believed that regulation should be weaker for certain purposes of data collection. The purpose named most frequently in this regard was marketing (5 %).

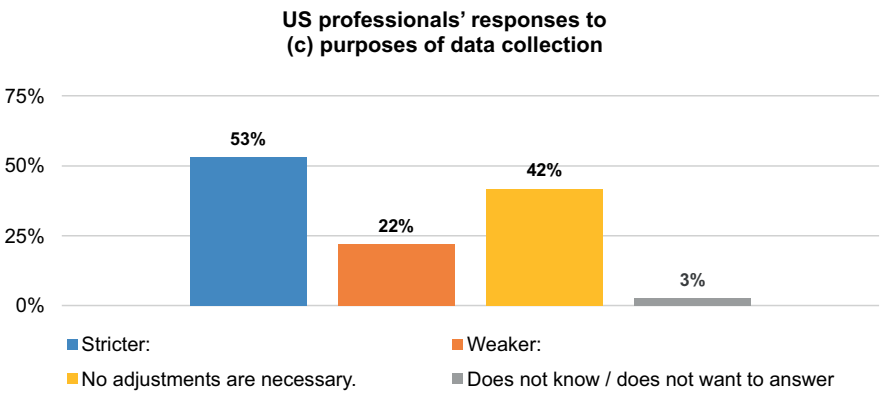

Fig. 15: US professionals' responses to Q6: Are there certain purposes of data collection (e.g., law enforcement, medical research, marketing, etc.) for which you think the regulation of data protection and informational privacy should be ...

Turning to Ghanaian respondents (Fig. 16), we see that a slight majority (52 %) advocated to increase the regulation of data protection and informational privacy for certain purposes of data collection. The most frequent purposes named by Ghanaian respondents in this respect were law enforcement and medical/health-related purposes (including medical research) (14 % each). This was closely followed by marketing, mentioned by 11 %. By contrast, only 15 % of Ghanaian professionals believed that regulation should be weaker for certain purposes of data collection. The purposes mentioned most frequently in this regard were medical research and marketing, each named by 5 % of respondents.

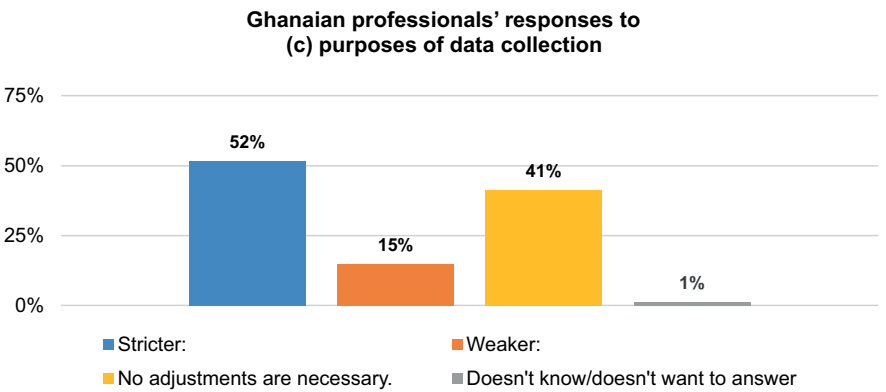

Fig. 16: Ghanaian professionals' responses to Q6: Are there certain purposes of data collection (e.g., law enforcement, medical research, marketing, etc.) for which you think the regulation of data protection and informational privacy should be …

1.2.4 Industries

Finally, let us examine the responses to the question of whether the regulation of data protection and informational privacy should be adjusted in certain industries (d). Fig. 17 shows that, again, a majority of respondents in China, Japan, Germany, and Switzerland believed that no adjustments were necessary, with China the country where the highest proportion of respondents (67 %) held this view. It should be noted, however, that in Germany, just over half of respondents (53 %) believed this to be the case. As for point (c), Ghana, the United States, and Brazil were the countries where only a minority of professionals saw no need for adjustment. Brazil was the country with the smallest proportion of respondents holding this view (27 %, compared with 43 % for Ghana and 39 % for the United States).

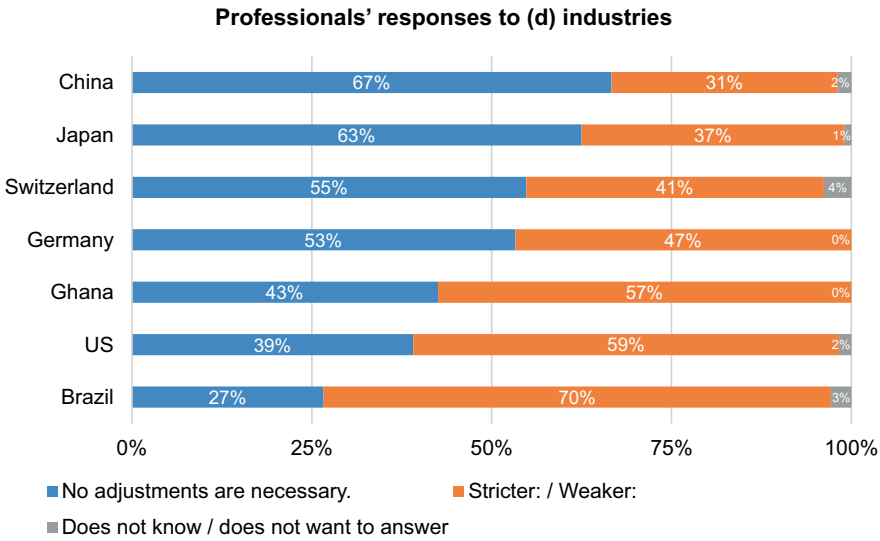

Fig. 17: Q7. Are there certain industries (e.g., healthcare, social media companies, financial sector, etc.) for which you think the regulation of data protection and informational privacy should be ...

We again removed respondents who had indicated that they did not have an answer or did not want to give one from the dataset (see Table 19 for the adjusted *n* values of the seven subsamples) and then computed a generalized logistic model with Brazil set as the reference category.

Table 19: Adjusted sample sizes for each country.

Country	***n***
Brazil	102
China	103
Germany	107
Ghana	87
Japan	103
Switzerland	100
US	113
N	**715**

The model summary in Table 20 shows that Brazilian respondents were significantly less likely to see no need for adjustment to the regulation of data protection and informational privacy in certain industries than respondents in *all* countries

except for the United States (with p varying between < 0.0005 and 0.031). They were 82 % less likely than Chinese respondents (OR = 0.18), 78 % less likely than Japanese respondents (OR = 0.22), 71 % less likely than Swiss respondents (OR = 0.29), 67 % less likely than German respondents (OR = 0.33), and 49 % less likely than Ghanaian respondents (OR = 0.51) to hold this view.

US respondents were also significantly less likely to see no need for adjustment than respondents in China (p = 0.001; see also Table 21) and Japan (p = 0.009), with a decrease in probability of 69 % relative to Chinese respondents (OR = 0.31) and 61 % relative to Japanese respondents (OR = 0.39). In addition to US and Brazilian respondents, Ghanaian respondents were significantly less likely to opt for *No adjustments are necessary* than Chinese respondents (p = 0.007), with a decrease in probability of 65 % (OR = 0.35).

Brazilian respondents were thus once again the odd ones out: They were significantly more likely to see a need for adjustment than professionals from *all* other countries but the United States. As for points (a) types or data and (c) purposes of data collection, Chinese respondents were less likely to hold such a view than respondents from three out of six countries (Brazil, the United States, and Ghana).

Table 20: Summary of logistic regression model regarding respondents' views on whether the regulation of data protection and informational privacy needs adjusting in certain industries.

Fixed effects	***Estimate***	***SE***	***z value***	***p* value**
Intercept	-0.972	0.222	-4.38	< 0.0005***
China	1.724	0.306	5.628	< 0.0005***
Japan	1.509	0.302	5.003	< 0.0005***
Switzerland	1.254	0.300	4.178	< 0.0005***
Germany	1.103	0.295	3.744	< 0.0005***
Ghana	0.671	0.310	2.162	0.031*
US	0.559	0.294	1.905	0.057

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Brazilian respondents were set as the reference category (intercept). Significant effects are shaded grey.

Table 21: *P* values of further significant differences regarding respondents' views on whether the regulation of data protection and informational privacy needs adjusting in certain industries.[10]

Contrast		*p*
US	China	0.001**
	Japan	0.009*
Ghana	China	0.007*

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05.

Let us again inspect Brazilian professionals' responses to this item more closely. As shown in Fig. 18, the majority of Brazilian respondents (66 %) advocated to increase the regulation of data protection and informational privacy in certain industries. The most frequently named industry in this respect was the financial sector, mentioned by 30 % of all Brazilian respondents. In contrast, only a minority of 20 % of Brazilian professionals believed that regulation should be weaker in certain industries. The most common industries named in this regard were social media companies and the healthcare sector (5 % each). For both industries, a greater proportion of Brazilian professionals advocated for the stricter regulation of data protection and informational privacy (10 % for the healthcare sector and 18 % for social media).

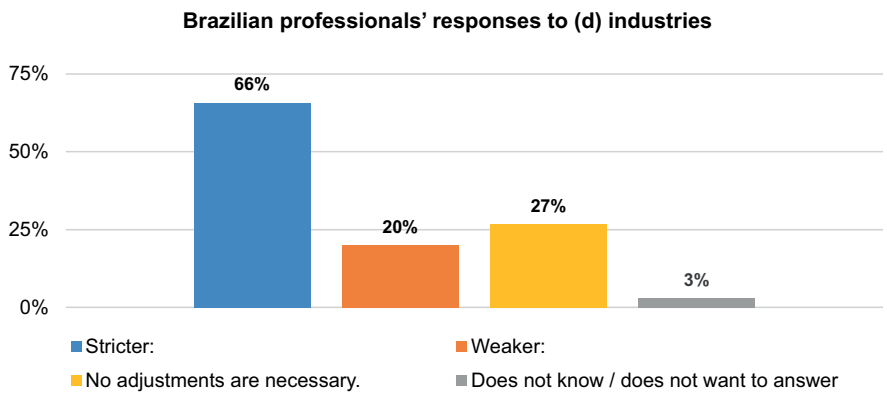

Fig. 18: Brazilian professionals' responses to Q7: Are there certain industries (e.g., healthcare, social media companies, financial sector, etc.) for which you think the regulation of data protection and informational privacy should be …

10 Any *p* values not contained in Table 20 were obtained by running the model again after adjusting the reference category for "country" and then applying Holm's (1979) method to correct for multiple comparisons. This table only contains statistically significant contrasts ($p < 0.05$), i.e., insignificant contrasts are not included.

Regarding US respondents (Fig. 19), a majority of 57 % advocated to increase the regulation of data protection and informational privacy in certain industries. The most frequently named industry in this respect was the financial sector (mentioned by 15 % of all US respondents), closely followed by the healthcare sector (14 %). In contrast, only a minority of 20 % of US professionals believed that regulation should be weaker in certain industries. The most common industries named in this regard were social media companies (6 %) and the healthcare sector (4 %). As for the healthcare sector, a greater proportion of US professionals advocated for the stricter regulation of data protection and informational privacy regarding social media companies (10 %).

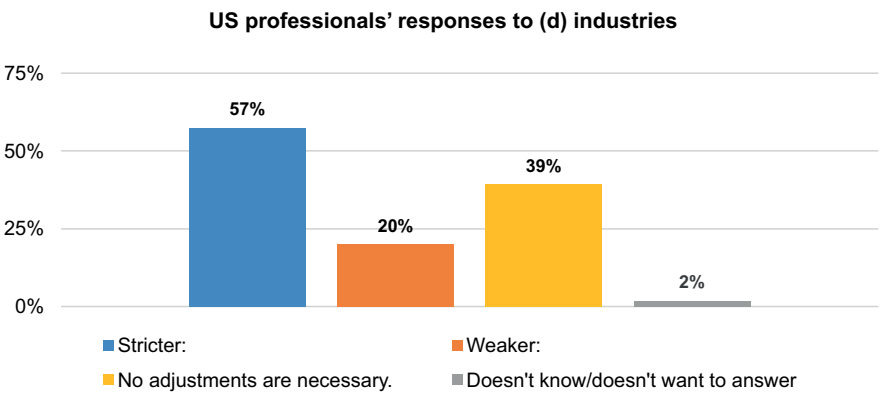

Fig. 19: US professionals' responses to Q7: Are there certain industries (e.g., healthcare, social media companies, financial sector, etc.) for which you think the regulation of data protection and informational privacy should be ...

Moving on to Ghanaian respondents, Fig. 20 shows that a slight majority (54 %) advocated to increase the regulation of data protection and informational privacy in certain industries. The most frequently named industry in this respect was the healthcare sector (mentioned by 18 % of all Ghanaian respondents), closely followed by social media companies (17 %) and the finance sector (16 %). Only a minority of 10 % of Ghanaian professionals believed that regulation should be weaker in certain industries. Respondents again mentioned the healthcare sector, the finance sector, and social media companies, but none of them were named by more than 3.5 %.

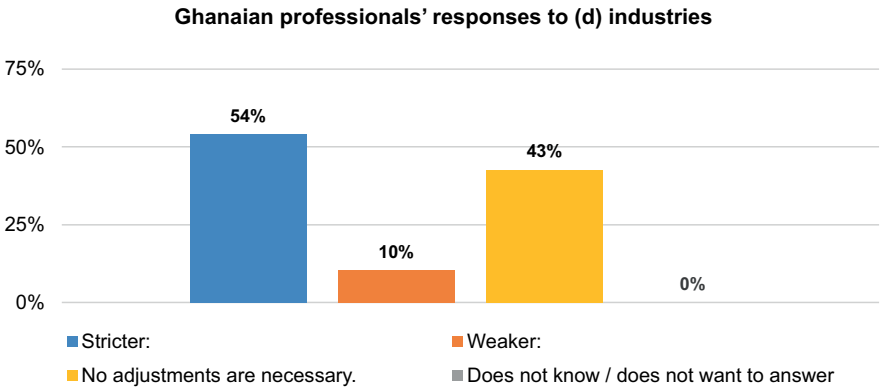

Fig. 20: Ghanaian professionals' responses to Q7: Are there certain industries (e.g., healthcare, social media companies, financial sector, etc.) for which you think the regulation of data protection and informational privacy should be …

1.2.5 High-satisfaction and low-satisfaction countries

Based on respondents' perceptions of whether the regulation of data protection and informational privacy needed adjusting, we clustered the countries into two groups: "high-satisfaction" countries and "low-satisfaction" countries. Brazil is clearly a low-satisfaction country (see Fig. 21): for all four categories surveyed, (a)–(d), a majority of 60–80 % of Brazilian professionals saw a need for adjustment, and they were significantly more likely to do so than those from at least four other countries (China, Germany, Japan, Switzerland, and often also Ghana). The United States also appeared to fall into this group: For all four categories, a majority of 56–65 % of US professionals saw a need for adjustment, and for two categories—(b) contexts of data disclosure and (c) purposes of data collection—they were significantly more likely to do so than half the other countries (China, Germany, and Japan).

Fig. 21: Satisfaction with the regulation of data protection and informational privacy.

By contrast, China clearly fell into the category of high-satisfaction countries: For all four categories surveyed, (a)—(d), a majority of 57–69 % of Chinese professionals were content with the current state of regulation, and for three out of four categories—(a) types of data, (c) purposes of data collection, and (d) industries—they

were significantly more likely to hold this opinion than half the other countries (Brazil, the United States, and Ghana).

The remaining countries—Germany, Ghana, Japan, and Switzerland—were a little more difficult to classify. Ghana was quite similar to the low-satisfaction countries: For three out of the four categories surveyed—(a) types of data, (c) purposes of data collection, and (d) industries)—a majority of 57–59 % of Ghanaian professionals saw a need for adjustment. For (b) contexts of data disclosure, this figure was just under half, at 48 %. However, unlike US and Brazilian respondents, Ghanaian respondents were neither significantly more nor significantly less likely to see a need for adjustment than respondents from most countries on any of the four points. They were significantly more likely to see a need for adjustment than Chinese respondents and significantly less likely to see a need for adjustment than Brazilian respondents in three out of four categories. Ghana is thus best classified as an intermediate case between the low- and high-satisfaction countries, but leaning more toward the low-satisfaction countries.

In Japan and Switzerland, a majority of professionals were content with the current state of regulation in all four categories, though these majorities were noticeably smaller than in China and often amounted to just over 50 % (52–55 % for Switzerland and 51–65 % for Japan). In Germany, a majority of 53–62 % were content with the current state of regulation in three out of four categories; in the fourth, (a) types of data, exactly 50 % held this opinion. Japan, Switzerland, and Germany are thus best classified as intermediate cases between the low- and high-satisfaction countries. Switzerland appears to be a true intermediate case, as Swiss response behavior differed significantly from only Brazilian behavior in all four categories. The same was true of German response behavior in two of the four categories. Regarding the remaining two categories—(b) contexts of data disclosure and (c) purposes of data collection—German professionals were significantly more likely to be content with the current state of regulation than Brazilian and US professionals. Thus, while still an intermediate case, Germany appeared to lean slightly more toward the high-satisfaction countries. Japanese professionals were more likely to be content with current regulations than professionals from two to three other countries (Brazil, the United States, and, in one case, Ghana) in three out of four categories. Regarding the fourth, (a) types of data, Japanese responses only differed significantly from Brazilian ones. Japan thus also appeared to lean more toward the high-satisfaction countries, though it should still primarily be viewed as an intermediate case between the high- and low-satisfaction countries.

1.3 Consumer data protection literacy

We also found significant cross-cultural differences regarding professionals' assessments of how aware people are of data protection and informational privacy regulation in their country, $H(6) = 65.69$, $p < 0.0005$. The United States was the only country where a majority of the professionals surveyed (52 %) believed that consumers in their country were very aware of it. In the other countries, the percentage of respondents who shared this opinion ranged from just 13 % (Japan) to 25 % (Germany) (see Fig. 22 below).

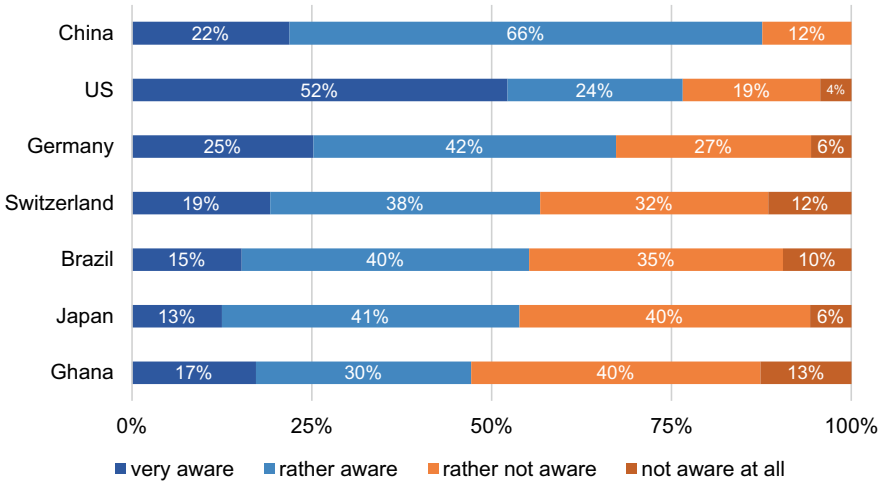

Fig. 22: Q8. In your expert opinion, how aware are consumers of the regulation of data protection and informational privacy in your country?

Accordingly, US professionals assessed people's awareness in this respect as significantly greater than professionals in all other countries except China did ($p < 0.0005$ and $p = 0.009$; see Table 22). All these differences amounted to medium effects (with r ranging from 0.32 to 0.37; see Table 23), except for the one between the United States and Germany, which constituted a small-to-medium effect ($r = 0.23$). Similarly, Chinese respondents rated Chinese consumers' awareness of data protection and informational privacy regulations as significantly higher than Brazilian, Ghanaian, Japanese, and Swiss respondents did regarding consumers in their own countries ($p < 0.0005$ and $p = 0.002$). All these differences were of a medium effect size (with r ranging from 0.31 to 0.35), except for the China-Switzerland comparison, which amounted to a small-to-medium effect ($r = 0.26$).

It is noteworthy that in in all countries except Ghana, the majority of professionals rated people's awareness of the respective legislation in their country as very or rather pronounced. Ghanaian professionals were the only group in which the majority (53 %) said that consumers were rather unaware or not aware at all of the relevant legislation in their country (see Fig. 22, above). However, no significant differences apart from the ones mentioned above could be found.

Table 22: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' assessments of consumers' awareness of data protection and informational privacy regulation in their countries.

	US	China	Germany	Switzerland	Brazil	Japan
China	0.183					
Germany	0.009*	0.469				
Switzerland	< 0.0005***	0.002**	0.554			
Brazil	< 0.0005***	< 0.0005***	0.266	1.000		
Japan	< 0.0005***	< 0.0005***	0.183	1.000	1.000	
Ghana	< 0.0005***	< 0.0005***	0.078	1.000	1.000	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 23: Effect sizes for significant differences in respondents' assessments of consumers' awareness of data protection and informational privacy regulation in their countries.

Contrast		*r*
US	Brazil	0.35
	Germany	0.23
	Ghana	0.37
	Japan	0.37
	Switzerland	0.32
China	Brazil	0.31
	Ghana	0.35
	Japan	0.34
	Switzerland	0.26

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

Significant cross-cultural differences were also found regarding professionals' assessments of whether consumers do enough to protect their personal data, $H(6) = 51.43$, $p < 0.0005$. In all the countries surveyed except for Japan and Switzerland, a

majority of professionals strongly or somewhat agreed that consumers do enough to protect their personal data (see Fig. 23 below). Agreement ranged from 76 % (Chinese respondents) to 53 % (German respondents), though it should be noted that, in Switzerland, slightly less than the majority agreed, at 49 %. At the same time, however, in neither Japan nor Switzerland did the majority think that consumers were not doing enough to protect their data, though it is noteworthy that in Japan, this view was held by almost half of respondents (46 %). At 28 %, the percentage of those who neither agreed nor disagreed with the statement was relatively high compared to the other countries (such as Switzerland, at 21 %; see Fig. 23).

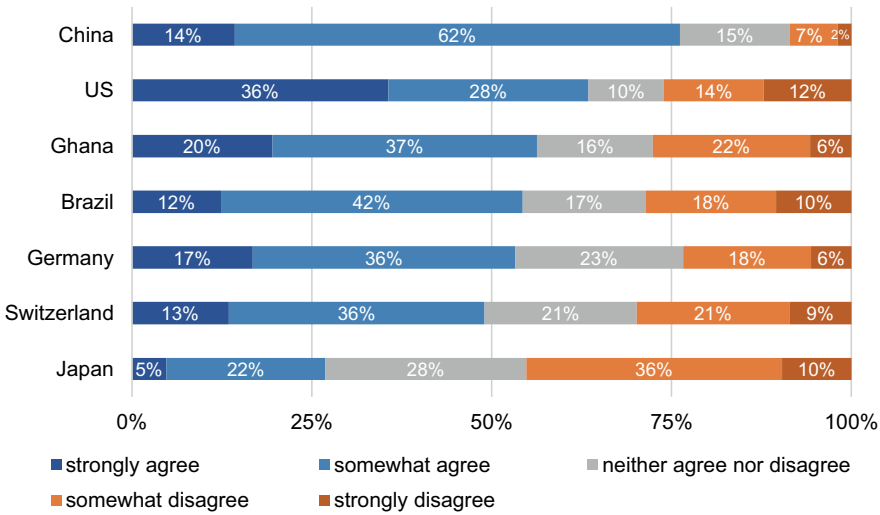

Fig. 23: Q9. In general, consumers do enough to protect their personal data.

Accordingly, pairwise comparisons revealed that Japanese professionals agreed significantly less with the statement that consumers do enough to protect their personal data than professionals in all other countries (with p ranging from < 0.0005 to 0.034; see Table 24, below). The difference between Japanese and Chinese respondents' agreement approached a large effect size (r = 0.49), whereas the difference between Japanese and US respondents amounted to a medium effect size (r = 0.33). The other contrasts constituted small-to-medium effects (see Table 25), though two of them approached a medium effect size (r = 0.29 for Japan-Germany and r = 0.28 for Japan-Ghana). Moreover, Chinese respondents exhibited significantly higher agreement than Swiss respondents (p = 0.006) and Brazilian respondents (p = 0.022), a small-to-medium effect in both cases (r = 0.25, r = 0.22).

Table 24: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' agreement with the statement that consumers do enough to protect their personal data.

	Japan	Switzerland	Brazil	Germany	Ghana	US
Switzerland	0.034*					
Brazil	0.013*	1.000				
Germany	0.001**	1.000	1.000			
Ghana	0.002**	1.000	1.000	1.000		
US	< 0.0005***	0.120	0.161	0.663	1.000	
China	< 0.0005***	0.006*	0.022*	0.120	0.423	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 25: Effect sizes for significant differences in respondents' agreement with the statement that consumers do enough to protect their personal data.

Contrast		*r*
Japan	Brazil	0.23
	China	0.49
	Germany	0.29
	Ghana	0.28
	Switzerland	0.21
	US	0.33
China	Brazil	0.22
	Switzerland	0.25

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

2 Data sensitivity

This chapter presents findings on the perceived sensitivity of various data categories in our seven countries. Respondents were asked to rate 33 data categories on a five-point sensitivity scale (*1 not at all sensitive – 2 not sensitive – 3 neutral – 4 sensitive – 5 very sensitive*). The data categories, mainly taken from the legal frameworks of the seven countries, were:

- religious beliefs
- religious activities
- health data
- genetic information
- biometric information
- sex life

- gender identity
- ethnicity or race
- political views
- political activities
- union membership
- union activity
- membership in a philosophical organization
- philosophical beliefs
- criminal records
- crime victim data
- minors' personal information
- financial data in general
- income
- assets
- social security measures
- location (tracking)
- personal identification numbers
- account logins
- digital signatures
- correspondence records
- content of correspondence
- citizenship or immigrant status
- property information
- social status
- website activity
- browsing history
- diet

To provide a first overview of respondents' tendencies when rating the sensitivity of the different data categories in each country, we computed the mean sensitivity rating for each data category in each country. That is, each country had 33 mean sensitivity ratings, one for each data category. The distribution of these mean sensitivity ratings in each country is summarized in the boxplots in Fig. 24. The boxplots appear in descending order, starting with the country with the highest median of all 33 mean sensitivity ratings (the United States) and ending with the country with the lowest median of all 33 mean sensitivity ratings (Japan).

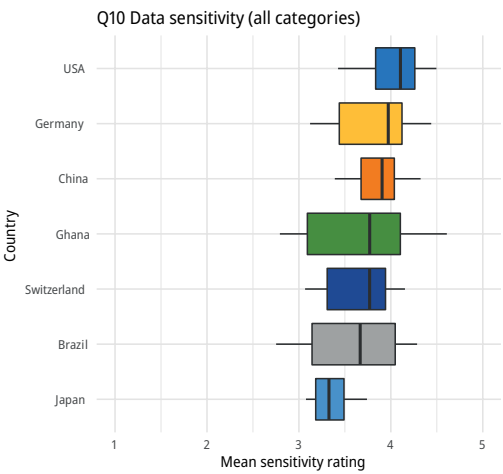

Fig. 24: Boxplots of mean sensitivity ratings for all 33 data categories in the seven countries.

The whiskers of the boxplots indicate the range of mean sensitivity ratings for each country, i.e., the maximum difference between mean sensitivity ratings, which is far greater for some countries than for others. Ghana is the country with the biggest range of mean sensitivity ratings (1.82, from a mean sensitivity rating of 2.79 for "diet" to 4.61 for "account login"), followed by Brazil (1.53), Germany (1.32), Switzerland (1.09), United States (1.07), China (0.93), and Japan (0.66). It is also apparent that the size of the boxes, and thus the interquartile range, differs greatly between countries: Ghana has the largest interquartile range (1.01), followed by Brazil (0.90), Germany (0.68), Switzerland (0.63), the United States (0.43), China (0.36), and Japan (0.31). Thus, both for the range and the interquartile range, the countries follow the same order. Ghana is the country where the mean sensitivity ratings for the 33 categories vary the greatest, followed by Brazil, Germany, Switzerland, the United States, and China. Japan is the country where mean sensitivity ratings vary the least. Based on a visual inspection, it also seems to be the country where sensitivity ratings are overall lower than in several other countries, such as the United States or China.

Let us therefore examine these possible differences more closely. A Kruskal-Wallis test[11] shows that mean sensitivity ratings varied significantly across countries, $H(6) = 53.205$, $p < 0.0001$. Pairwise comparisons show that mean sensitivity ratings were significantly lower in Japan than in the United States, China, Germany, and Switzerland (with p ranging from < 0.0005 to 0.003; see Table 26). Japan's contrast with the United States and China constituted particularly large effects ($r = 0.82$, $r = 0.71$; see also Table 27), while its contrast with Germany also amounted to a large effect ($r = 0.55$), and the contrast with Switzerland approached a large effect size ($r = 0.46$). Moreover, mean sensitivity ratings were significantly greater for the United States than for Switzerland ($p = 0.001$) and Brazil ($p = 0.004$), with the former contrast constituting and the latter one approaching a large effect size ($r = 0.51$, $r = 0.45$). All the other country comparisons yielded non-significant results.

Thus, we can observe two overall, statistically significant trends: While Japanese respondents tended to rate the sensitivity of the examined data categories significantly lower than respondents did in most other countries (the United States, China, Germany, and Switzerland), US respondents tended to rate them significantly higher than respondents did in half the other countries (Japan, Switzerland, and Brazil).

11 This test was used instead of a parametric alternative as most of the datasets were not normally distributed and because the data violated the assumption of the homogeneity of variances.

Table 26: *P* values of pairwise Wilcoxon rank-sum tests regarding mean sensitivity ratings for all 33 data categories in the seven countries.

	Japan	Brazil	Switzerland	Ghana	China	Germany
Brazil	0.482					
Switzerland	0.003**	1.000				
Ghana	0.482	1.000	1.000			
China	< 0.0005***	0.624	0.292	1.000		
Germany	< 0.0005***	0.489	0.412	1.000	1.000	
US	< 0.0005***	0.004**	0.001**	0.103	0.059	0.412

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 27: Effect sizes for significant differences in mean sensitivity ratings for all 33 data categories.

Contrast		*r*
Japan	China	0.71
	Germany	0.55
	Switzerland	0.46
	US	0.82
US	Brazil	0.45
	Switzerland	0.51

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

3 Data power of companies and governments

The survey items presented in this section were designed to establish

- what general rules should ideally apply to the collection of personal data by companies according to professionals;
- whether professionals trust different industries and domestic and foreign governments to use consumers' personal data correctly; and
- whether they think that
  - the protection of consumer data in the context of collection and use by companies and governments is adequately ensured;

  and whether
  - the data protection provisions are observed and enforced by companies; or
  - improvements need to be made in these respects.

3.1 Responsibilities of companies when collecting consumer data

Professionals in the field of data protection in our seven selected countries were first asked about the extent to which they agreed or disagreed with the following statements on the data collection practices of companies:

- "Companies should only be allowed to collect consumers' personal data with their consent."
- "Companies should always be required to provide deletion options for personal data so that consumers can delete their personal data at any time should they change their mind about the disclosure."
- "Companies should always be required to state explicitly what consumers' personal data will be used for."
- "Companies should always be required to ask again for consumers' consent when using their data for purposes other than previously stated."

As can be seen in Fig. 25 below, a majority of Ghanaian (89 %), Brazilian (79 %), US (66 %), and Chinese (55 %) professionals *strongly* agreed that companies should only be permitted to collect personal data with consumers' consent. A large majority in all countries showed some or strong agreement with this statement. These results can be interpreted as a strong professional response in favor of companies in Ghana, Brazil, the United States, and China always obtaining consumers' consent before collecting their personal data, and a more moderate response in this respect for the rest of the countries.

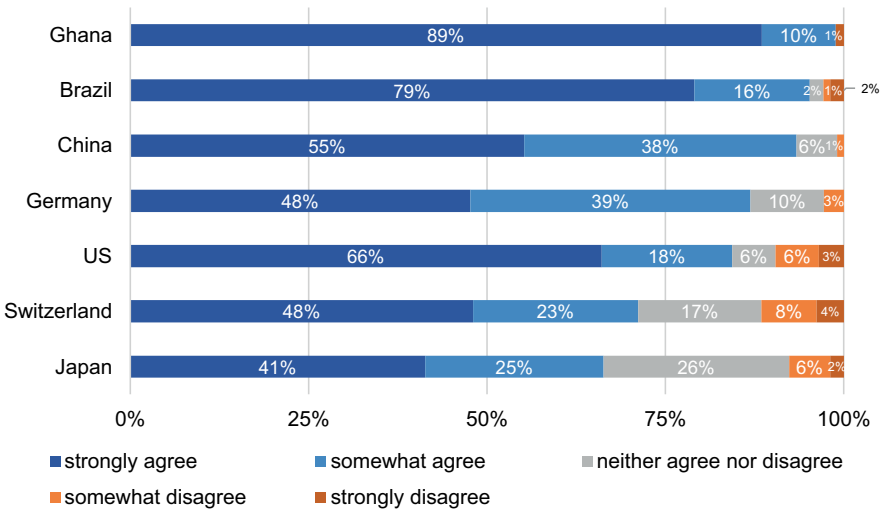

Fig. 25: Q11r1. Companies should only be allowed to collect consumers' personal data with their consent.

There were, however, significant cross-cultural differences in the strength of respondents' agreement with the statement (see Fig. 25), $H(6) = 81.62$, $p < 0.0005$. Pairwise comparisons reveal that Ghanaian respondents agreed significantly more with the statement than respondents in all other countries ($p < 0.0005$ and $p = 0.002$; see Table 28) except for Brazil ($p = 0.367$). The contrast between Japan and Ghana amounted to a large effect ($r = 0.50$) and the contrasts Ghana-Germany and Ghana-Switzerland amounted to medium-to-large effects ($r = 0.43$, $r = 0.44$; see also Table 29). The comparison with China constituted a medium effect ($r = 0.36$) and with the United States a small-to-medium effect ($r = 0.27$). Moreover, Brazilian respondents' agreement was significantly greater than that of Chinese, German, Swiss, and Japanese respondents ($p < 0.0005$ and $p = 0.006$). The difference between Brazil and Japan amounted to a medium-to-large effect ($r = 0.41$), the contrasts Brazil-Germany and Brazil-Switzerland amounted to medium effects ($r = 0.32$, $r = 0.34$), and the contrast Brazil-China amounted to a small-to-medium effect ($r = 0.24$). Further significant, small-to-medium effects were found regarding Japan and two other countries: Japanese respondents agreed significantly less with the statement than US respondents ($p = 0.006$, $r = 0.24$) and Chinese respondents ($p = 0.007$, $r = 0.24$).

Table 28: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' agreement with the statement that companies should only be allowed to collect consumers' personal data with their consent.

	Ghana	Brazil	US	China	Germany	Switzerland
Brazil	0.367					
US	0.002**	0.160				
China	< 0.0005***	0.006*	0.821			
Germany	< 0.0005***	< 0.0005***	0.279	0.645		
Switzerland	< 0.0005***	< 0.0005***	0.076	0.160	0.717	
Japan	< 0.0005***	< 0.0005***	0.006*	0.007*	0.195	0.822

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 29: Effect sizes for significant differences in respondents' agreement with the statement that companies should only be allowed to collect consumers' personal data with their consent.

Contrast		*r*
Ghana	China	0.36
	Germany	0.43
	Japan	0.50
	Switzerland	0.44
	US	0.27
Brazil	China	0.24
	Germany	0.32
	Japan	0.41
	Switzerland	0.34
Japan	China	0.24
	US	0.24

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

Moving on to the second statement, we found that an overwhelming majority of professionals in all countries strongly or somewhat agreed that companies should always be required to provide deletion options so that consumers can delete their personal data at any time if they change their minds about disclosure. However, we again found significant cross-cultural differences in the strength of respondents' agreement, $H(6) = 72.99$, $p < 0.0005$. As can be seen in Fig. 26 below, Ghana stood out in that as many as 84 % of professionals believed strongly that companies should always be required to provide deletion options, followed by Brazilian (75 % strong agreement) and US professionals (58 % strongly agree). Thus, we see strong responses from professionals in Ghana, Brazil, and the United States for regular deletion options and more moderate responses in the other countries.

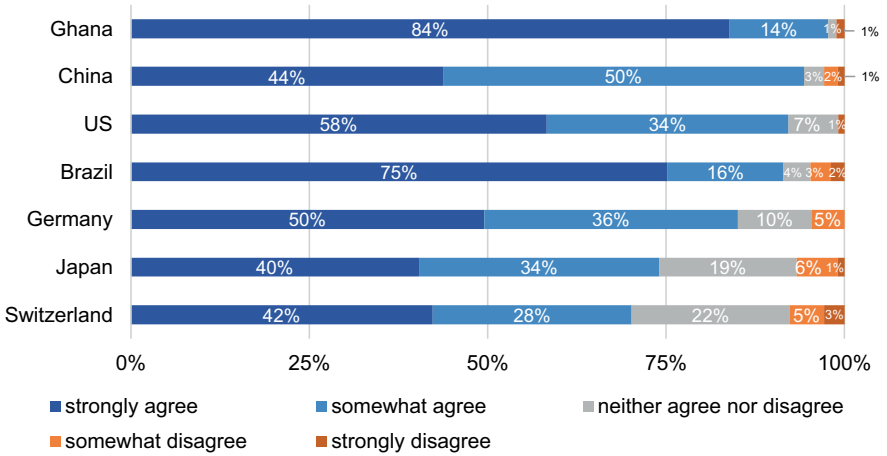

Fig. 26: Q11r2. Companies should always be required to provide deletion options for personal data so that consumers can delete their personal data at any time should they change their mind about the disclosure.

Looking at pairwise comparisons, we found that Ghanaian professionals' agreement was significantly stronger than that of respondents in all other countries ($p < 0.0005$ and $p = 0.001$), except for Brazil ($p = 0.478$). Brazilian respondents agreed significantly more with the statement than respondents in Japan, Switzerland, China, and Germany (with p ranging from = < 0.0005 to 0.004; see Table 30). Most of these differences amounted to medium effects (with r ranging from 0.34 to 0.40; see Table 31). The contrasts Ghana-Japan and Ghana-Switzerland, however, amounted to medium-to-large effects ($r = 0.45$, $r = 0.44$). All remaining contrasts were small-to-medium effects (with r ranging from 0.25 to 0.28; see Table 31). Furthermore, US respondents were found to agree significantly more with the statement than Japanese and Swiss respondents, two more small-to-medium effects ($p = 0.008$ and $r = 0.23$ each).

Table 30: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' agreement with the statement that companies should always be required to provide deletion options for personal data so that consumers can delete their personal data at any time should they change their mind about the disclosure.

	Ghana	Brazil	US	China	Germany	Japan
Brazil	0.478					
US	0.001**	0.204				
China	< 0.0005***	0.001**	0.478			
Germany	< 0.0005***	0.004**	0.478	1.000		
Japan	< 0.0005***	< 0.0005***	0.008*	0.449	0.478	
Switzerland	< 0.0005***	< 0.0005***	0.008*	0.449	0.478	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 31: Effect sizes for significant differences in respondents' agreement with the statement that companies should always be required to provide deletion options for personal data so that consumers can delete their personal data at any time should they change their mind about the disclosure.

Contrast		*r*
Ghana	China	0.40
	Germany	0.36
	Japan	0.45
	Switzerland	0.44
	US	0.27
Brazil	China	0.28
	Germany	0.25
	Japan	0.34
	Switzerland	0.34
US	Japan	0.23
	Switzerland	0.23

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

Professionals from all countries surveyed also strongly or somewhat agreed that companies should always be required to explicitly state what consumers' personal data will be used for, i.e., they advocated for transparent communication in this respect. As shown in Fig. 27, Ghanaian professionals emphasized this most clearly, with 87 % strongly agreeing, followed by Brazilian (74 %), US (65 %), and Chinese professionals (54 %). Thus, we can derive a strong vote from professionals in Ghana,

Brazil, the United States, and China for transparent corporate communication with regard to data use, and a more moderate response in the other countries.

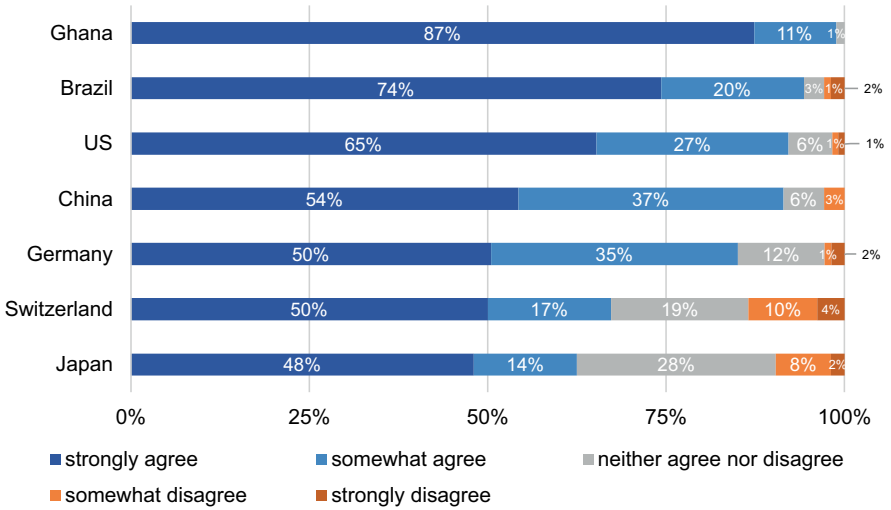

Fig. 27: Q11r3. Companies should always be required to state explicitly what consumers' personal data will be used for.

We again found significant differences in the strength of professionals' agreement with the statement, $H(6) = 67.33$, $p < 0.0005$. Ghanaian professionals agreed significantly more with the statement than respondents in all other countries ($p < 0.0005$ and $p = 0.004$) except for Brazil ($p = 0.172$). Whereas the contrasts with Japan and Switzerland amounted to medium-to-large effects ($r = 0.45$, $r = 0.42$), the contrasts with Germany and China constituted medium effects ($r = 0.40$, $r = 0.36$) and the contrast with the United States a small-to-medium effect ($r = 0.26$). Moreover, Brazilian respondents' agreement with the statement was significantly greater than that of Japanese, Swiss, German, and Chinese respondents (with p ranging from < 0.0005 to 0.043; see Table 32). US respondents also agreed significantly more with the statement than Japanese and Swiss respondents ($p = 0.003$ and $p = 0.011$ respectively). These differences mostly amounted to small-to-medium effects (with r ranging from 0.22 to 0.29; see Table 33), except for the Brazil-Japan contrast, which constituted a medium effect ($r = 0.32$), and the Brazil-China contrast, which constituted a small effect ($r = 0.20$).

Table 32: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' agreement with the statement that companies should always be required to explicitly state what consumers' personal data will be used for.

	Ghana	Brazil	US	China	Germany	Japan
Brazil	0.172					
US	0.004**	0.627				
China	< 0.0005***	0.043*	0.627			
Germany	< 0.0005***	0.004**	0.172	0.762		
Japan	< 0.0005***	< 0.0005***	0.003**	0.110	0.410	
Switzerland	< 0.0005***	< 0.0005***	0.011*	0.259	0.627	0.823

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 33: Effect sizes for significant differences in respondents' agreement with the statement that companies should always be required to explicitly state what consumers' personal data will be used for.

Contrast		*r*
Ghana	China	0.36
	Germany	0.40
	Japan	0.45
	Switzerland	0.42
	US	0.26
Brazil	China	0.20
	Germany	0.25
	Japan	0.32
	Switzerland	0.29
US	Japan	0.25
	Switzerland	0.22

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

Moving on to the last question, we found that, once again, a majority of professionals in all countries strongly or somewhat agreed that companies should always be required to obtain consent from consumers again when using their data for purposes other than those previously stated. Despite this general trend, we once more found significant cross-cultural differences regarding respondents' agreement, $H(6) = 81.95$, $p < 0.0005$. As shown in Fig. 28, Ghana stood out once more in that as many as 89 % of professionals strongly believed in repeatedly obtaining consu-

mer consent, followed by Brazilian (74 %) and US professionals (52 %). These results indicate a strong vote from professionals in Ghana, Brazil, and the United States for repeatedly obtaining consent from consumers if the purpose of using their data should differ from the one originally stated, and a more moderate response in the other countries.

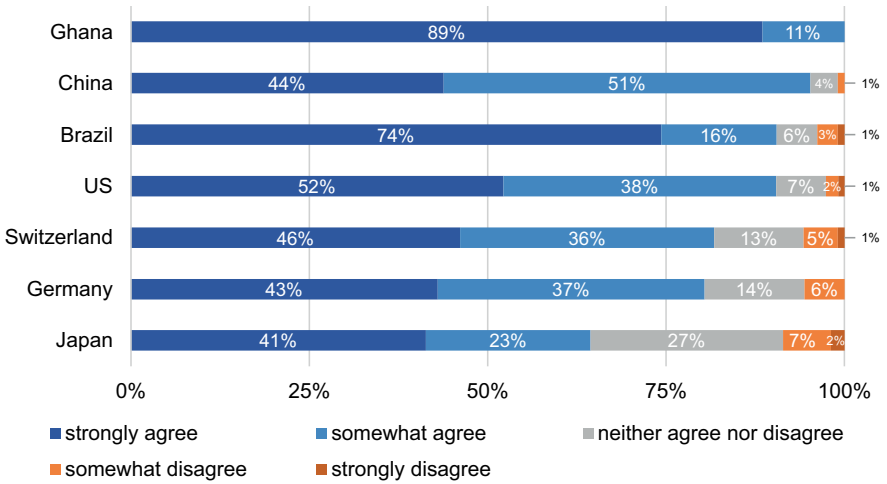

Fig. 28: Q11r4. Companies should always be required to ask again for consumers' consent when using their data for purposes other than previously stated.

Looking at pairwise comparisons, we see the same pattern that we have already observed in the previous three questionnaire items: Ghanaian respondents' agreement was significantly greater than that of respondents in all other countries ($p < 0.0005$ each) except for Brazil ($p = 0.079$). This time, these differences mostly approached or constituted a large effect size (with r ranging from 0.46 to 0.51; see Table 35), except for the Ghana-United States contrast, which was a medium effect ($r = 0.39$). Moreover, Brazilian respondents once again agreed significantly more with the statement than respondents in Japan, Germany, Switzerland, and China, and—this time—significantly more than respondents in the United States as well (with p ranging from < 0.0005 to 0.032; see Table 34). In addition, US respondents' agreement was significantly greater than that of Japanese respondents ($p = 0.028$). These differences were mostly small-to-medium in size (with r ranging from 0.21 to 0.27; see Table 35), though the contrasts Brazil-Japan and Brazil-Germany each amounted to medium effects ($r = 0.35$, $r = 0.30$). By contrast, the difference between Brazilian and US respondents' agreement merely constituted a small effect ($r = 0.20$).

Table 34: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' agreement with the statement that companies should always be required to request consumers' consent once more when using their data for purposes other than those previously stated.

	Ghana	Brazil	US	China	Switzerland	Germany
Brazil	0.079					
US	< 0.0005***	0.032*				
China	< 0.0005***	0.002**	1.000			
Switzerland	< 0.0005***	0.001**	1.000	1.000		
Germany	< 0.0005***	< 0.0005***	0.525	1.000	1.000	
Japan	< 0.0005***	< 0.0005***	0.028*	0.079	0.629	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 35: Effect sizes for significant differences in respondents' agreement with the statement that companies should always be required to request consumers' consent once more when using their data for purposes other than those previously stated.

Contrast		*r*
Ghana	China	0.47
	Germany	0.48
	Japan	0.51
	Switzerland	0.46
	US	0.39
Brazil	China	0.26
	Germany	0.30
	Japan	0.35
	Switzerland	0.27
	US	0.20
US	Japan	0.21

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

3.2 Trust in different institutions regarding the correct use of consumer data

Respondents were also asked to what extent, if any, they trusted nine institutions to use consumers' personal data in the right way, using a four-point scale (*a great deal – a fair amount – rather little – not at all*). These included the following seven industries, as well as "the national government" and "foreign governments":

- healthcare providers
- financial services companies
- shipping/delivery companies
- telecommunications companies
- retailers selling goods and services
- search and social media sites
- media companies

3.2.1 Trust in different industries and domestic and foreign governments

In all seven countries, we found significant differences ($p < 0.0005$ and $p = 0.002$) in respondents' trust in the seven industries to use consumers' personal data correctly (for details, see Table 40 in 3.2.3, p. 69). We will first consider the industries that respondents in the seven countries perceived to be particularly trustworthy, before considering those that were considered less trustworthy. Fig. 29 (a)–(g) on p. 56 renders the results of respondents' trust ratings for each country. The nine different institutions are listed in descending order according to the combined percentage of respondents who expressed *a great deal* or *a fair amount* of trust in them to correctly use consumer data. The seven industries are ranked according to this percentage (from 1 for the highest to 7 for the lowest). If the percentage was the same for two industries, the one with the lower percentage for *a great deal* is ranked lower.

Fig. 29 (a)–(g) shows that, of all seven industries, healthcare providers were trusted the most in all seven countries[12] to correctly use consumer's personal data. Moreover, as can be seen in Fig. 30 on p. 57, a majority of professionals in *all* countries trusted[13] them to handle personal consumer data correctly. Their special status in almost all countries was supported by statistical tests: In Japan, healthcare providers were trusted significantly more than any of the other six industries (see Table 45

12 When using expressions such as "trusted the most" or discussing the ranking of industries and governments in terms of trust, we are referring to the combined percentage of respondents who opted for *a great deal* or *a fair amount*.

13 That is, respondents trusted them either *a great deal* or *a fair amount*.

in 3.2.3, p. 71[14]). In all other countries except China, healthcare providers were trusted significantly more than five of the remaining industries (see Table 41, p. 69; Table 43, p. 70; Table 44, p. 71; Table 46, p. 72; and Table 47, p. 72). The odd one out was always financial services companies, which did not differ significantly from healthcare providers in terms of trustworthiness. China was the only country where healthcare providers significantly surpassed only two other industries in terms of trustworthiness (retailers and media companies; see Table 42, p. 70).

Moreover, it is noteworthy that in all countries with the exception of China, healthcare providers were trusted more than the national government (see also Fig. 29). This difference is statistically significant for Brazil ($p = 0.001$, $r = -0.26$; see also Table 36, Table 37), Ghana ($p < 0.0005$, $r = -0.32$), Japan ($p < 0.0005$, $r = -0.32$), and the United States ($p = 0.001$, $r = -0.23$). By contrast, in China, healthcare providers were trusted significantly less than the national government ($p < 0.0005$, $r = -0.34$), although there, too, healthcare was the industry that was trusted the most in terms of the combined percentage of respondents who opted for *a great deal* and *a fair amount* of trust. This is because almost half of Chinese respondents (49 %) expressed strong trust (i.e., *a great deal*) in their national government.

14 The tables containing the *p* values for the comparisons of the seven industries for each country as well as those containing the *p* values for the comparisons of the seven countries for each industry can be found at the end of this section (3.2.3.). This is because, at several points in this section, we refer to multiple such tables at once, and including them as usual in the running text would unnecessarily disrupt the flow of the text.

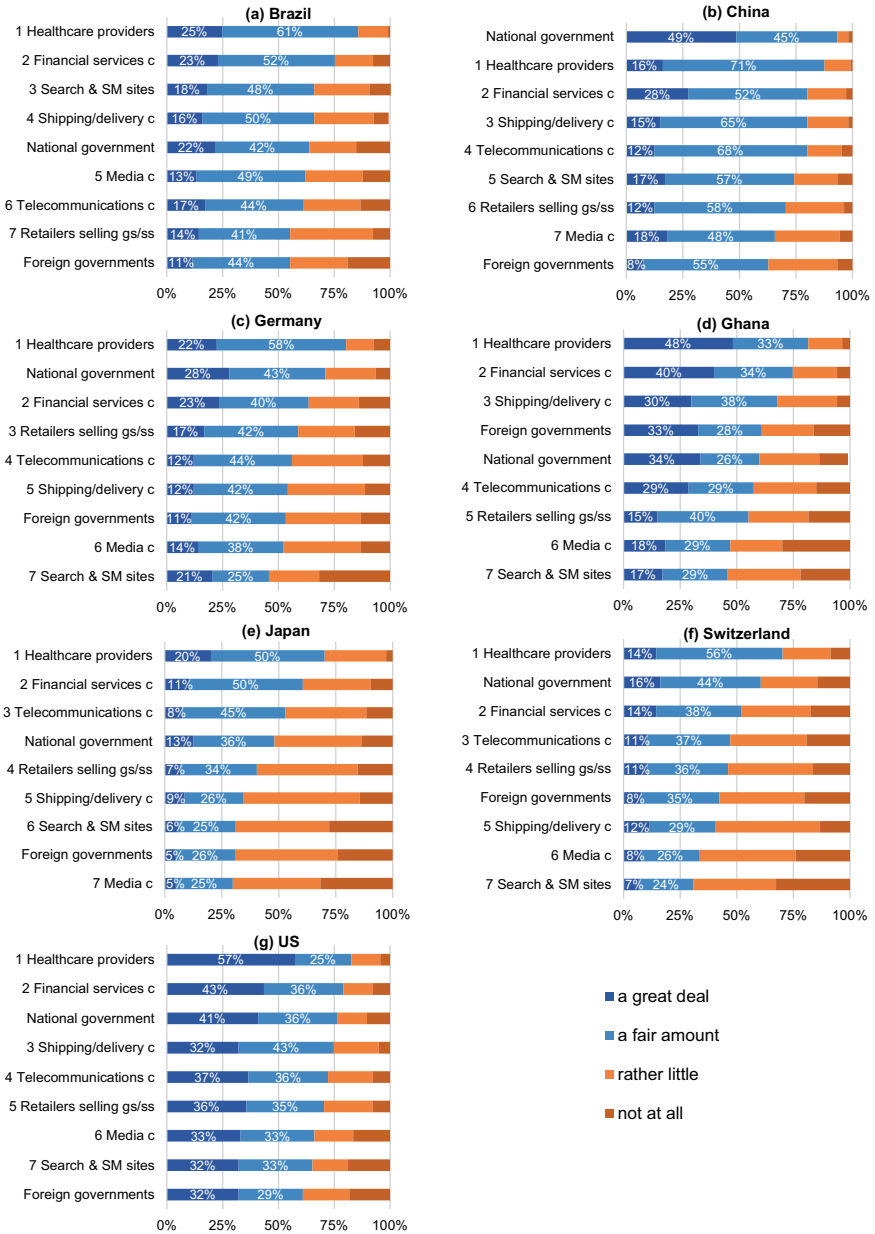

Fig. 29: Brazilian (a), Chinese (b), German (c), Ghanaian (d), Japanese (e), Swiss (f), and US (g) professionals' trust in nine institutions to use consumers' personal data correctly.

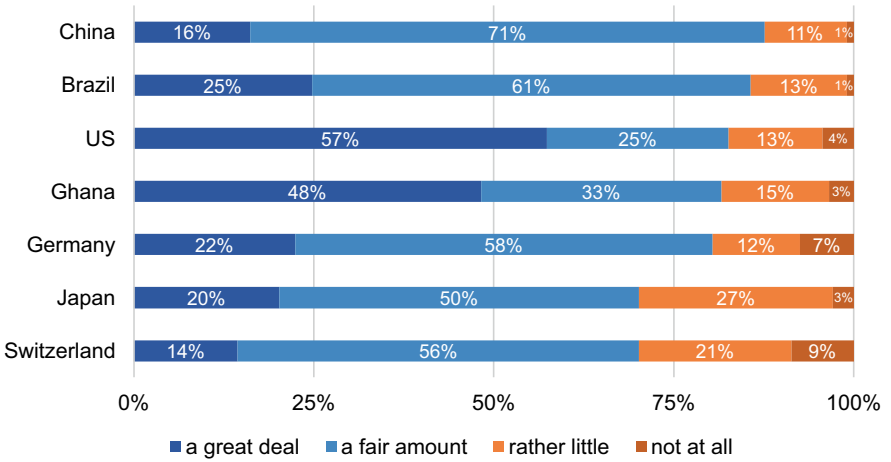

Fig. 30: Q12. Healthcare providers: To what extent, if at all, do you trust the following institutions to use consumers' personal data in the right way?

Table 36: *P* values of pairwise Wilcoxon signed rank tests regarding respondents' trust in the national government vs. healthcare providers to use consumers' personal data correctly.

	p
Brazil	0.001**
China	< 0.0005***
Germany	0.677
Ghana	< 0.0005***
Japan	< 0.0005***
Switzerland	0.271
US	0.001**

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 37: Effect sizes for significant differences in trust in the *national government* and *healthcare providers* to use consumers' personal data correctly.

	r
Brazil	-0.26
China	-0.34
Ghana	-0.32
Japan	-0.32
US	-0.23

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

Fig. 29 also shows that, in all countries, financial services companies followed in second place in terms of trust, at least when national and foreign governments are excluded.[15] Moreover, in all countries, they were trusted by a majority of respondents (see Fig. 31). However, in most countries (Brazil, China, Germany, Switzerland, and the United States), significant differences in trust ratings could only be found between one or two industries and financial services companies (for *p* values, see Table 41–Table 43, Table 46, and Table 47). In Japan and Ghana, financial services companies were considered significantly more trustworthy than four out of six industries (media companies, search and social media sites, shipping/delivery companies, and retailers in Japan; and search and social media sites, media companies, retailers, and telecommunications companies in Ghana; for *p* values, see Table 44 and Table 45).

15 In Switzerland and Germany, the national government ranked between healthcare providers and financial services companies in terms of trust.

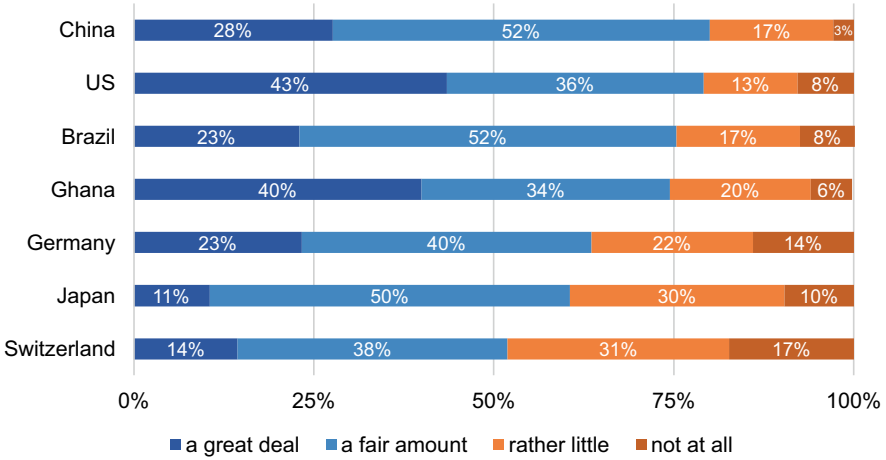

Fig. 31: Q12. Financial services companies: To what extent, if at all, do you trust the following institutions to use consumers' personal data in the right way?

Media companies and search and social media sites were typically "bottom of the barrel" according to the professionals' assessments: They were considered the least trustworthy of all industries in the United States, Germany, Switzerland, Japan, and Ghana. In China, media companies were trusted the least, but search and social media sites were trusted more than retailers. In Brazil, both occupied the middle ground in terms of trust. While media companies were trusted by a majority of professionals in most countries (the United States, China, Brazil, and Germany; see Fig. 32), search and social media sites were only trusted by a majority of professionals in China, Brazil, and the United States (see Fig. 33). Looking at significant differences, we see that, in most cases (Brazil, China, Germany, and the United States for both industries; Switzerland for media companies), the trust ratings for these two industries were significantly lower than those for only two other industries at most (healthcare providers, or healthcare providers and financial services companies; for p values, see Table 41–Table 43, Table 46, and Table 47). In China, search and social media sites did not differ significantly from any other industry in terms of trust ratings (see Table 42). However, in Japan and Ghana, both media companies and search and social media sites received significantly lower trust ratings than four to five out of the six remaining industries (see Table 44 and Table 45). In Switzerland, search and social media sites were trusted significantly less than five out of the six remaining industries (see Table 46).

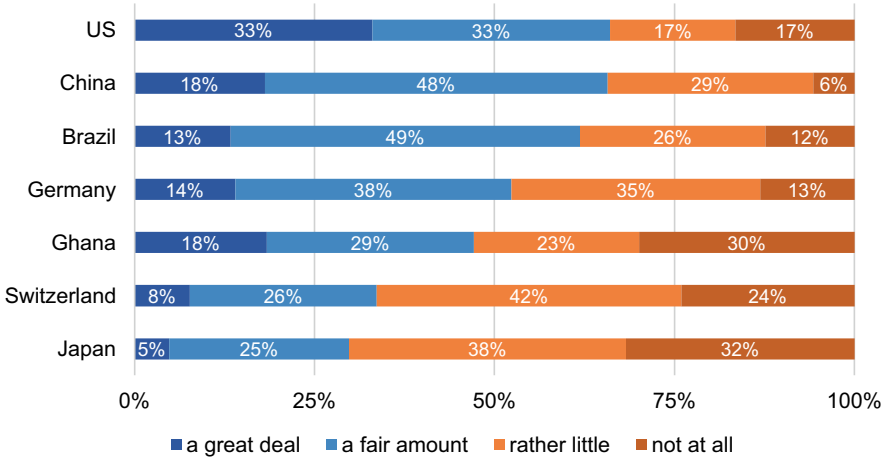

Fig. 32: Q12. Media companies: To what extent, if at all, do you trust the following institutions to use consumers' personal data in the right way?

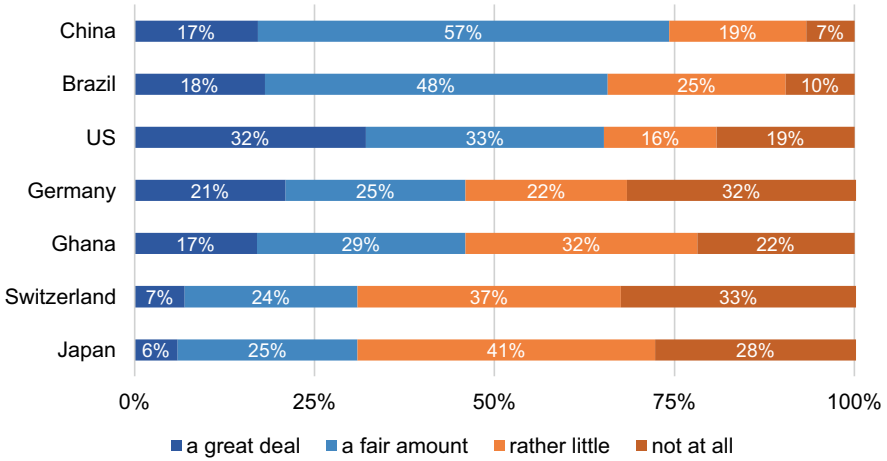

Fig. 33: Q12. Search and social media sites: To what extent, if at all, do you trust the following institutions to use consumers' personal data in the right way?

The industry midfield (i.e., positions three through five) is predominantly occupied by telecommunications companies, shipping/delivery companies, and retailers. Telecommunications companies placed third in Switzerland and Japan, fourth in the United States, Germany, China, and Ghana, and sixth in Brazil. As can be seen in Fig. 34, a majority of professionals in all countries but Switzerland trusted telecommunications companies to use consumers' personal data correctly. In terms of sig-

nificant differences, they received significantly higher or significantly lower trust ratings than two industries at the most in all countries but Japan (for p values, see Table 41–Table 44, Table 46, and Table 47). In Japan, they received significantly lower ratings than healthcare providers ($p < 0.0005$) and significantly higher ratings than shipping/delivery companies ($p = 0.030$), search and social media sites ($p < 0.0005$), and media companies ($p < 0.0005$).

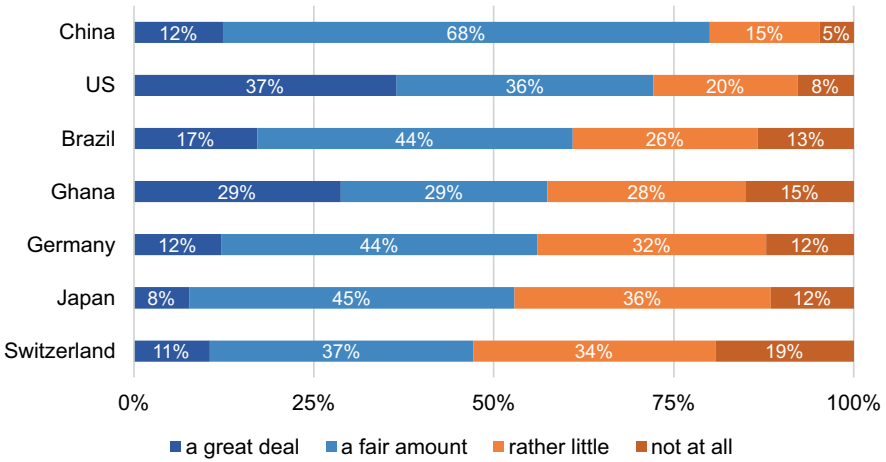

Fig. 34: Q12. Telecommunications companies: To what extent, if at all, do you trust the following institutions to use consumers' personal data in the right way?

Shipping/delivery companies ranked third in the United States, China, and Ghana; fourth in Brazil; and fifth in Germany, Switzerland, and Japan. Fig. 35 shows that a majority of professionals in all countries except for Japan and Switzerland trusted shipping/delivery companies to use consumers' personal data correctly. In most countries (the United States, Germany, Switzerland, China, and Brazil), they received significantly higher or significantly lower trust ratings than one industry at most (for p values, see Table 41–Table 43, Table 46, and Table 47). In Japan, three industries were trusted to a significantly greater extent (healthcare providers, financial service companies, and telecommunications companies) and one to a significantly lesser extent (media companies; for p values, see Table 45). By contrast, in Ghana, three industries were trusted to a significantly lesser extent (retailers, media companies, and search and social media sites) and one to a significantly greater extent (healthcare providers; for p values, see Table 44).

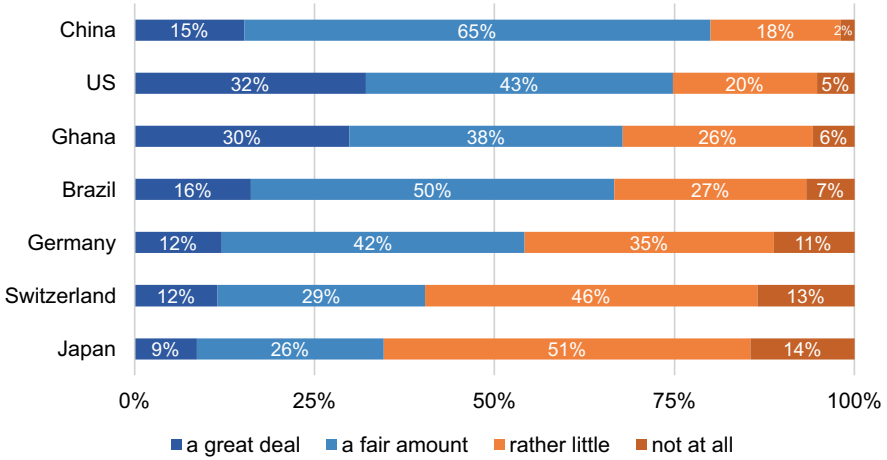

Fig. 35: Q12. Shipping/delivery companies: To what extent, if at all, do you trust the following institutions to use consumers' personal data in the right way?

Retailer rankings varied widely across countries: They ranked third in Germany, fourth in Switzerland and Japan, fifth in the United States and Ghana, sixth in China, and seventh in Brazil. They were trusted by a majority of respondents in all countries except Japan and Switzerland to correctly handle consumers' personal data (Fig. 36). In all countries but Ghana, they received significantly lower trust ratings than one or two industries (healthcare providers and sometimes also financial services companies; for *p* values, see Table 41–Table 43 and Table 45–Table 47). In Ghana, three industries (healthcare providers, financial services companies, and shipping/delivery companies) were trusted significantly more than retailers (for *p* values, see Table 44). In Switzerland and Japan, they significantly surpassed one or two industries in terms of trust (see Table 45, Table 46).

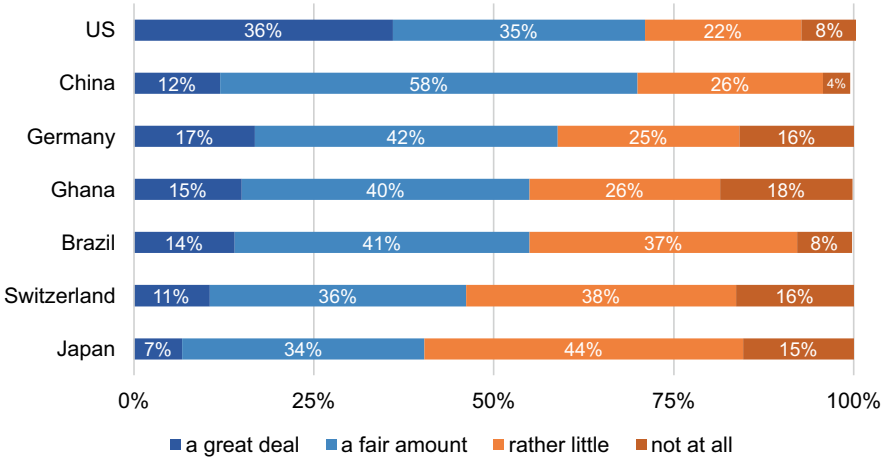

Fig. 36: Q12. Retailers selling goods and services: To what extent, if at all, do you trust the following institutions to use consumers' personal data in the right way?

Regarding trust in governments to use data correctly, we found that national governments were trusted by a majority of respondents in all countries but Japan (where the national government was trusted by just under half of respondents, at 49 %; see Fig. 37). It is noteworthy that this majority was exceptionally large in China (94 %). Further examining this difference in trust using the entire range of the scale, we found statistically significant cross-cultural differences in respondents' trust in the national government to use consumers' personal data correctly, $H(6) = 71.13$, $p < 0.0005$. Chinese respondents had significantly more trust than respondents in all other countries (with p ranging from < 0.0005 to 0.002; see Table 56), except those in the United States ($p = 0.253$). Furthermore, US respondents' trust in their national government was significantly higher than that of Japanese, Swiss, and Brazilian respondents (with p ranging from < 0.0005 to 0.043; see Table 56). Japanese respondents' trust ratings were also significantly lower than those given by German respondents ($p = 0.003$).

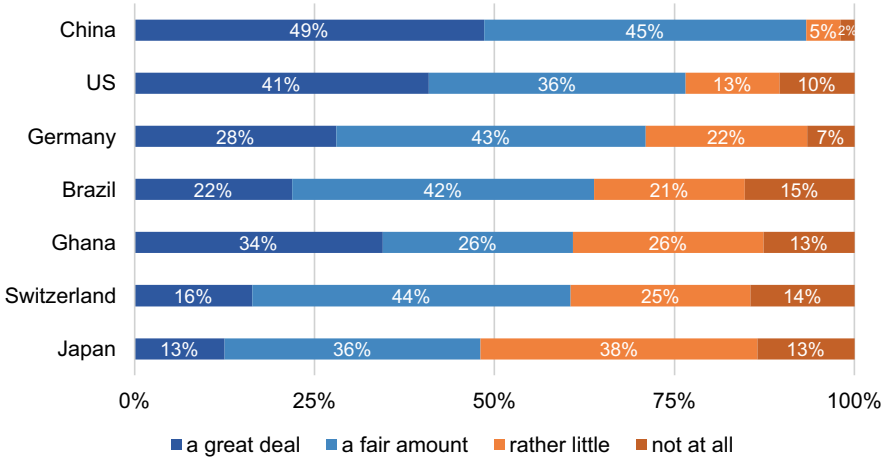

Fig. 37: Q12. The national government: To what extent, if at all, do you trust the following institutions to use consumers' personal data in the right way?

Furthermore, foreign governments were trusted by a majority in all countries but Switzerland and Japan (see Fig. 38). Here, too, we found statistically significant cross-cultural differences in respondents' trust in foreign governments to use consumers' personal data correctly, $H(6) = 40.82$, $p < 0.0005$. Japanese respondents had significantly less trust in foreign governments in this respect than respondents in all other countries (with p ranging from < 0.0005 to 0.012; see Table 57) except Switzerland ($p = 0.966$). Moreover, Swiss respondents' trust ratings for foreign governments were significantly lower than those of Ghanaian, US, and Chinese respondents ($p = 0.017$ and $p = 0.037$).

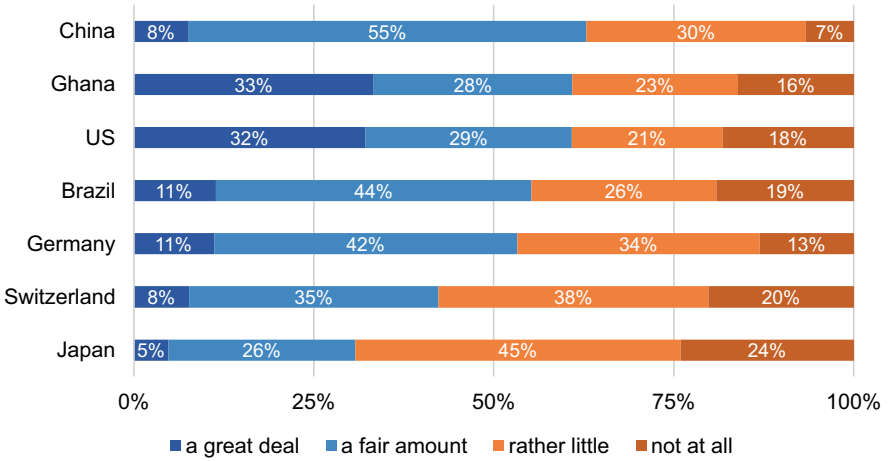

Fig. 38: Q12. Foreign governments: To what extent, if at all, do you trust the following institutions to use consumers' personal data in the right way?

The national government was always trusted more to use personal data correctly than foreign governments, with the exception of Ghana, where both were trusted to roughly the same degree.[16] This difference was considerable in most countries (United States: 16 %; Germany: 18 %; Switzerland: 17 %; Japan: 18 %), and particularly so in China (31 %), with the exception of Brazil (9 %). Examining this difference in trust further using the entire range of the scale, we found that respondents trusted foreign governments significantly less than the national government in all countries (with p ranging from < 0.0005 to 0.007; see Table 38)[17] except for Ghana (p = 0.560). This difference in trust was greatest in China, where it approached a large effect size (r = -0.45). In Germany and Japan, it amounted to or approached a medium effect size (r = -0.30, r = -0.29). In the remaining countries, it amounted to a small-to-medium effect (see Table 39).

16 The combined percentage of Ghanaian respondents who opted for *a great deal* or *a fair amount* was 61 % for foreign governments and 60 % for the national government, though it should be noted that the proportion of Ghanaian respondents who chose the stronger option, *a great deal*, was slightly higher for the national government than for foreign governments (34 % vs. 33 %).

17 *P* values were adjusted using Holm's (1979) method to correct for multiple comparisons.

Table 38: *P* values of pairwise Wilcoxon signed rank tests regarding respondents' trust in the national government vs. their trust in foreign governments to use consumers' personal data correctly.

	p
Brazil	0.006*
China	< 0.0005***
Germany	< 0.0005***
Ghana	0.566
Japan	< 0.0005***
Switzerland	0.007*
US	0.002**

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 39: Effect sizes for significant differences in trust in the national government and foreign governments to use consumers' personal data correctly.

	r
Brazil	-0.21
China	-0.45
Germany	-0.30
Japan	-0.29
Switzerland	-0.20
US	-0.23

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

3.2.2 High-trust and low-trust countries

We found significant differences ($p < 0.0005$) between the seven countries regarding respondents' trust in each of the seven industries to use consumers' personal data correctly (for details, see Table 48 in 3.2.3). Let us now consider these differences more closely. We were able to cluster countries into two different groups, "high-trust" countries on the one hand and "low-trust" countries on the other hand. The United States, China, and Brazil are high-trust countries (see Fig. 39 below): Here, *all* seven industries were trusted by a majority of the population to use consumers' personal data in the right way (at least 65 % in the United States, at least 66 % in China, and at least 55 % in Brazil). In the low-trust countries Japan and Switzerland, most industries were trusted by a minority only, i.e., by less than 50 % of respondents. In

Switzerland, only healthcare providers and financial services companies and, in Japan, only healthcare providers, financial service companies, and telecommunications companies were trusted by over 50 % of respondents.

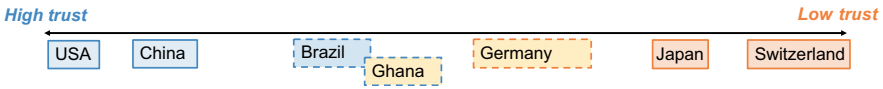

Fig. 39: Scale of trust regarding the correct use of consumers' personal data.

The classification of Japan and Switzerland in the same trust-rating category is supported by the fact that Japanese and Swiss respondents' ratings for each of the seven industries did not differ significantly (for p values, see Table 49–Table 55). Likewise, their classification as low-trust countries compared to the United States and China is supported by the fact that both countries had significantly lower trust ratings than the United States for all industries and significantly lower trust ratings than China for six out of seven industries (the exception being healthcare providers). Brazil's status as a high-trust country vis-à-vis Switzerland is supported by the fact that Swiss trust ratings were significantly lower than Brazilian ratings for five out of seven industries. However, Brazilian trust ratings significantly surpassed those of Japanese respondents for only three industries (shipping/delivery companies, search and social media sites, and media companies).

The similarity between the three high-trust countries is corroborated by the fact that, for five out of the seven industries (financial services companies, shipping/delivery companies, telecommunications companies, search and social media sites and media companies), these three countries' trust ratings did not differ significantly from each other (see Table 50–Table 52, Table 54, and Table 55). For the remaining two industries (healthcare providers and retailers), Brazilian respondents' trust ratings did not differ significantly from those of Chinese respondents (see Table 49 and Table 53). Regarding healthcare providers, US respondents' trust ratings significantly surpassed those of both Brazilian and Chinese respondents ($p = 0.007$ and $p < 0.0005$), while their ratings for retailers significantly surpassed those of Brazilian respondents ($p = 0.024$).

Germany and Ghana occupy a somewhat intermediate position between the high-trust countries and the low-trust countries. These two countries were very similar to each other in terms of trust ratings in that they only differed significantly from each other regarding healthcare providers and shipping/delivery companies. Ghanaian respondents exhibited significantly higher trust ratings than German respondents in each case ($p = 0.045$, $p = 0.048$). At first glance, it seems that Germany and Ghana leaned more toward the high-trust countries, as in both countries, most industries were trusted by a majority (in Germany this was six out of seven indus-

tries, the exception being search and social media sites; in Ghana it was five out of seven industries, the exceptions being media companies and search and social media sites). Indeed, upon closer inspection, Ghana seems to be slightly more similar to the high-trust countries than the low-trust countries (as visualized in Fig. 39). Thus, Brazil and Ghana never differed significantly from each other. Like Brazil, Ghana differed significantly from the United States in respect of just two industries, with US respondents' ratings significantly surpassing Ghanaian respondents' trust ratings for media companies and retailers (p = 0.039, p = 0.014). Ghana also differed from China regarding just two industries, with Ghanaian respondents significantly surpassing Chinese respondents in terms of trust regarding healthcare providers (p = 0.035) and being significantly surpassed by them regarding search and social media sites (p = 0.019). However, Ghanaians' trust ratings significantly surpassed both Japanese and Swiss respondents' trust ratings in only three out of seven industries (healthcare providers, financial services companies, and shipping delivery companies; see Table 49–Table 51).

Germany, however, seems to be somewhat more similar to the low-trust countries than most of the high-trust countries upon closer inspection. There were almost no significant differences between German and Japanese or Swiss respondents' trust in different industries. It was only regarding media companies that German respondents' trust ratings significantly surpassed those of Japanese and Swiss respondents (p = 0.001, p = 0.045). In contrast, German respondents demonstrated significantly lower trust ratings than US respondents for five out of seven industries (healthcare providers, financial services companies, shipping delivery companies, telecommunications companies, and retailers; see Table 49–Table 53) and significantly lower trust ratings than Chinese respondents regarding three industries (shipping delivery companies, telecommunications companies, and search and social media sites; see Table 51, Table 52, and Table 54). However, it is noteworthy that Brazilian and German respondents' trust ratings never significantly differed from each other.

3.2.3 Tables

This section contains tables with the p values for comparisons of the seven industries regarding respondents' trust in them to use consumer's personal data correctly for each of the seven countries (Table 40–Table 47), as well as those containing the p values for the comparisons of trust ratings for each industry in the seven countries (Table 48–Table 57).

Industry comparison

Table 40: Output of Friedman's ANOVAS regarding differences between the seven industries concerning respondents' trust in them to use consumers' personal data correctly by country.

	$\chi 2$	*df*	*p*
Brazil	59.76	6	< 0.0005***
China	20.31	6	0.002**
Germany	52.56	6	< 0.0005***
Ghana	114.51	6	< 0.0005***
Japan	131.44	6	< 0.0005***
Switzerland	63.66	6	< 0.0005***
US	58.54	6	< 0.0005***

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 41: *P* values of pairwise Wilcoxon signed rank tests regarding Brazilian respondents' trust in different industries to use consumers' personal data correctly.

	Healthcare providers	Financial services c	Shipping/ delivery c	Search & SM sites	Media c	Telecommu-nications c
Financial services c	0.134					
Shipping/ delivery c	0.001**	0.662				
Search & SM sites	< 0.0005***	0.437	1.000			
Media c	< 0.0005***	0.019*	0.662	0.466		
Telecommu-nications c	< 0.0005***	0.073	0.753	1.000	1.000	
Retailers selling Gs/Ss	< 0.0005***	0.013*	0.304	0.753	1.000	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 42: *P* values of pairwise Wilcoxon signed rank tests regarding Chinese respondents' trust in different industries to use consumers' personal data correctly.

	Healthcare providers	Financial services c	Shipping/ delivery c	Telecommu-nications c	Search & SM sites	Retailers selling Gs/Ss
Financial services c	1.000					
Shipping/ delivery c	1.000	1.000				
Telecommu-nications c	0.421	0.315	1.000			
Search & SM sites	0.315	0.251	1.000	1.000		
Retailers selling Gs/Ss	0.016*	0.020*	0.264	1.000	1.000	
Media c	0.045*	0.054	0.455	1.000	1.000	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 43: *P* values of pairwise Wilcoxon signed rank tests regarding German respondents' trust in different industries to use consumers' personal data correctly.

	Healthcare providers	Financial services c	Retailers selling Gs/Ss	Telecommu-nications c	Shipping/ Delivery c	Media c
Financial services c	0.068					
Retailers selling Gs/Ss	0.006*	0.970				
Telecommu-nications c	< 0.0005***	0.427	1.000			
Shipping/ delivery c	< 0.0005***	0.395	1.000	1.000		
Media c	< 0.0005***	0.250	1.000	1.000	1.000	
Search & SM sites	< 0.0005***	0.005*	0.181	0.181	0.395	0.395

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 44: *P* values of pairwise Wilcoxon signed rank tests regarding Ghanaian respondents' trust in different industries to use consumers' personal data correctly.

	Healthcare providers	Financial services c	Shipping/ Delivery c	Telecommu-nications c	Retailers selling Gs/Ss	Media c
Financial services c	0.251					
Shipping/ delivery c	0.007*	0.219				
Telecommu-nications c	< 0.0005***	0.007*	0.189			
Retailers selling Gs/Ss	< 0.0005***	< 0.0005***	0.002**	0.251		
Media c	< 0.0005***	< 0.0005***	< 0.0005***	0.005*	0.286	
Search & SM sites	< 0.0005***	< 0.0005***	< 0.0005***	0.018*	0.606	0.606

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 45: *P* values of pairwise Wilcoxon signed rank tests regarding Japanese respondents' trust in different industries to use consumers' personal data correctly.

	Healthcare providers	Financial services c	Telecommu-nications c	Retailers selling Gs/Ss	Shipping/ Delivery c	Search & SM sites
Financial services c	0.010*					
Telecommu-nications c	< 0.0005***	0.160				
Retailers selling Gs/Ss	< 0.0005***	0.005*	0.073			
Shipping/ delivery c	< 0.0005***	0.002**	0.030*	0.947		
Search & SM sites	< 0.0005***	< 0.0005***	< 0.0005***	0.020*	0.073	
Media c	< 0.0005***	< 0.0005***	< 0.0005***	0.007*	0.010*	0.947

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 46: *P* values of pairwise Wilcoxon signed rank tests regarding Swiss respondents' trust in different industries to use consumers' personal data correctly.

	Healthcare providers	Financial services c	Telecommu-nications c	Retailers selling Gs/Ss	Shipping/ Delivery c	Media c
Financial services c	0.058					
Telecommu-nications c	0.005*	1.000				
Retailers selling Gs/Ss	0.007*	1.000	1.000			
Shipping/ delivery c	0.004**	1.000	1.000	1.000		
Media c	< 0.0005***	0.070	0.148	0.058	0.148	
Search & SM sites	< 0.0005***	0.001**	0.005*	0.005*	0.005*	0.651

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 47: *P* values of pairwise Wilcoxon signed rank tests regarding US respondents' trust in different industries to use consumers' personal data correctly.

	Healthcare providers	Financial services c	Shipping/ Delivery c	Telecommu-nications c	Retailers selling Gs/Ss	Media c
Financial services c	0.107					
Shipping/ delivery c	< 0.0005***	0.523				
Telecommu-nications c	< 0.0005***	0.523	1.000			
Retailers selling Gs/Ss	< 0.0005***	0.477	1.000	1.000		
Media c	< 0.0005***	0.012*	0.152	0.137	0.477	
Search & SM sites	< 0.0005***	0.009*	0.115	0.079	0.137	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Country comparison

Table 48: Output of Kruskal-Wallis tests regarding cross-cultural differences in respondents' trust in a particular industry/institution to use consumers' personal data correctly.

	H	*df*	*p*
Healthcare providers	54.97	6	< 0.0005***
Financial services companies	51.38	6	< 0.0005***
Shipping/delivery companies	74.20	6	< 0.0005***
Telecommunications companies	39.67	6	< 0.0005***
Retailers selling goods and services	42.44	6	< 0.0005***
Search and social media sites	70.82	6	< 0.0005***
Media companies	62.85	6	< 0.0005***
The national government	71.13	6	< 0.0005***
Foreign governments	40.82	6	< 0.0005***

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 49: *P* values of pairwise Wilcoxon signed rank tests regarding respondents' trust in healthcare providers to use consumers' personal data correctly.

	US	Ghana	Brazil	China	Germany	Japan
Ghana	1.000					
Brazil	0.007*	0.292				
China	< 0.0005***	0.035*	1.000			
Germany	< 0.0005***	0.045*	1.000	1.000		
Japan	< 0.0005***	0.005*	0.292	0.773	1.000	
Switzerland	< 0.0005***	< 0.0005***	0.035*	0.149	0.429	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 50: *P* values of pairwise Wilcoxon signed rank tests regarding respondents' trust in financial services companies to use consumers' personal data correctly.

	US	Ghana	China	Brazil	Germany	Japan
Ghana	1.000					
China	0.893	1.000				
Brazil	0.142	0.754	1.000			
Germany	0.012*	0.111	0.219	1.000		
Japan	< 0.0005***	0.002**	0.002**	0.090	1.000	
Switzerland	< 0.0005***	< 0.0005***	< 0.0005***	0.013*	0.566	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 51: *P* values of pairwise Wilcoxon signed rank tests regarding respondents' trust in shipping/ delivery companies to use consumers' personal data correctly.

	US	Ghana	China	Brazil	Germany	Switzerland
Ghana	1.000					
China	0.951	1.000				
Brazil	0.154	0.951	0.780			
Germany	0.001**	0.048*	0.005*	0.498		
Switzerland	< 0.0005***	0.001**	< 0.0005***	0.008*	0.780	
Japan	< 0.0005***	< 0.0005***	< 0.0005***	< 0.0005***	0.140	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 52: *P* values of pairwise Wilcoxon signed rank tests regarding respondents' trust in telecommunications companies to use consumers' personal data correctly.

	US	China	Ghana	Brazil	Germany	Japan
China	0.894					
Ghana	0.539	1.000				
Brazil	0.051	0.635	1.000			
Germany	0.003**	0.043*	1.000	1.000		
Japan	< 0.0005***	0.002**	0.894	1.000	1.000	
Switzerland	< 0.0005***	< 0.0005***	0.353	0.472	1.000	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 53: *P* values of pairwise Wilcoxon signed rank tests regarding respondents' trust in retailers selling goods and services to use consumers' personal data correctly.

	US	China	Germany	Ghana	Brazil	Switzerland
China	0.454					
Germany	0.042*	1.000				
Ghana	0.014*	0.531	1.000			
Brazil	0.024*	0.840	1.000	1.000		
Switzerland	< 0.0005***	0.012*	0.840	1.000	0.840	
Japan	< 0.0005***	< 0.0005***	0.210	0.840	0.145	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 54: *P* values of pairwise Wilcoxon signed rank tests regarding respondents' trust in search and social media sites to use consumers' personal data correctly.

	China	US	Brazil	Germany	Ghana	Switzerland
US	1.000					
Brazil	1.000	1.000				
Germany	0.011*	0.056	0.090			
Ghana	0.019*	0.128	0.155	1.000		
Switzerland	< 0.0005***	< 0.0005***	< 0.0005***	0.475	0.133	
Japan	< 0.0005***	< 0.0005***	< 0.0005***	0.736	0.214	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 55: *P* values of pairwise Wilcoxon signed rank tests regarding respondents' trust in media companies to use consumers' personal data correctly.

	US	China	Brazil	Germany	Ghana	Switzerland
China	1.000					
Brazil	0.522	1.000				
Germany	0.154	0.395	1.000			
Ghana	0.039*	0.066	0.522	1.000		
Switzerland	< 0.0005***	< 0.0005***	0.002**	0.045*	1.000	
Japan	< 0.0005***	< 0.0005***	< 0.0005***	0.001**	0.395	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 56: *P* values of pairwise Wilcoxon signed rank tests regarding respondents' trust in the national government to use consumers' personal data correctly.

	China	US	Germany	Brazil	Ghana	Switzerland
US	0.253					
Germany	0.001**	0.804				
Brazil	< 0.0005***	0.043*	0.804			
Ghana	0.002**	0.774	1.000	1.000		
Switzerland	< 0.0005***	0.003**	0.227	1.000	0.804	
Japan	< 0.0005***	< 0.0005***	0.003**	0.412	0.133	0.804

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 57: *P* values of pairwise Wilcoxon signed rank tests regarding respondents' trust in foreign governments to use consumers' personal data correctly.

	Ghana	US	China	Brazil	Germany	Switzerland
US	1.000					
China	0.996	1.000				
Brazil	0.405	0.435	1.000			
Germany	0.480	0.522	1.000	1.000		
Switzerland	0.017*	0.017*	0.037*	0.966	0.660	
Japan	< 0.0005***	< 0.0005***	< 0.0005***	0.037*	0.012*	0.966

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

3.3 Compliance with the regulation of consumer data protection and informational privacy

Respondents were also asked how they would assess the compliance of the aforementioned seven industries with the regulation of consumer data protection and informational privacy in their country on a five-point scale (*sufficient – rather sufficient – neutral – rather insufficient – insufficient*).

3.3.1 Compliance of different industries

In all seven countries, we found significant differences ($p < 0.0005$) between the seven industries we surveyed regarding perceived compliance with consumer data protection and informational privacy regulations (for details, see Table 58 in 3.3.3,

p. 88[18]). Let us first examine which industries respondents in the seven countries perceived as demonstrating particularly high compliance, before considering which were perceived to demonstrate particularly low compliance. Fig. 40 (a)—(g) on p. 78 presents the survey results of professionals' assessments of different industries' compliance with their respective country's consumer data protection and informational privacy regulations. The seven different industries are listed in descending order according to the combined percentage of respondents who rated their compliance with consumer data protection and informational privacy regulations as *sufficient* or *rather sufficient*.

Across all countries, healthcare providers and financial services companies ranked highest[19] in terms of perceived compliance (see Fig. 40 on the following page). Moreover, as can be seen in Fig. 41 and Fig. 42 below (p. 79–80), in all countries, with the exception of Japan, a majority of professionals considered compliance to be *sufficient* or *rather sufficient* in the healthcare (≥ 60 %) and financial services sectors (≥ 53 %). Notably, the two industries did not differ significantly in terms of perceived compliance in any country except the United States (p = 0.030), where the compliance of healthcare providers was rated as significantly more sufficient than that of financial services companies (see Table 59–Table 65, p. 88–91). Healthcare providers ranked first in terms of perceived compliance in China (78 % positive assessment), the United States (76 %), Germany (72 %), and Switzerland (66 %), and second in Brazil (71 %), Ghana (60 %), and Japan (45 %). In most countries, their special status was supported by statistical tests: Compliance ratings for healthcare providers significantly surpassed those of all or most other industries in the United States (all industries); in Germany, Switzerland, and Japan (five out of six industries); and in Ghana (four out of six industries; see Table 61–Table 65). Only in Brazil and China did they only surpass two out of six industries to a statistically significant extent (see Table 59 and Table 60).

18 All tables can be found at the end of this section (3.3.3.). This is because, at several points in the section, we refer to multiple such tables at once, and including them in the running text would unnecessarily disrupt the flow of the text.

19 When using expressions such as "most compliant"/"least compliant," and when discussing industry rankings in terms of perceived compliance, we are referring to the combined percentage of respondents who opted for *sufficient* or *rather sufficient*. If this percentage is the same for two countries, the country whose percentage of *sufficient* responses is greater is ranked higher.

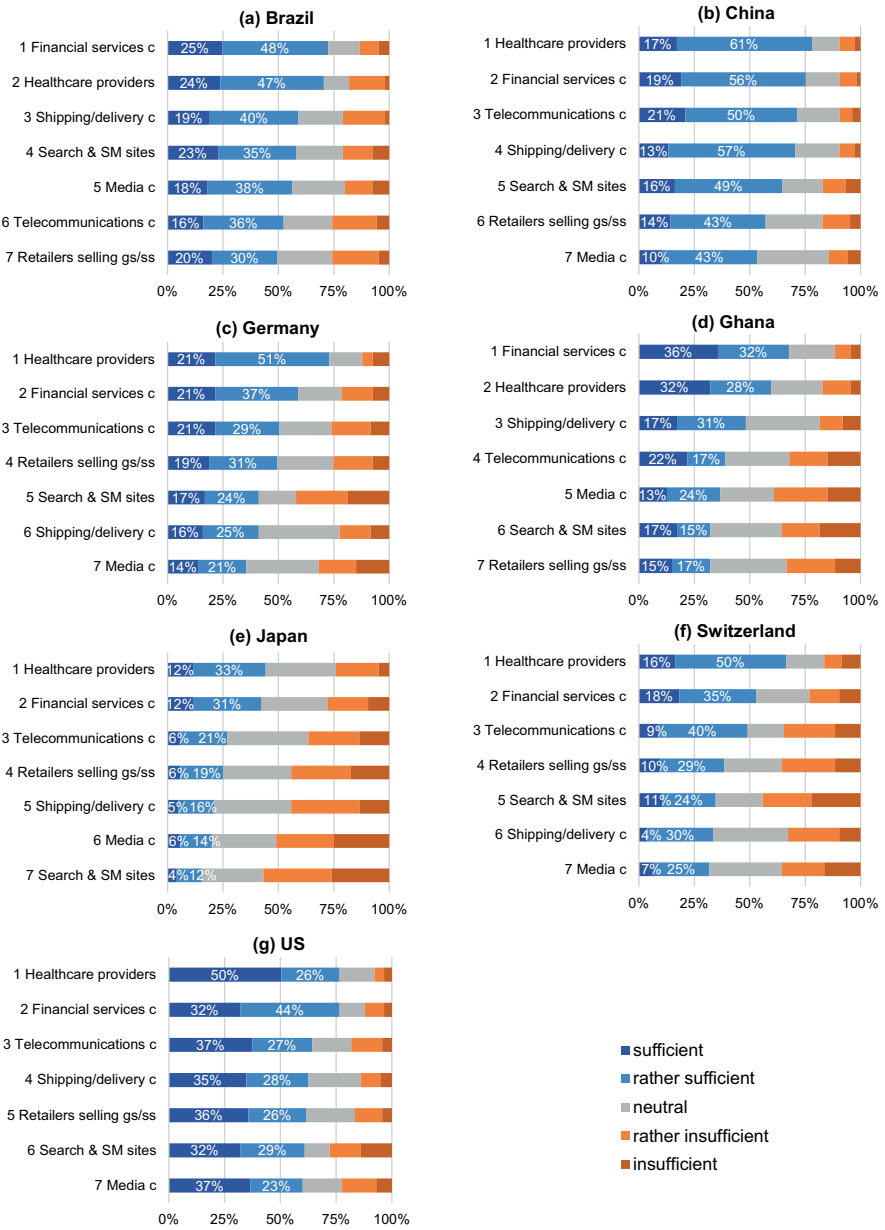

Fig. 40: Brazilian (a), Chinese (b), German (c), Ghanaian (d), Japanese (e), Swiss (f), and US (g) professionals' assessments of seven industries' compliance with the regulation of consumer data protection and informational privacy in their countries.

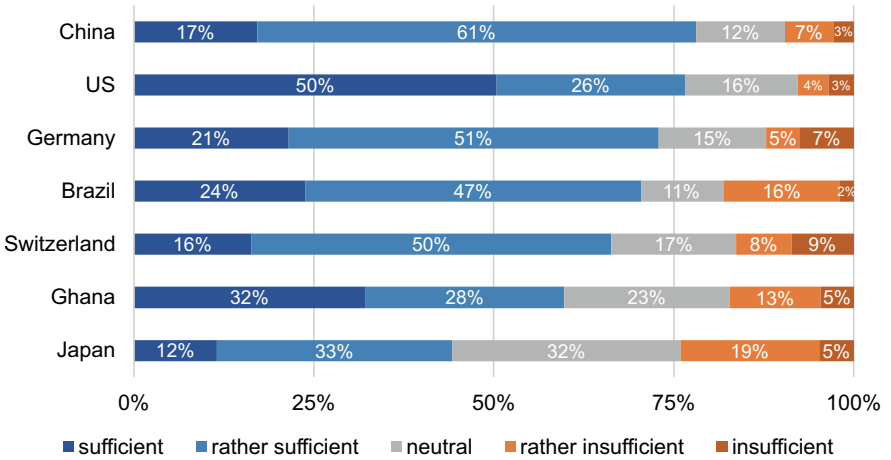

Fig. 41: Q13. Healthcare providers: How would you assess compliance with the regulation of consumer data protection and informational privacy in your country by the following industries?

Fig. 40 (p. 78) shows that financial services companies were considered the most compliant of all industries in Brazil (73 % agreement) and Ghana (68 %). They ranked second in the United States (76 %), China (75 %), Germany (58 %), Switzerland (53 %), and Japan (43 %). Thus, as is also evident in Fig. 42 below, a majority of professionals in all countries but Japan regarded their compliance as *sufficient* or *rather sufficient*. In Germany, Ghana, Japan, and Switzerland, their compliance was rated significantly higher than that of most other industries (four to five out of six; see Table 61, Table 62, Table 63, and Table 64 in 3.3.3). In Brazil and China, their perceived compliance was significantly greater than that of retailers (p = 0.005, p = 0.003) and media companies (p = 0.031, p < 0.0005). In the United States, however, they only surpassed search and social media sites in terms of perceived compliance to a statistically significant extent (p = 0.002).

Notably, while Japanese professionals also ranked healthcare and financial services companies first and second with regard to compliance, only a minority of them (45 % for healthcare providers and 43 % for financial services companies) considered their compliance *sufficient* or *rather sufficient* (see Fig. 41 above, Fig. 42 below). Almost one-third expressed a neutral view (32 % for healthcare, 30 % for financial services). Indeed, Japanese respondents perceived healthcare providers' compliance to be significantly less sufficient than respondents in the United States (p < 0.0005), China (p < 0.0005), Germany (p = 0.003), and Brazil (p = 0.011) did; and they considered the compliance of financial services companies to be significantly less sufficient than respondents in the United States, Ghana, China (< 0.0005 each), and Brazil (p = 0.001) did.

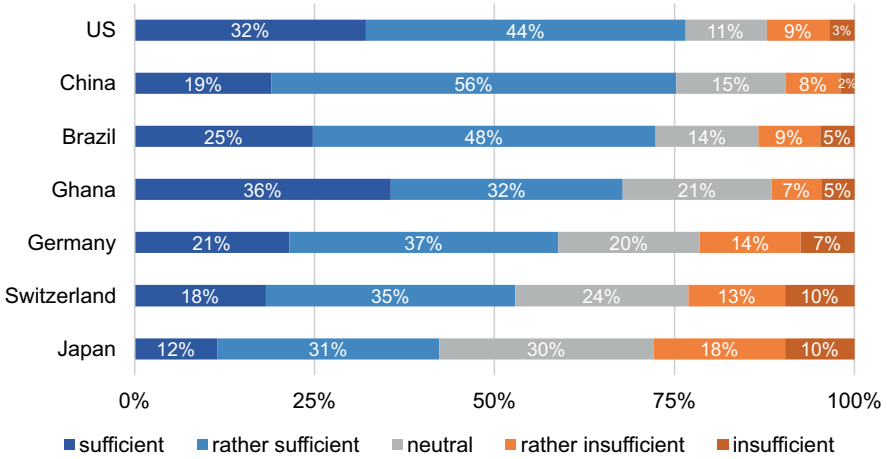

Fig. 42: Q13. Financial services companies: How would you assess compliance with the regulation of consumer data protection and informational privacy in your country by the following industries?

Let us now move on to the industries that tended to rank low in terms of perceived compliance. Similar to respondents' trust ratings (see section 3.2.), media companies' compliance was not seen in a particularly positive light in several countries: They came last in four countries (China, Germany, Switzerland, and the United States) and sixth (i.e., second last) in Japan, where a majority assessed their compliance as *insufficient* or *rather insufficient*. It is noteworthy that only a minority assessed their compliance as *sufficient* or *rather sufficient* in Japan (20 %), Switzerland (32 %) and Germany (35 %) (see Fig. 43, p. 81). In Japan, a majority of 51 % even assessed the compliance of media companies as *insufficient* or *rather insufficient*. However, it was only in two countries—China and Germany—that media companies received significantly lower compliance ratings than a majority of the other industries (four out of six each; see Table 60 and Table 61 in 3.3.3). In Japan and Ghana (where they were ranked fifth), media companies received significantly lower ratings than three out of six industries (see Table 62 and Table 63). In Switzerland, this figure was two out of six ($p < 0.0005$ and $p = 0.001$), and in both the United States and Brazil (where they rank fifth) only one out of six industries ($p < 0.0005$, $p = 0.031$). Thus, statistical tests supported media companies' comparatively low perceived compliance with the regulation of consumer data protection and informational privacy for Germany and China alone, and to some extent for Japan and Ghana.

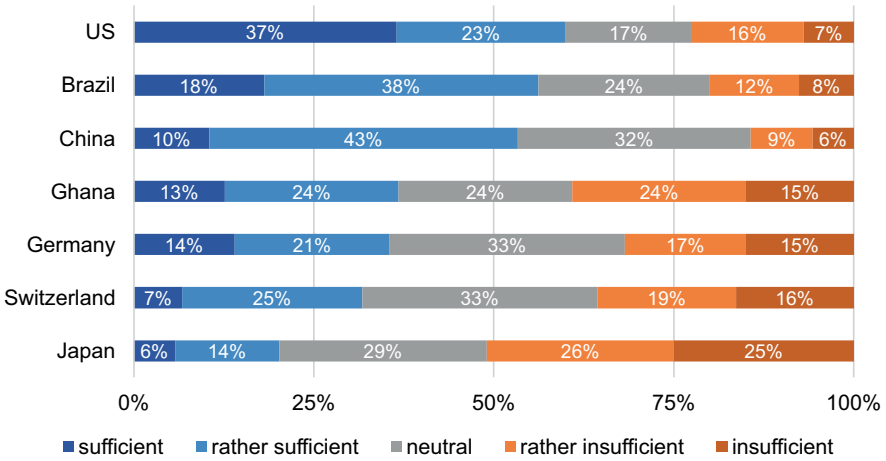

Fig. 43: Q13. Media companies: How would you assess compliance with the regulation of consumer data protection and informational privacy in your country by the following industries?

Another pattern similar to the one observed for respondents' trust ratings was that search and social media sites did not compare very well with other industries in terms of perceived compliance in several countries. Their compliance was regarded as *sufficient* or *rather sufficient* by only a minority in four out of seven countries, namely in Japan (16 %), Ghana (32 %), Switzerland (35 %), and Germany (41 %) (Fig. 44, p. 82). Moreover, they came last in terms of perceived compliance in Japan and second last in Ghana and the United States. In Japan, a majority of 57 % even assessed their compliance as *insufficient* or *rather insufficient*. However, only in Germany and Japan did search and social media sites receive significantly lower compliance ratings than most other (i.e., four to five out of six) industries (see Table 61 and Table 63 in 3.3.3). In Ghana, they received significantly lower ratings than half the remaining industries (Table 62). By contrast, only two industries significantly surpassed them in terms of perceived compliance in Switzerland and the United States (healthcare providers at $p < 0.0005$ and financial services companies at $p = 0.002$ in both countries), and no industry surpassed them to this extent in China or Brazil. Thus, statistical tests only confirmed their comparatively low perceived compliance with the regulation of consumer data protection and informational privacy for Germany and Japan, and to some extent for Ghana.

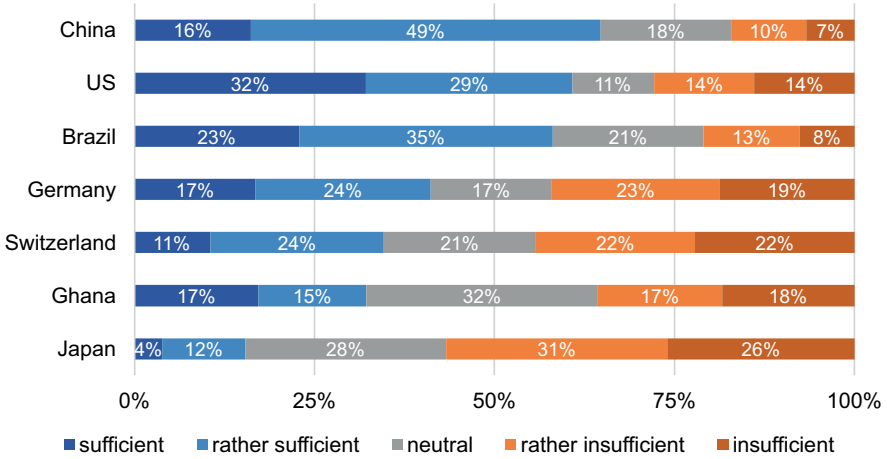

Fig. 44: Q13. Search and social media sites: How would you assess compliance with the regulation of consumer data protection and informational privacy in your country by the following industries?

Another industry which received satisfactory compliance ratings from only a minority of respondents in four countries was shipping/delivery companies. Their compliance was deemed *sufficient* or *rather sufficient* by 21 % of Japanese respondents, 34 % of Swiss respondents, 41 % of German respondents, and 48 % of Ghanaian respondents (Fig. 45 below). Moreover, they ranked second last in terms of perceived compliance in Germany and Switzerland. However, their compliance ratings were significantly lower than those of only two other industries in Japan ($p < 0.0005$ each) and Switzerland ($p < 0.0005$, $p = 0.002$), and only one other industry in Germany ($p < 0.0005$) and Ghana ($p = 0.002$).

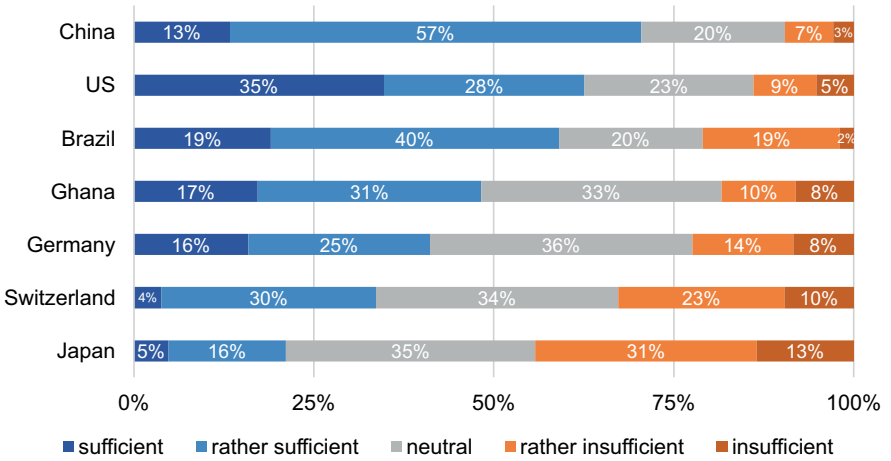

Fig. 45: Q13. Shipping/delivery companies: How would you assess compliance with the regulation of consumer data protection and informational privacy in your country by the following industries?

In three countries—Japan, Ghana, and Switzerland—telecommunications companies and retailers selling goods and services likewise only received satisfactory compliance ratings (i.e., *sufficient* or *rather sufficient*) from a minority of respondents (see Fig. 46, and Fig. 47, p. 84). In Japan, retailers' compliance was assessed as *sufficient* or *rather sufficient* by 25 % of respondents, whereas this figure was 32 % in Ghana and 39 % in Switzerland. Moreover, retailers came in last in Brazil and Ghana, and second last in China. Indeed, in China and Ghana, their compliance ratings were significantly lower than those of half the other industries (i.e., three out of six) (see Table 60 and Table 62). However, their ratings were significantly lower than those of only two other industries in Switzerland ($p < 0.0005$, $p = 0.037$), Japan ($p < 0.0005$, $p = 0.001$), and Brazil ($p = 0.005$ and $p = 0.011$). Thus, statistical tests only somewhat confirmed their comparatively low perceived compliance with the regulation of consumer data protection and informational privacy for China and Ghana.

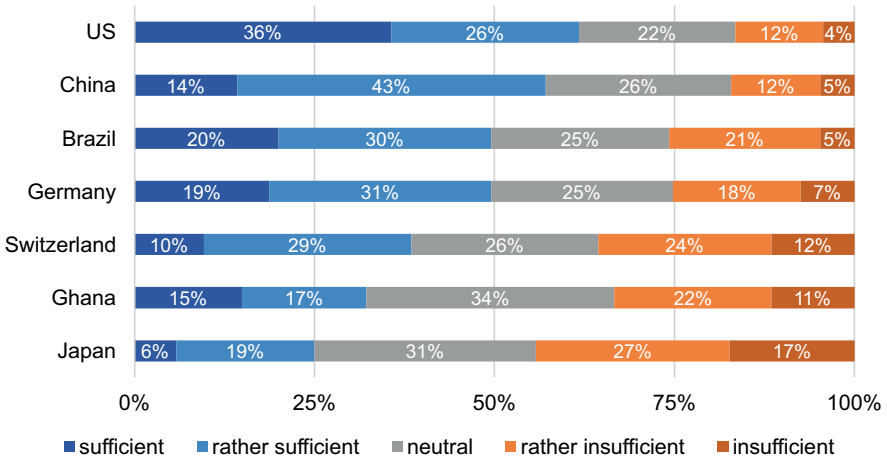

Fig. 46: Q13. Retailers selling goods and services: How would you assess compliance with the regulation of consumer data protection and informational privacy in your country by the following industries?

Telecommunications companies' compliance was considered *sufficient* or *rather sufficient* by 27 % of Japanese respondents, 39 % of Ghanaian respondents, and 49 % of Swiss respondents (see Fig. 47 below). They did not rank last in any country, but came second last in Brazil. Yet, their compliance ratings were significantly lower than those of only one or two other industries in those four countries (see Table 59 and Table 62–Table 64).

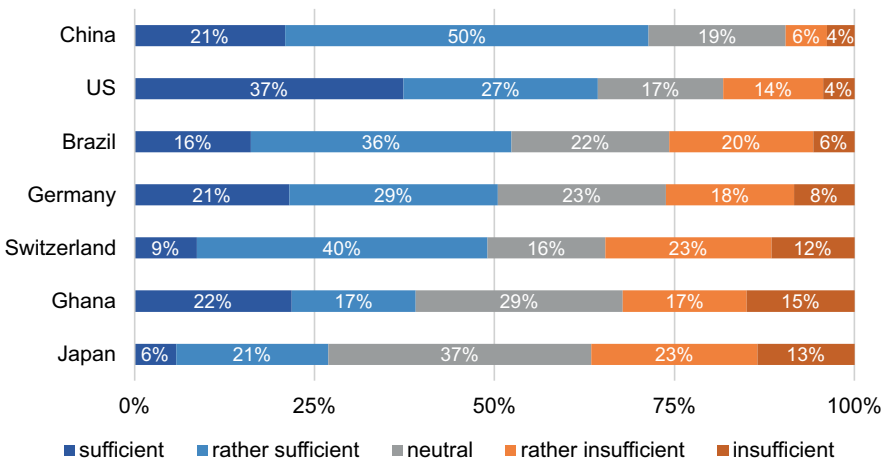

Fig. 47: Q13. Telecommunications companies: How would you assess compliance with the regulation of consumer data protection and informational privacy in your country by the following industries?

3.3.2 Countries with high perceived compliance and low perceived compliance

Let us now compare the seven countries in terms of the levels of compliance with the regulation of consumer data protection and informational privacy that respondents attributed to each of the seven industries. We found significant cross-cultural differences regarding the perceived compliance of each of the seven industries ($p < 0.0005$; for details, see Table 66, p. 92). Again, we attempted to cluster the countries into two different groups, the countries with "high perceived compliance" on the one hand and the countries with "low perceived compliance" on the other. As with trust ratings (see section 3.2.2), the United States and China fell into the former group (see Fig. 48 below): Here, a majority of professionals were content with the compliance of all sectors included in the survey (≥ 60 % United States, ≥ 53 % China) in their country (see also Fig. 40 [b] and [g] on p. 78). Brazil also seemed to belong to this group, as at least half of Brazilian respondents (≥ 50 %) assessed all industries' compliance with the regulation of consumer data protection and informational privacy as *sufficient* or *rather sufficient* (Fig. 40 [a]). This classification was also supported by the fact that the compliance ratings assigned by US. Chinese, and Brazilian respondents did not differ significantly from each other for six out of the seven industries surveyed (see Table 67–Table 73, p. 92–94). Only healthcare providers were rated significantly higher in terms of compliance by US respondents than by Chinese respondents ($p = 0.010$) and Brazilian respondents ($p = 0.011$). The latter two did not differ significantly in this regard.

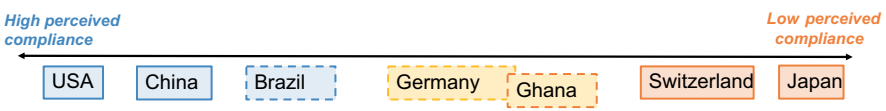

Fig. 48: Perceived compliance scale.

By contrast, in the countries with low perceived compliance, only a minority (< 50 %) of respondents assessed the compliance of (almost) all industries as satisfactory (i.e., as *sufficient* or *rather sufficient*). Japan most clearly belongs to this category: It was the only country where this was the case for *all* industries (Fig. 40 [e]). Moreover, it is noteworthy that—in comparison to the other countries—the percentage of those who answered neutrally was relatively high for Japan (between 28 % and 37 %), as was the combined percentage of *rather insufficient* and *insufficient* responses (between 24 % for the compliance of healthcare providers and 57 % for search and social media sites and 51 % for media companies). It is equally noteworthy that in no other country did a majority assess compliance as *insufficient* or *rather insufficient* for any of the industries surveyed. Japan was thus the only country in which a majority of local professionals saw a need for two industries—search

and social media sites as well as media companies—to improve their compliance. Accordingly, Japanese respondents' compliance ratings were significantly lower for those two industries than the ratings given by US. Chinese, Brazilian, and German respondents, and, regarding search and social media sites, those provided by Ghanaian respondents as well (see Table 72 and Table 73 in 3.3.3).

The classification of Japan as a country with low perceived compliance vis-à-vis the countries with high perceived compliance—namely the United States, China, and possibly also Brazil—is also supported by the fact that Japanese compliance ratings were significantly lower than the ratings given by respondents in the United States, China, and Brazil for *all* industries surveyed (see Table 67–Table 73). In fact, the compliance ratings assigned by Japanese respondents were significantly lower than those given by respondents in most other countries for all seven industries. In addition to the ratings given by the United States, China, and Brazil, German compliance ratings significantly surpassed Japanese ones for all industries but financial services companies. Ghanaian compliance ratings significantly surpassed them for financial services companies, shipping/delivery companies, and search and social media sites.

In contrast, Swiss compliance ratings did not differ significantly from Japanese compliance ratings for any of the industries surveyed (see Table 67–Table 73). Thus, Switzerland could also be classified as a country with low perceived compliance. Switzerland fits the above definition of a country with low perceived compliance as, in most industries surveyed, only a minority of Swiss respondents assessed compliance with the regulation of consumer data protection and informational privacy as *sufficient* or *rather sufficient* (Fig. 40 [f]). Moreover, Swiss compliance ratings were significantly lower than those given by US respondents for all seven industries and significantly lower than those provided by Chinese respondents for five of the seven industries. The same applies when comparing them to Brazilian compliance ratings, but only for three out of seven industries. It thus seems apt to classify Switzerland, alongside Japan, as a country with low perceived compliance compared to the United States and China.

Ghana and Germany both seem to fall somewhere between the countries with low perceived compliance and the countries with high perceived compliance. Thus, though Ghanaian compliance ratings were fairly similar to Swiss and Japanese ratings (never differing significantly to the Swiss and only significantly surpassing the Japanese regarding three industries at $p < 0.0005$ and $p = 0.023$), they were also similar to the ratings assigned in China, a country with high perceived compliance, for most industries (see Table 67–Table 73). Thus, they were significantly lower than Chinese ratings in only three out of seven industries ($p = 0.043$ for retailers and $p = 0.007$ for search and social media sites and telecommunications companies) and significantly lower than Brazilian ratings in only two out of seven industries

(p = 0.024 for search and social media sites and p = 0.048 for media companies). However, they were significantly lower than US ratings in five out of seven industries (see Table 67 and Table 70–Table 73). Ghana should therefore be classified as falling somewhere between the countries with high perceived compliance and those with low perceived compliance, but leaning more toward the latter (see Fig. 48, p. 85). This is also reflected in the fact that, as in Japan and Switzerland, only a minority of Ghanaian respondents assessed compliance with the regulation of consumer data protection and informational privacy as *sufficient* or *rather sufficient* for most industries surveyed (see Fig. 40 [d]).

German compliance ratings were very similar to Swiss and Ghanaian ratings: No significant differences were found between German ratings on the one hand and Swiss and Ghanaian compliance ratings on the other for any of the industries surveyed (see Table 67–Table 73). However, as mentioned above, German respondents' assessments of compliance were significantly higher than those of Japanese respondents for all industries except for financial services companies (see Table 67–Table 73). German ratings were also very similar to Brazilian and Chinese ratings: No significant differences were found between German ratings and Brazilian ratings for six out of seven industries (the exception being search and social media sites, with Brazilian ratings significantly higher at p = 0.031) or between German and Chinese ratings for five out of seven industries (the exceptions being search and social media sites and shipping/delivery companies, with Chinese ratings significantly surpassing German ratings at p = 0.019 and p = 0.012). When comparing Germany to the United States, we see that German compliance ratings were significantly lower than US ratings for four out of seven industries (p = 0.011 for healthcare providers, p = 0.007 for shipping/delivery companies, p = 0.031 for search and social media sites, and p = 0.003 for media companies). Given its similarity to Switzerland, Ghana, Brazil, and China, and the fact that Germany differed significantly from both the United States and Japan in several industries, Germany can probably be best classified as a truly intermediary case between the countries with high perceived compliance and those with low perceived compliance (see Fig. 48, p. 85). This classification is also suggested by the fact that, for three out of the seven industries, only a minority of German respondents assessed compliance with the regulation of consumer data protection and informational privacy as *sufficient* or *rather sufficient* (Fig. 40 [c]). For the remaining four industries, a majority or exactly half (50 %) of German respondents were satisfied with their compliance.

3.3.3 Tables
Industry comparison

Table 58: Output of Friedman's ANOVAS regarding differences in perceived compliance with the regulation of consumer data protection and informational privacy between the seven industries by country.

	χ^2	*df*	*p*
Brazil	38.40	6	< 0.0005***
China	39.76	6	< 0.0005***
Germany	63.71	6	< 0.0005***
Ghana	89.71	6	< 0.0005***
Japan	100.46	6	< 0.0005***
Switzerland	63.87	6	< 0.0005***
US	44.72	6	< 0.0005***

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 59: *P* values of pairwise Wilcoxon signed rank tests regarding differences in compliance with the regulation of consumer data protection and informational privacy between the seven industries, as perceived by Brazilian respondents.

	Financial services c	**Healthcare providers**	**Shipping/ Delivery c**	**Search & SM sites**	**Media c**	**Retailers selling Gs/Ss**
Healthcare providers	1.000					
Shipping/ delivery c	0.098	0.394				
Search & SM sites	0.123	0.385	1.000			
Media c	0.031*	0.115	1.000	1.000		
Retailers selling Gs/Ss	0.005*	0.011*	0.871	1.000	1.000	
Telecommu-nications c	0.004**	0.027*	0.325	1.000	1.000	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 60: *P* values of pairwise Wilcoxon signed rank tests regarding differences in compliance with the regulation of consumer data protection and informational privacy between the seven industries, as perceived by Chinese respondents.

	Healthcare providers	Financial services c	Telecommu-nications c	Shipping/ Delivery c	Search & SM sites	Retailers selling Gs/Ss
Financial services c	1.000					
Telecommu-nications c	1.000	1.000				
Shipping/ delivery c	1.000	1.000	1.000			
Search & SM sites	0.180	0.052	0.296	1.000		
Retailers selling Gs/Ss	0.003**	0.003**	0.033*	0.096	1.000	
Media c	0.002**	< 0.0005***	0.003**	0.015*	0.799	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 61: *P* values of pairwise Wilcoxon signed rank tests regarding differences in compliance with the regulation of consumer data protection and informational privacy between the seven industries, as perceived by German respondents.

	Healthcare providers	Financial services c	Telecommu-nications c	Retailers selling Gs/Ss	Shipping/ Delivery c	Media c
Financial services c	0.074					
Telecommu-nications c	0.015*	1.000				
Retailers selling Gs/Ss	0.010*	1.000	1.000			
Shipping/ delivery c	< 0.0005***	0.074	1.000	1.000		
Media c	< 0.0005***	0.001**	0.023*	0.003**	0.060	
Search & SM sites	< 0.0005***	0.002**	0.010*	0.002**	0.071	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 62: *P* values of pairwise Wilcoxon signed rank tests regarding differences in compliance with the regulation of consumer data protection and informational privacy between the seven industries, as perceived by Ghanaian respondents.

	Financial services c	Healthcare providers	Shipping/ Delivery c	Telecommu-nications c	Retailers selling Gs/Ss	Media c
Healthcare providers	0.664					
Shipping/ delivery c	0.002**	0.137				
Telecommu-nications c	< 0.0005***	0.002**	0.227			
Retailers selling Gs/Ss	< 0.0005***	< 0.0005***	0.012*	1.000		
Media c	< 0.0005***	< 0.0005***	0.012*	0.770	1.000	
Search & SM sites	< 0.0005***	< 0.0005***	0.013*	0.664	1.000	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 63: *P* values of pairwise Wilcoxon signed rank tests regarding differences in compliance with the regulation of consumer data protection and informational privacy between the seven industries, as perceived by Japanese respondents.

	Healthcare providers	Financial services c	Telecommu-nications c	Retailers selling Gs/Ss	Shipping/ Delivery c	Media c
Financial services c	0.591					
Telecommu-nications c	0.001**	0.003**				
Retailers selling Gs/Ss	< 0.0005***	0.001**	0.591			
Shipping/ delivery c	< 0.0005***	< 0.0005***	0.570	0.847		
Media c	< 0.0005***	< 0.0005***	0.005*	0.580	0.591	
Search & SM sites	< 0.0005***	< 0.0005***	< 0.0005***	0.009*	0.014*	0.591

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 64: *P* values of pairwise Wilcoxon signed rank tests regarding differences in compliance with the regulation of consumer data protection and informational privacy between the seven industries, as perceived by Swiss respondents.

	Healthcare providers	Financial services c	Telecommu-nications c	Retailers selling Gs/Ss	Shipping/ Delivery c	Media c
Financial services c	0.553					
Telecommu-nications c	0.004**	0.164				
Retailers selling Gs/Ss	< 0.0005***	0.037*	1.000			
Shipping/ delivery c	< 0.0005***	0.002**	0.553	1.000		
Media c	< 0.0005***	0.001**	0.159	1.000	1.000	
Search & SM sites	< 0.0005***	0.002**	0.074	0.297	0.817	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 65: *P* values of pairwise Wilcoxon signed rank tests regarding differences in compliance with the regulation of consumer data protection and informational privacy between the seven industries, as perceived by US respondents.

	Healthcare providers	Financial services c	Telecommu-nications c	Shipping/ Delivery c	Retailers selling Gs/Ss	Media c
Financial services c	0.030*					
Telecommu-nications c	0.001**	0.538				
Shipping/ delivery c	0.002**	0.455	1.000			
Retailers selling Gs/Ss	0.002**	0.455	1.000	1.000		
Media c	< 0.0005***	0.082	1.000	1.000	1.000	
Search & SM sites	< 0.0005***	0.002**	0.074	0.112	0.229	0.455

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Country comparison

Table 66: Output of Kruskal-Wallis tests regarding cross-cultural differences in respondents' perceptions of a particular industry's compliance with the regulation of consumer data protection and informational privacy.

	H	*df*	*p*
Healthcare providers	48.33	6	< 0.0005***
Financial services companies	42.93	6	< 0.0005***
Shipping/delivery companies	84.36	6	< 0.0005***
Telecommunications companies	57.15	6	< 0.0005***
Retailers selling goods and services	57.23	6	< 0.0005***
Search and social media sites	75.86	6	< 0.0005***
Media companies	70.02	6	< 0.0005***

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 67: *P* values of pairwise Wilcoxon signed rank tests regarding healthcare providers' perceived compliance with the regulation of consumer data protection and informational privacy in different countries.

	US	China	Germany	Brazil	Ghana	Switzerland
China	0.010*					
Germany	0.011*	1.000				
Brazil	0.011*	1.000	1.000			
Ghana	0.042*	1.000	1.000	1.000		
Switzerland	< 0.0005***	1.000	1.000	1.000	1.000	
Japan	< 0.0005***	< 0.0005***	0.003**	0.011*	0.065	0.125

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 68: *P* values of pairwise Wilcoxon signed rank tests regarding financial services companies' perceived compliance with the regulation of consumer data protection and informational privacy in different countries.

	US	Ghana	Brazil	China	Germany	Switzerland
Ghana	1.000					
Brazil	1.000	1.000				
China	1.000	1.000	1.000			
Germany	0.090	0.336	0.795	0.795		
Switzerland	0.006*	0.062	0.133	0.098	1.000	
Japan	< 0.0005***	< 0.0005***	0.001**	< 0.0005***	0.242	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 69: *P* values of pairwise Wilcoxon signed rank tests regarding shipping/delivery companies' perceived compliance with the regulation of consumer data protection and informational privacy in different countries.

	US	China	Brazil	Ghana	Germany	Switzerland
China	1.000					
Brazil	0.370	1.000				
Ghana	0.111	0.263	1.000			
Germany	0.007*	0.012*	0.370	1.000		
Switzerland	< 0.0005***	< 0.0005***	0.001**	0.062	0.370	
Japan	< 0.0005***	< 0.0005***	< 0.0005***	< 0.0005***	0.002**	0.370

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 70: *P* values of pairwise Wilcoxon signed rank tests regarding telecommunications companies' perceived compliance with the regulation of consumer data protection and informational privacy in different countries.

	US	China	Germany	Brazil	Ghana	Switzerland
China	1.000					
Germany	0.102	0.138				
Brazil	0.057	0.072	1.000			
Ghana	0.009*	0.007*	1.000	1.000		
Switzerland	0.001**	0.001**	0.950	0.950	1.000	
Japan	< 0.0005***	< 0.0005***	0.012*	0.009*	0.810	0.431

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 71: *P* values of pairwise Wilcoxon signed rank tests regarding retailers selling goods and services' perceived compliance with the regulation of consumer data protection and informational privacy in different countries.

	US	China	Brazil	Germany	Ghana	Switzerland
China	0.359					
Brazil	0.163	1.000				
Germany	0.113	1.000	1.000			
Ghana	< 0.0005***	0.043*	0.359	0.359		
Switzerland	< 0.0005***	0.033*	0.279	0.359	1.000	
Japan	< 0.0005***	< 0.0005***	0.001**	0.001**	0.359	0.359

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 72: *P* values of pairwise Wilcoxon signed rank tests regarding search and social media sites' perceived compliance with the regulation of consumer data protection and informational privacy in different countries.

	China	US	Brazil	Germany	Ghana	Switzerland
US	1.000					
Brazil	1.000	1.000				
Germany	0.019*	0.031*	0.031*			
Ghana	0.007*	0.031*	0.024*	1.000		
Switzerland	< 0.0005***	0.001**	0.001**	1.000	1.000	
Japan	< 0.0005***	< 0.0005***	< 0.0005***	0.019*	0.023*	0.142

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 73: *P* values of pairwise Wilcoxon signed rank tests regarding media companies' perceived compliance with the regulation of consumer data protection and informational privacy in different countries.

	US	Brazil	China	Germany	Ghana	Switzerland
Brazil	0.580					
China	0.255	1.000				
Germany	0.003**	0.070	0.081			
Ghana	0.002**	0.048*	0.054	1.000		
Switzerland	< 0.0005***	0.003**	0.003**	1.000	1.000	
Japan	< 0.0005***	< 0.0005***	< 0.0005***	0.026*	0.110	0.145

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

3.4 Levels of consumer data protection

Respondents were also asked how they would assess the levels of consumer data protection offered by the aforementioned seven industries in their country on the same five-point scale as before (*sufficient – rather sufficient – neutral – rather insufficient – insufficient*).

3.4.1 Levels of consumer data protection in different industries

In all seven countries, we found significant differences ($p < 0.0005$) in the perceived levels of consumer data protection offered by the seven industries (for details, see Table 74 in section 3.4.3., p. 107).[20] Again, we will first consider the industries that respondents in the seven countries perceived as offering a particularly high level of consumer data protection, before considering the industries that were perceived as providing a rather low level. Fig. 49 (a)–(g) on p. 96 presents the survey results of professionals' assessments of the levels of consumer data protection in the seven different industries. In each figure, the industries are ranked in descending order according to the combined percentage of respondents who assessed the level of consumer data protection as *sufficient* or *rather sufficient*. If this combined percentage was the same for two industries, the one with the lower percentage for *sufficient* was ranked lower.

As shown in Fig. 49, healthcare providers ranked first in terms of the percentage of respondents who said the level of consumer data protection they offered was *sufficient* or *rather sufficient* in most countries (US, Germany, China, and Japan; in Switzerland and Brazil, they ranked first together with financial services companies) and second in Ghana. Moreover, the level of consumer data protection offered by healthcare providers was considered satisfactory (i.e., *sufficient* or *rather sufficient*) by a majority of professionals in all countries (see Fig. 50 below): 79 % of Chinese, 74 % of German, 74 % of Brazilian, 71 % of US, 63 % of Ghanaian, 56 % of Swiss, and 51 % of Japanese respondents were of this opinion.

20 All tables can be found at the end of this section (3.4.3.). This is because, at several points in the section, we refer to multiple such tables at once, and including them in the running text would unnecessarily disrupt the flow of the text.

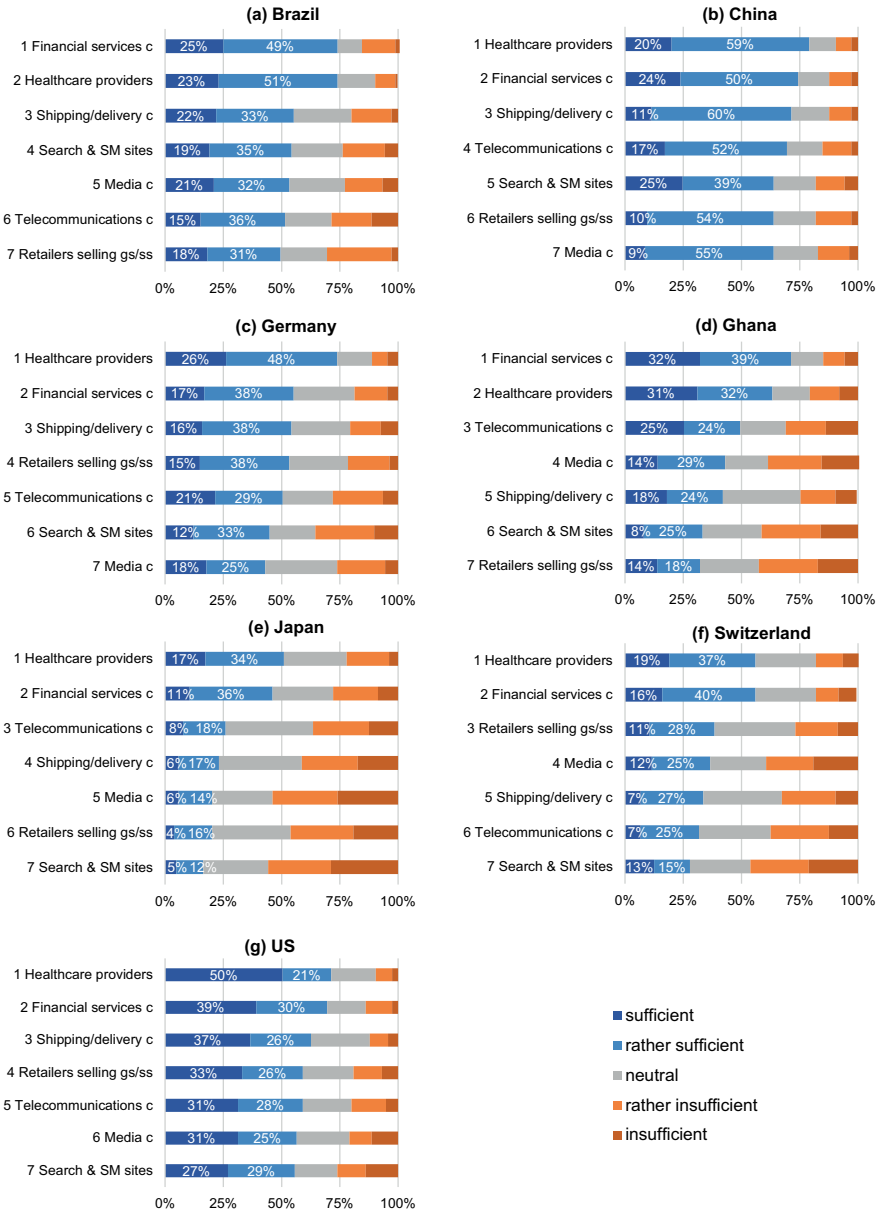

Fig. 49: Brazilian (a), Chinese (b), German (c), Ghanaian (d), Japanese (e), Swiss (f), and US (g) professionals' assessments of the levels of consumer data protection offered by seven industries in their countries.

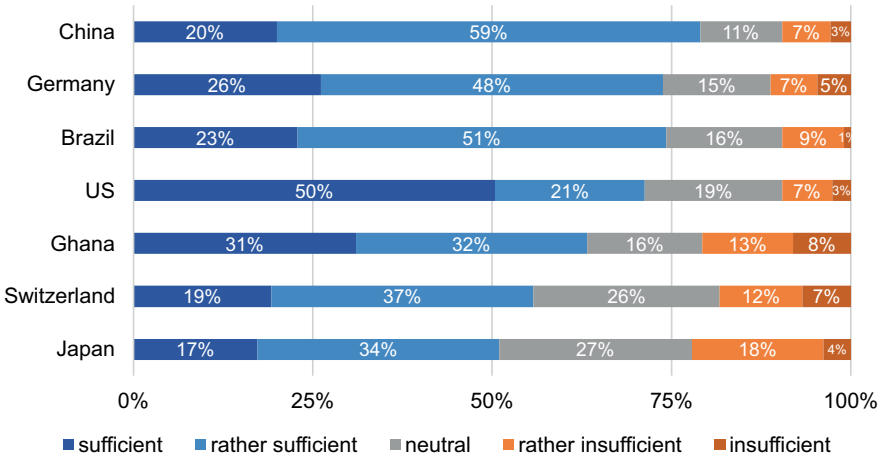

Fig. 50: Q17. Healthcare providers: How would you assess the level of consumer data protection in your country for the following industries?

A majority of professionals in all countries except for Japan were also satisfied with the consumer data protection provided by financial services companies (see Fig. 51). In both China and Brazil, 74 % of respondents considered the level of consumer data protection to be *sufficient* or *rather sufficient*, while this figure was 71 % in Ghana, 69 % in the United States, 56 % in Switzerland, and 55 % in Germany. However, only 47 % of Japanese respondents expressed that view for their country. As shown in Fig. 49, financial services companies ranked second in most countries (United States, Germany, China, and Japan) based on the percentage of respondents opting for *sufficient* or *rather sufficient*, and first in the remaining countries (Ghana; in Switzerland and Brazil, they ranked first together with healthcare providers).

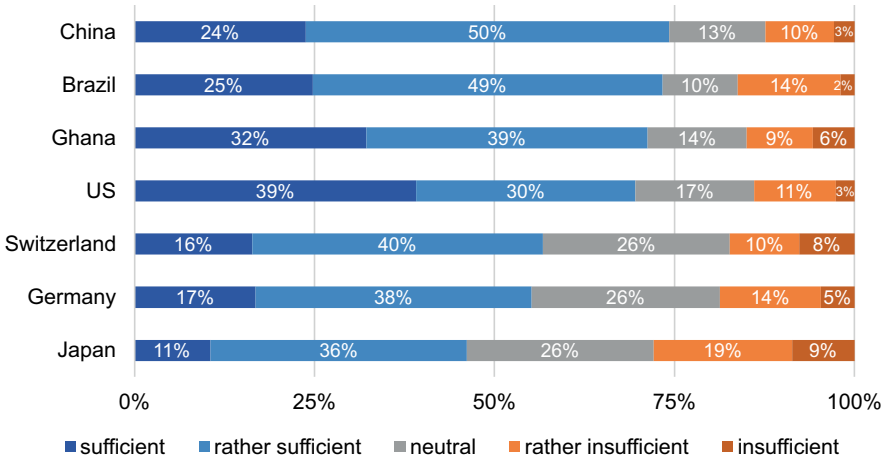

Fig. 51: Q17. Financial services companies: How would you assess the level of consumer data protection in your country for the following industry?

Thus, it appears that healthcare providers and financial services companies were regarded similarly highly in terms of the level of consumer data protection they were perceived to provide in the countries surveyed. It is noteworthy that they did not differ significantly from each other in this regard in any country except for Germany, where professionals regarded the level of consumer data protection offered by healthcare providers as significantly more sufficient than that provided by financial services companies ($p = 0.004$). The level of consumer data protection attributed to healthcare providers was indeed significantly higher than that attributed to most (i.e., at least four out of six) other industries in almost all countries (see Table 75, and Table 77–Table 81 in 3.4.3.). The exception here was China, where it significantly surpassed only two other industries (retailers at $p = 0.002$ and media companies at $p < 0.0005$). The comparatively high level of consumer data protection they were perceived to offer was thus also supported by statistical tests for all countries except China.

Financial services companies also significantly surpassed most other industries in terms of the level of consumer data protection they were perceived to provide in Brazil, Ghana, Japan, and Switzerland (see Table 75, and Table 78–Table 80). In the United States, they significantly surpassed search and social media sites ($p < 0.0005$), media companies ($p = 0.008$), and telecommunications companies ($p = 0.020$) in this regard. In China, they significantly surpassed media companies ($p = 0.005$) and retailers ($p = 0.002$), and in Germany they significantly surpassed search and social media sites ($p = 0.031$). The comparatively high level of consumer data protection that financial services companies were perceived to offer was thus

confirmed on the basis of statistical tests for Brazil, Ghana, Japan, and Switzerland, and to some extent for the United States.

In contrast, one industry whose level of consumer data protection was assessed as comparatively low was search and social media sites (Fig. 52). In only three countries was a majority of local professionals satisfied with the level of consumer data protection offered by this business sector (64 % in China, 56 % in the United States, and 54 % in Brazil), while only a minority in the remaining four countries expressed satisfaction. It is noteworthy that in Switzerland and Ghana, a greater proportion of respondents were dissatisfied with the level of consumer data protection in this industry than those who considered it satisfactory (46 % vs. 28 % for Switzerland, 41 % vs. 33 % for Ghana). In Japan, a majority of 56 % actually considered the level of consumer data protection provided by this sector to be *insufficient* or *rather insufficient*. If we compare the level of consumer data protection that search and social media sites were perceived to offer with that of other industries, we find that they were typically one of the bottom two industries regarding the proportion of respondents who considered the level of consumer data protection they offer to be *sufficient* or *rather sufficient* (see Fig. 49). This was the case for the United States, Germany, Switzerland, Japan, and Ghana. Indeed, search and social media sites received significantly lower ratings than most other industries in Germany, Ghana, and Japan (see Table 77–Table 79). In Switzerland and the United States, they received significantly lower ratings than three out of the six remaining industries (see Table 80 and Table 81). Thus, statistical tests confirmed the comparatively low level of consumer data protection that they were perceived to offer for Germany, Japan, and Ghana, and to some extent for the United States and Switzerland.

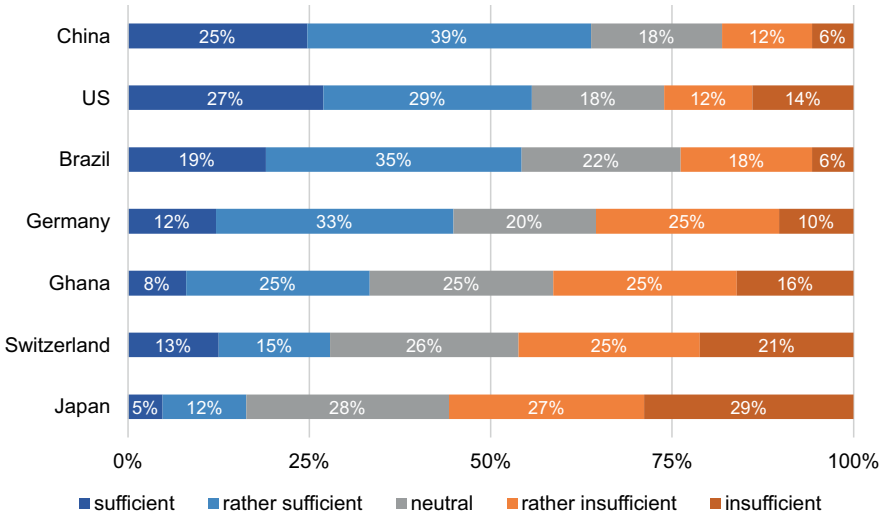

Fig. 52: Q17. Search and social media sites: How would you assess the level of consumer data protection in your country for the following industries?

Retailers selling goods and services were another industry seen to provide a comparatively low level of consumer data protection in most countries. As for search and social media sites, it was only in three countries that a majority of local professionals assessed the level of consumer data protection they provide as *sufficient* or *rather sufficient* (see Fig. 53): 64 % of Chinese, 59 % of US, and 53 % of German respondents held this view. In both Ghana and Japan, a greater proportion of respondents were dissatisfied with the level of consumer data protection afforded by this business sector than those who were content with it (42 % vs. 32 % for Ghana, 46 % vs. 20 % for Japan). If we compare the level of consumer data protection that they were perceived to offer with that of the other industries, we find that *retailers* were one of the bottom two industries in most countries (namely in China, Japan, Brazil, and Ghana; see Fig. 49). However, they only received significantly lower ratings than most other industries in Ghana (see Table 78) and significantly lower ratings than three out of the six remaining industries in Japan (see Table 79). In Brazil and China, only two other industries significantly surpassed retailers in terms of the level of consumer data protect they were seen to provide (see Table 75 and Table 76). This was also the case in Switzerland (Table 80). Thus, statistical tests confirmed the comparatively low level of consumer data protection that they were perceived to offer for Ghana alone and to some extent for Japan.

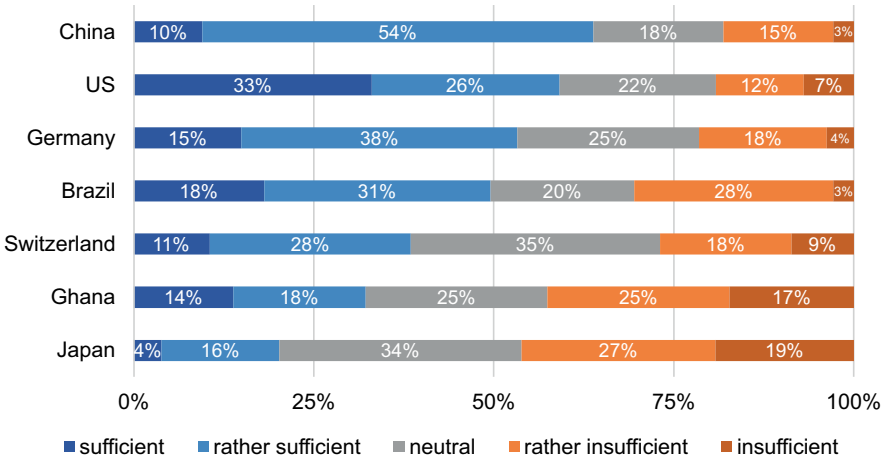

Fig. 53: Q17. Retailers selling goods and services: How would you assess the level of consumer data protection in your country for the following industries?

Media companies also tended to occupy the lower industry ranks in most countries (Fig. 49). Again, there were only three countries where a majority of professionals were satisfied with their level of consumer data protection these companies provided. These were the usual three suspects: China (64 %), the United States (56 %), and Brazil (53 %; see Fig. 54). It is noteworthy that a majority of Japanese professionals (54 %) was dissatisfied with the level of consumer data protection offered by media companies. In Switzerland, a slightly higher proportion of respondents (39 %) were dissatisfied with media companies than those who were (37 %). Media companies ranked last in Germany and China, second last in the United States, and third last in Japan and Brazil. However, it was only in Japan and the United States that they received significantly lower ratings than three of the remaining six industries (see Table 79 and Table 81). In all other countries, their ratings were significantly lower than only one or two other industries (see Table 75–Table 78, and Table 80). Statistical tests thus only somewhat confirmed the comparatively low level of consumer data protection they were perceived to offer in the United States and Japan.

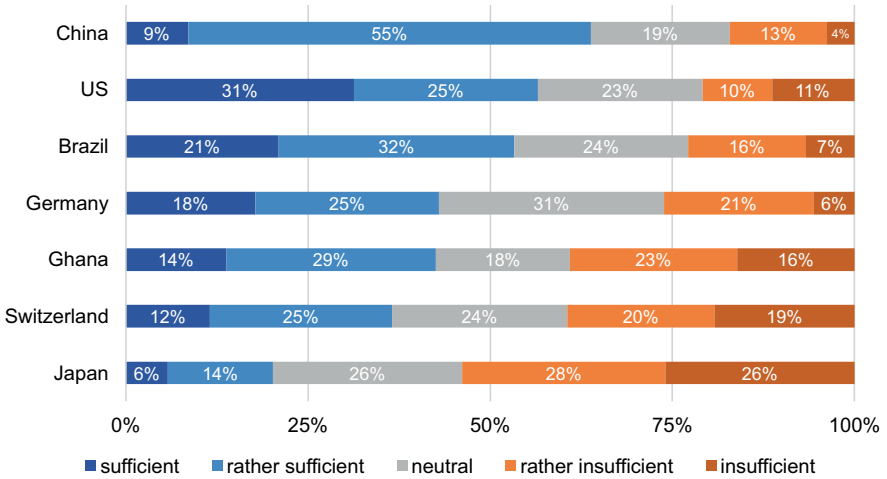

Fig. 54: Q17. Media companies: How would you assess the level of consumer data protection in your country for the following industries?

The last two industries to consider, shipping/delivery companies and telecommunications companies, typically placed in the industry midfield in terms of the level of consumer data protection they were perceived to offer. As regards shipping/delivery companies (see Fig. 55), the majority of professionals in four countries were content with the level of consumer data protection: 71 % of Chinese respondents, 63 % of the US professionals, 55 % of Brazilian, and 54 % of German respondents considered consumer data protection to be *sufficient* or *rather sufficient* in this sector. By contrast, in Japan, a markedly greater proportion of respondents regarded it as *insufficient* or *rather insufficient* (41 %) than those who deemed it *sufficient* or *rather sufficient* (23 %). Shipping/delivery companies ranked third in most countries (the United States, Germany, China, and Brazil) and either fourth or fifth in the remaining three countries. Accordingly, they only received significantly lower ratings than two other industries at most in all countries and significantly higher ratings than two other industries at most in all countries (see Table 75–Table 81).

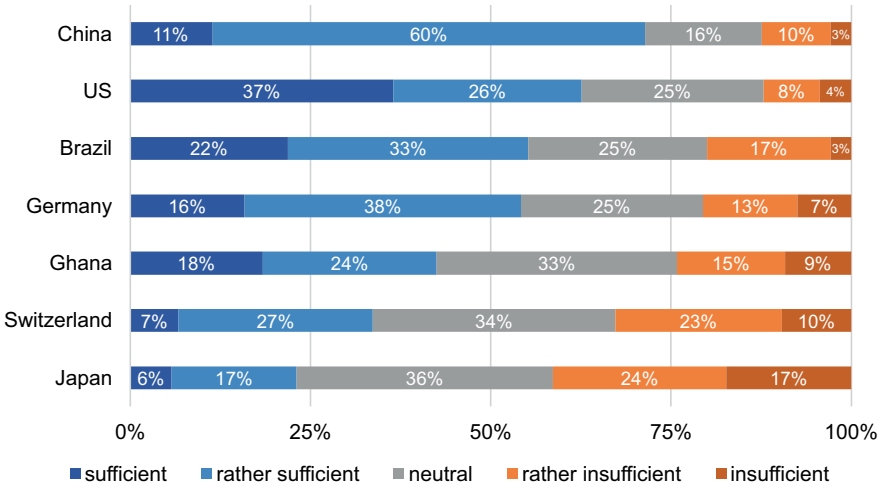

Fig. 55: Q17. Shipping/delivery companies: How would you assess the level of consumer data protection in your country for the following industries?

Moving on to telecommunications companies (Fig. 56), their level of consumer data protection was regarded as satisfactory (i.e., as *sufficient* or *rather sufficient*) by a majority of professionals in three countries: 69 % of Chinese, 59 % of US, and 51 % of Brazilian professionals expressed this view. Half of German respondents (50 %) felt the same way. In contrast, in both Switzerland and Japan, a greater proportion of respondents regarded the level of consumer data protection in this business sector as *insufficient* or *rather insufficient* than those who were content with it (38 % vs. 32 % for Switzerland, 37 % vs. 26 % for Japan). The ranking of telecommunications companies varied, from third place in Japan and Ghana to sixth place in Brazil and Switzerland. In Japan, they were rated significantly higher than three other industries ($p < 0.0005$ and $p = 0.031$) in terms of the level of consumer data protection they were seen to offer, while this figure was only two in Ghana ($p = 0.007$, $p = 0.013$). In contrast, their level of consumer data protection was rated significantly lower in Brazil than that of three other industries ($p < 0.0005$ and $p = 0.021$). In the remaining six countries, they received significantly lower ratings than at most two industries (see Table 76–Table 81). Thus, statistical tests suggested that, when compared with other industries, telecommunications companies were perceived to offer somewhat more consumer data protection in Japan and somewhat less consumer data protection in Brazil.

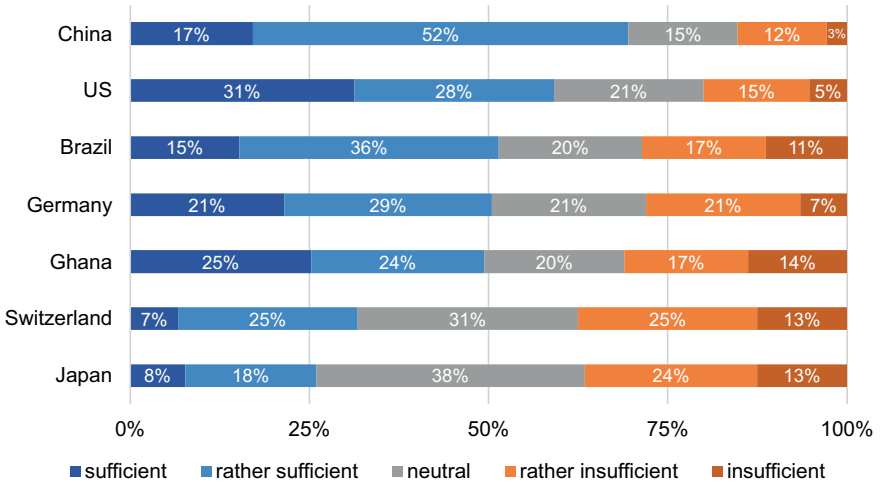

Fig. 56: Q17. Telecommunications companies: How would you assess the level of consumer data protection in your country for the following industries?

3.4.2 High-satisfaction countries and low-satisfaction countries

Let us now consider differences between the seven countries regarding the ratings they assigned the levels of consumer data protection in different business sectors. As with the trust ratings (section 3.2.) and perceived compliance ratings (section 3.3), we found significant, cross-cultural differences regarding the perceived levels of consumer data protection in each of the seven industries ($p < 0.0005$; for details, see Table 82, section 3.4.3.). Again, countries appear to fall into two different groups: high-satisfaction countries on the one hand and low-satisfaction countries on the other. As with the trust ratings (see section 3.2.2) and the compliance ratings (see section 3.3.2), the United States and China fall into the former group (see Fig. 57). They are in fact the only countries where local professionals indicated that consumer data protection was satisfactory in *all* the industries surveyed. In Brazil, professionals indicated this for all industries except *retailers*, so we can also include Brazil in this group. This classification is supported by the fact that the ratings given by US. Chinese, and Brazilian respondents did not differ significantly from each other for any of the industries surveyed (see Table 83–Table 89).

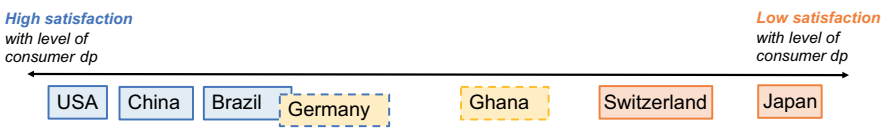

Fig. 57: Scale of satisfaction with level of consumer data protection.

The country that contrasted most strongly with these high-satisfaction countries was Japan, where satisfaction with consumer data protection levels was generally low. Japanese professionals were the only ones who predominantly indicated that the data protection provided by search and social media sites (56 %) and media companies (54 %) in their country was *rather insufficient* or *insufficient* and consequently in need of improvement. Japanese respondents considered the level of consumer data protection in both industries to be significantly less sufficient than respondents in most other countries ($p < 0.0005$, except for Ghana regarding media companies, where $p = 0.049$). The exceptions to this trend were Switzerland and Ghana for search and social media sites and Switzerland for media companies. Japan also stood out as it was the only country where only a single industry (healthcare providers) was considered satisfactory in terms of consumer data protection. In Switzerland and Ghana, there were only two such industries (healthcare providers and financial services companies). All this suggests that Japan should be classified as a low-satisfaction country. This classification is also supported by the fact that Japanese professionals considered the level of consumer data protection provided by each of the industries surveyed to be significantly less sufficient than US and Chinese respondents did (see Table 83–Table 89). Japan also contrasts with Brazil, with Brazilian sufficiency ratings significantly higher than Japanese ones for six out of seven industries (the exception being telecommunications companies). We can thus classify Japan as a low-satisfaction country vis-à-vis the three high-satisfaction countries: the United States, China, and Brazil.

Let us now turn to Switzerland and Ghana, which seem fairly similar to Japan in terms of how local professionals perceived the level of consumer data protection provided there. As mentioned above, we generally found that the majority of professionals there considered consumer data protection in the industries surveyed to be neutral or unsatisfactory rather than satisfactory.

Indeed, Japanese and Swiss sufficiency ratings were very similar: They did not differ significantly for any industry except for retailers (see Table 83–Table 89), with Swiss ratings significantly higher than Japanese ones ($p = 0.007$). Thus, Switzerland could also fall in the category of low-satisfaction countries. This classification is supported by the fact that Switzerland contrasts with the United States and China in a manner similar to Japan: Swiss ratings were significantly lower than US ratings for all industries (see Table 83–Table 89) and significantly lower than Chinese ratings regarding four out of seven industries ($p < 0.0005$ for shipping/delivery companies, telecommunications companies, and search and social media sites; and $p = 0.004$ for media companies). However, Switzerland only differed significantly from Brazil regarding three out of seven industries, with Brazilian ratings significantly surpassing Swiss ones for shipping/delivery companies ($p = 0.006$), search and social media sites ($p = 0.001$), and media companies ($p = 0.032$). We can thus clas-

sify Switzerland as a low-satisfaction country vis-à-vis the United States and China, whereas this trend was less clear vis-à-vis Brazil.

Ghanaian sufficiency ratings were also similar to Japanese ratings most of the time, but significantly surpassed them for financial services companies ($p = 0.001$), shipping/delivery companies ($p = 0.014$), and media companies ($p = 0.049$). In fact, Ghanaian ratings were more similar to Brazilian and Chinese ratings than to Japanese ones, as they only differed significantly from Brazilian ratings for search and social media sites ($p = 0.010$) and from Chinese ratings regarding search and social media sites ($p < 0.0005$) and retailers ($p = 0.002$). They were, however, significantly lower than US ratings regarding four out of seven industries ($p = 0.014$ for shipping/delivery companies, $p < 0.0005$ for retailers, $p = 0.013$ for search and social media sites, and $p = 0.049$ for media companies). Ghanaian ratings were most similar to Swiss ones, from which they never significantly differed (see Table 83–Table 89). Thus, Ghana is probably best classified in an intermediate category between high-satisfaction and low-satisfaction countries (see Fig. 57, p. 104).

The last country that remains to be classified is Germany. German professionals were mostly satisfied with the levels of consumer data protection provided by the surveyed industries, with a majority considering consumer data protection *sufficient* or *rather sufficient* in four industries and 50 % considering it *sufficient* or *rather sufficient* in telecommunications companies. However, no such majority was found for search and social media sites or media companies. The ratings assigned by German professionals to the levels of consumer data protection provided by various industries were similar to those in almost all other countries, with the exception of Japan, as we will see below. German ratings were most similar to Brazilian ratings, from which they never significantly differed (see Table 83–Table 89). Moreover, they only differed significantly from US. Chinese, Swiss, and Ghanaian ratings regarding a single industry, with German ratings significantly lower than US ratings for financial services companies ($p = 0.024$) and Chinese ratings for search and social media sites ($p = 0.013$), and significantly surpassing Swiss ratings for shipping/delivery companies ($p = 0.032$) and Ghanaian ratings for retailers ($p = 0.018$). In contrast, German ratings significantly surpassed Japanese ratings for all industries surveyed except financial services companies (see Table 83–Table 89). Like Ghana, Germany is thus probably best classified in an intermediate category between high-satisfaction and low-satisfaction countries, leaning slightly more toward the former than the latter.

3.4.3 Tables

Industry comparison

Table 74: Output of Friedman's ANOVAS regarding differences in the levels of consumer data protection that the seven industries were perceived to provide by country.

	χ^2	*df*	*p*
Brazil	54.23	6	< 0.0005***
China	36.30	6	< 0.0005***
Germany	41.99	6	< 0.0005***
Ghana	100.90	6	< 0.0005***
Japan	147.19	6	< 0.0005***
Switzerland	74.85	6	< 0.0005***
US	69.06	6	< 0.0005***

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 75: *P* values of pairwise Wilcoxon signed rank tests regarding differences in the levels of consumer data protection the seven industries were perceived to provide by Brazilian respondents.

	Healthcare providers	**Financial services c**	**Shipping/ Delivery c**	**Media c**	**Search & SM sites**	**Retailers selling Gs/Ss**
Financial services c	1.000					
Shipping/ delivery c	0.017*	0.230				
Media c	0.001**	0.015*	1.000			
Search & SM sites	< 0.0005***	0.011*	1.000	1.000		
Retailers selling Gs/Ss	< 0.0005***	0.001**	0.230	1.000	1.000	
Telecommu-nications c	< 0.0005***	< 0.0005***	0.021*	0.548	0.818	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 76: *P* values of pairwise Wilcoxon signed rank tests regarding differences in the levels of consumer data protection the seven industries were perceived to provide by Chinese respondents.

	Healthcare providers	Financial services c	Telecommu-nications c	Shipping/ Delivery c	Search & SM sites	Retailers selling Gs/Ss
Financial services c	1.000					
Telecommu-nications c	0.576	0.688				
Shipping/ delivery c	0.247	0.576	1.000			
Search & SM sites	0.576	0.576	1.000	1.000		
Retailers selling Gs/Ss	0.002**	0.002**	0.576	0.417	0.725	
Media c	< 0.0005***	0.005*	0.688	0.576	0.688	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 77: *P* values of pairwise Wilcoxon signed rank tests regarding differences in the levels of consumer data protection the seven industries were perceived to provide by German respondents.

	Healthcare providers	Financial services c	Retailers selling Gs/Ss	Shipping/ Delivery c	Telecommu-nications c	Media c
Financial services c	0.004**					
Retailers selling Gs/Ss	0.008*	1.000				
Shipping/ delivery c	0.012*	1.000	1.000			
Telecommu-nications c	0.002**	1.000	1.000	1.000		
Media c	< 0.0005***	0.557	1.000	1.000	1.000	
Search & SM sites	< 0.0005***	0.031*	0.031*	0.049*	0.119	0.622

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 78: *P* values of pairwise Wilcoxon signed rank tests regarding differences in the levels of consumer data protection the seven industries were perceived to provide by Ghanaian respondents.

	Financial services c	Healthcare providers	Telecommu-nications c	Shipping/ Delivery c	Media c	Retailers selling Gs/Ss
Healthcare providers	0.295					
Telecommu-nications c	0.002**	0.082				
Shipping/ delivery c	< 0.0005***	0.042*	1.000			
Media c	< 0.0005***	0.001**	0.157	0.295		
Retailers selling Gs/Ss	< 0.0005***	< 0.0005***	0.013*	0.001**	0.736	
Search & SM sites	< 0.0005***	< 0.0005***	0.007*	0.013*	0.422	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 79: *P* values of pairwise Wilcoxon signed rank tests regarding differences in the levels of consumer data protection the seven industries were perceived to provide by Japanese respondents.

	Healthcare providers	Financial services c	Telecommu-nications c	Shipping/ Delivery c	Retailers selling Gs/Ss	Media c
Financial services c	0.088					
Telecommu-nications c	< 0.0005***	< 0.0005***				
Shipping/ delivery c	< 0.0005***	< 0.0005***	0.376			
Retailers selling Gs/Ss	< 0.0005***	< 0.0005***	0.031*	0.506		
Media c	< 0.0005***	< 0.0005***	< 0.0005***	0.161	0.506	
Search & SM sites	< 0.0005***	< 0.0005***	< 0.0005***	0.005*	0.088	0.506

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 80: *P* values of pairwise Wilcoxon signed rank tests regarding differences in the levels of consumer data protection the seven industries were perceived to provide by Swiss respondents.

	Healthcare providers	Financial services c	Retailers selling Gs/Ss	Shipping/ Delivery c	Media c	Telecommu-nications c
Financial services c	1.000					
Retailers selling Gs/Ss	0.018*	0.030*				
Shipping/ delivery c	0.001**	< 0.0005***	0.519			
Media c	0.001**	< 0.0005***	0.216	1.000		
Telecommu-nications c	< 0.0005***	< 0.0005***	0.164	1.000	1.000	
Search & SM sites	< 0.0005***	< 0.0005***	0.002**	0.226	0.787	0.787

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 81: *P* values of pairwise Wilcoxon signed rank tests regarding differences in the levels of consumer data protection the seven industries were perceived to provide by US respondents.

	Healthcare providers	Financial services c	Shipping/ Delivery c	Retailers selling Gs/Ss	Telecommu-nications c	Media c
Financial services c	0.094					
Shipping/ delivery c	0.008*	0.683				
Retailers selling Gs/Ss	0.001**	0.143	0.219			
Telecommu-nications c	< 0.0005***	0.020*	0.146	0.922		
Media c	< 0.0005***	0.008*	0.011*	0.683	0.683	
Search & SM sites	< 0.0005***	< 0.0005***	< 0.0005***	0.094	0.180	0.316

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Country comparison

Table 82: Output of Kruskal-Wallis tests regarding cross-cultural differences in respondents' perceptions of the level of consumer data protection provided by a particular industry.

	H	*df*	*p*
Healthcare providers	34.02	6	< 0.0005***
Financial services companies	39.54	6	< 0.0005***
Shipping/delivery companies	76.59	6	< 0.0005***
Telecommunications companies	49.81	6	< 0.0005***
Retailers selling goods and services	65.13	6	< 0.0005***
Search and social media sites	79.72	6	< 0.0005***
Media companies	63.07	6	< 0.0005***

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 83: *P* values of pairwise Wilcoxon signed rank tests regarding the level of consumer data protection healthcare providers were perceived to provide in different countries.

	US	Brazil	China	Germany	Ghana	Switzerland
Brazil	0.175					
China	0.171	1.000				
Germany	0.217	1.000	1.000			
Ghana	0.140	1.000	1.000	1.000		
Switzerland	0.001**	0.198	0.171	0.198	1.000	
Japan	< 0.0005***	0.040*	0.024*	0.041*	0.744	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 84: *P* values of pairwise Wilcoxon signed rank tests regarding the level of consumer data protection financial services companies were perceived to provide in different countries.

	US	China	Ghana	Brazil	Germany	Switzerland
China	1.000					
Ghana	1.000	1.000				
Brazil	1.000	1.000	1.000			
Germany	0.024*	0.169	0.169	0.214		
Switzerland	0.028*	0.180	0.180	0.234	1.000	
Japan	< 0.0005***	0.001**	0.001**	0.001**	0.595	0.586

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 85: *P* values of pairwise Wilcoxon signed rank tests regarding the level of consumer data protection shipping/delivery companies were perceived to provide in different countries.

	US	China	Brazil	Germany	Ghana	Switzerland
China	0.650					
Brazil	0.377	1.000				
Germany	0.073	0.555	1.000			
Ghana	0.014*	0.088	0.650	1.000		
Switzerland	< 0.0005***	< 0.0005***	0.006*	0.032*	0.555	
Japan	< 0.0005***	< 0.0005***	< 0.0005***	< 0.0005***	0.014*	0.543

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 86: *P* values of pairwise Wilcoxon signed rank tests regarding the level of consumer data protection telecommunications companies were perceived to provide in different countries.

	China	US	Germany	Ghana	Brazil	Switzerland
US	1.000					
Germany	0.599	0.653				
Ghana	0.653	0.653	1.000			
Brazil	0.185	0.227	1.000	1.000		
Switzerland	< 0.0005***	< 0.0005***	0.056	0.227	0.185	
Japan	< 0.0005***	< 0.0005***	0.025*	0.170	0.088	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 87: *P* values of pairwise Wilcoxon signed rank tests regarding the level of consumer data protection retailers selling goods and services were perceived to provide in different countries.

	US	China	Germany	Brazil	Switzerland	Ghana
China	0.956					
Germany	0.552	0.956				
Brazil	0.297	0.956	0.956			
Switzerland	0.008*	0.054	0.440	0.956		
Ghana	< 0.0005***	0.002**	0.018*	0.106	0.738	
Japan	< 0.0005***	< 0.0005***	< 0.0005***	< 0.0005***	0.007*	0.956

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 88: *P* values of pairwise Wilcoxon signed rank tests regarding the level of consumer data protection search and social media sites were perceived to provide in different countries.

	China	US	Brazil	Germany	Ghana	Switzerland
US	1.000					
Brazil	0.637	1.000				
Germany	0.013*	0.355	0.355			
Ghana	< 0.0005***	0.013*	0.010*	0.610		
Switzerland	< 0.0005***	0.002**	0.001**	0.231	1.000	
Japan	< 0.0005***	< 0.0005***	< 0.0005***	< 0.0005***	0.066	0.355

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 89: *P* values of pairwise Wilcoxon signed rank tests regarding the level of consumer data protection media companies were perceived to provide in different countries.

	US	China	Brazil	Germany	Ghana	Switzerland
China	1.000					
Brazil	1.000	1.000				
Germany	0.423	0.639	1.000			
Ghana	0.049*	0.080	0.233	0.984		
Switzerland	0.004**	0.004**	0.032*	0.287	1.000	
Japan	< 0.0005***	< 0.0005***	< 0.0005***	< 0.0005***	0.049*	0.158

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

3.5 Enforcement of consumer data protection

Respondents were also asked to assess the enforcement of consumer data protection by the government and private parties, and within companies in their country on a five-point scale (*heavily – robustly – moderately – to a limited extent – not at all*).

Regarding respondents' assessments of government enforcement, we found significant cross-cultural differences across the countries examined , $H(6) = 70.15$, $p < 0.0005$. As can be seen in Fig. 58, a majority of professionals in all countries except for Ghana and Japan believed that their government enforced consumer data protection *heavily* or *robustly*. China stood out, with a total of 75 % of respondents expressing this view—in comparison to 58 % in Brazil, 54 % in Germany, 52 % in Switzerland, and 51 % in the United States. Only a small minority of Ghanaian

(25 %) and Japanese (20 %) respondents said the same for their countries. In both of those countries, the numbers of professionals who said that the enforcement of consumer data protection was moderate (Ghana 44 %, Japan 42 %), or either limited or non-existent (38 % for Japan, 31 % for Ghana) was relatively high in comparison to the other countries. Indeed, Japanese professionals rated government enforcement as significantly weaker than respondents in all other countries ($p < 0.0005$ each) except for Ghana ($p = 1.000$) did. Whereas the contrast with China amounted to a large effect ($r = 0.53$), the contrasts with the remaining countries amounted to medium effects (with r ranging from 0.31 to 0.38; see Table 91). Similarly, Ghanaian respondents perceived government enforcement to be significantly weaker than respondents in China, Brazil, and Germany did (with p ranging from < 0.0005 to 0.024; see Table 90), with the contrast with China amounting to a medium effect ($r = 0.38$) and the contrasts with the remaining countries amounting to small-to-medium effects ($r = 0.22$, $r = 0.25$). Finally, Swiss respondents also assessed their government's enforcement of consumer data protection as significantly weaker than those in China did ($p = 0.006$), amounting to a small-to-medium effect ($r = 0.24$).

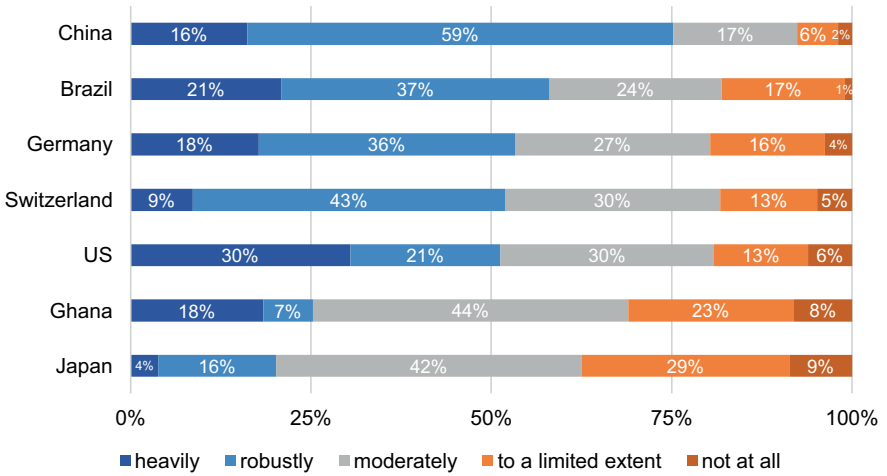

Fig. 58: Q14. How would you assess the enforcement of consumer data protection by the government in your country? It is enforced ...

Table 90: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' assessments of their government's enforcement of consumer data protection.

	Japan	Ghana	Switzerland	Germany	Brazil	US
Ghana	1.000					
Switzerland	< 0.0005***	0.124				
Germany	< 0.0005***	0.054	1.000			
Brazil	< 0.0005***	0.008*	1.000	1.000		
US	< 0.0005***	0.024*	1.000	1.000	1.000	
China	< 0.0005***	< 0.0005***	0.006*	0.133	1.000	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 91: Effect sizes for significant differences in respondents' assessments of their government's enforcement of consumer data protection.

Contrast		*r*
Japan	Brazil	0.38
	China	0.53
	Germany	0.33
	Switzerland	0.31
	US	0.34
Ghana	Brazil	0.25
	China	0.38
	US	0.22
Switzerland	China	0.24

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

Based on these results, we again clustered countries into different groups according to perceived levels of government enforcement of consumer data protection. Ghana and, in particular, Japan can be classified as countries with "low perceived government enforcement" (see Fig. 59). China constitutes the opposite pole as a country with "high perceived government enforcement" in this regard, not only due to the large majority of Chinese people who considered government enforcement to be heavy or robust but also because Chinese enforcement ratings significantly surpassed those of three other countries (Japan, Ghana, and Switzerland). The remaining countries—the United States, Switzerland, Germany, and Brazil—constitute intermediate cases, with the United States and Brazil appearing to lean more toward

the countries with high perceived government enforcement (as they significantly surpassed both Japanese and Ghanaian ratings in this respect).

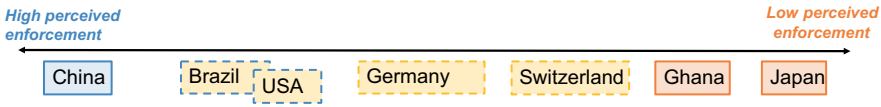

Fig. 59: Scale of perceived government enforcement of consumer data protection.

We also found significant cross-cultural differences regarding respondents' assessments of the enforcement of consumer data protection by private parties, $H(6) = 81.57$, $p < 0.0005$. Fig. 60 shows that private parties play a dominant role in terms of the heavy or robust enforcement of consumer data protection in China, Brazil, and the United States according to professionals' assessments (with 70 % choosing these answer options in China, 65 % in Brazil, and 53 % in the United States). Again, enforcement by private parties was considered to be limited or non-existent by the largest proportions of respondents from Japan (45 %) and Ghana (31 %), with Switzerland following closely at 29 %. Japanese professionals stood out in that they considered enforcement by private parties to be significantly weaker than respondents in all other countries did (with p ranging from < 0.0005 to 0.029; see Table 92). This difference amounted to or approached a large effect size regarding China ($r = 0.51$) and Brazil ($r = 0.49$), and amounted to a medium effect size regarding Germany and the United States ($r = 0.30$, $r = 0.38$), and a small effect size regarding the remaining countries (see Table 93). Moreover, German, Swiss, and Ghanaian respondents assessed enforcement by private parties as significantly weaker than Brazilian and Chinese respondents did (with p ranging from < 0.0005 to 0.023), with the contrasts Switzerland-Brazil and Switzerland-China constituting medium effects ($r = 0.32$, $r = 0.34$) and those involving Germany and Ghana constituting small-to-medium effects ($r = 0.22$, $r = 0.24$). In addition, Swiss respondents assessed enforcement by private parties as being significantly weaker than US respondents did ($p = 0.012$), another small-to-medium effect ($r = 0.23$).

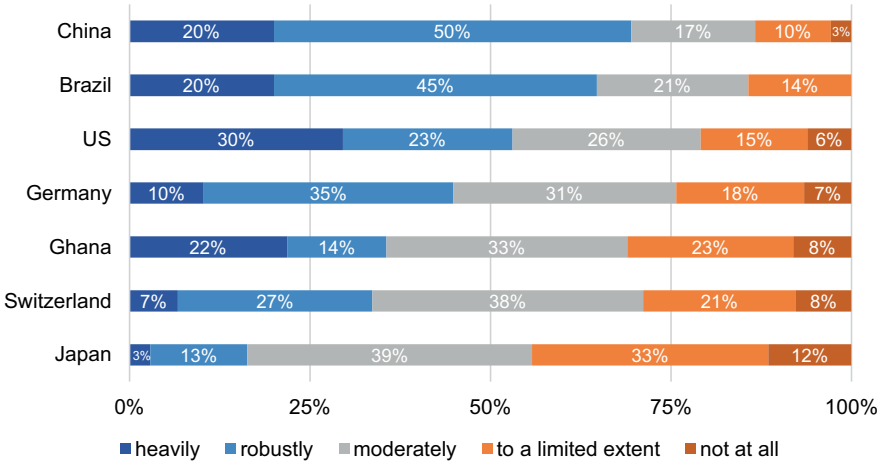

Fig. 60: Q15. How would you assess the enforcement of consumer data protection by private parties in your country? It is enforced ...

Table 92: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' assessments of the enforcement of consumer data protection by private parties.

	Japan	Switzerland	Ghana	Germany	US	Brazil
Switzerland	0.029*					
Ghana	0.026*	1.000				
Germany	< 0.0005***	0.818	1.000			
US	< 0.0005***	0.012*	0.244	0.255		
Brazil	< 0.0005***	< 0.0005***	0.023*	0.020*	1.000	
China	< 0.0005***	< 0.0005***	0.012*	0.006*	1.000	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 93: Effect sizes for significant differences in respondents' assessments of the enforcement of consumer data protection by private parties.

Contrast		*r*
Japan	Brazil	0.49
	China	0.51
	Germany	0.30
	Ghana	0.22
	Switzerland	0.20
	US	0.38
Switzerland	Brazil	0.32
	China	0.34
	US	0.23
Ghana	Brazil	0.22
	China	0.24
Germany	Brazil	0.22
	China	0.24

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

Japan can thus be characterized as a country with "low perceived enforcement by private parties," while China and Brazil can be classified as countries with "high perceived enforcement" in this respect (see Fig. 61). The United States, Germany, Ghana, and Switzerland constitute intermediate cases, with the United States leaning more strongly toward the countries with high perceived enforcement and Switzerland more strongly toward those with low perceived enforcement.

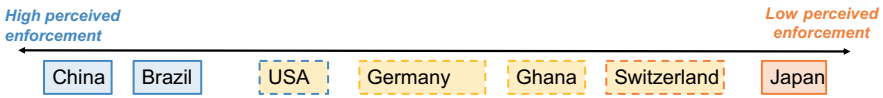

Fig. 61: Scale of perceived enforcement of consumer data protection by private parties.

Finally, we also found significant cross-cultural differences regarding respondents' assessments of the corporate enforcement of consumer data protection, $H(6) = 58.91$, $p < 0.0005$. Enforcement within companies was again rated as heavy or robust by the majority of respondents from China (65 %), Brazil (57 %), and the United States (54 %) (see Fig. 62), with the highest percentage of ratings for *heavily* found in the United States (31 %). In Japan, Switzerland, and Ghana, comparatively

large percentages of professionals considered enforcement to be limited or non-existent (Japan 39 %, Switzerland 28 %, Ghana 22 %) or moderate (Ghana 44 %, Japan 41 %, Switzerland 36 %). Once again, Japanese professionals stood out in that they assessed corporate enforcement as significantly weaker than respondents in all other countries (with p ranging from < 0.0005 to 0.023; see Table 94) except Switzerland (p = 0.079) did. This difference amounted to a medium-to-large effect regarding China (r = 0.46) and a medium effect regarding Brazil (r = 0.38) and the United States (r = 0.39). The remaining contrasts constituted small-to-medium effects (see Table 95). Moreover, both Swiss and Ghanaian respondents assessed the enforcement of consumer data protection within companies in their country as significantly weaker than Chinese respondents did (p = 0.003, p = 0.036), while Swiss respondents additionally assessed it as significantly weaker than US respondents did (p = 0.028). All these contrasts amounted to small-to-medium effects (r = 0.26, r = 0.22, r = 0.21).

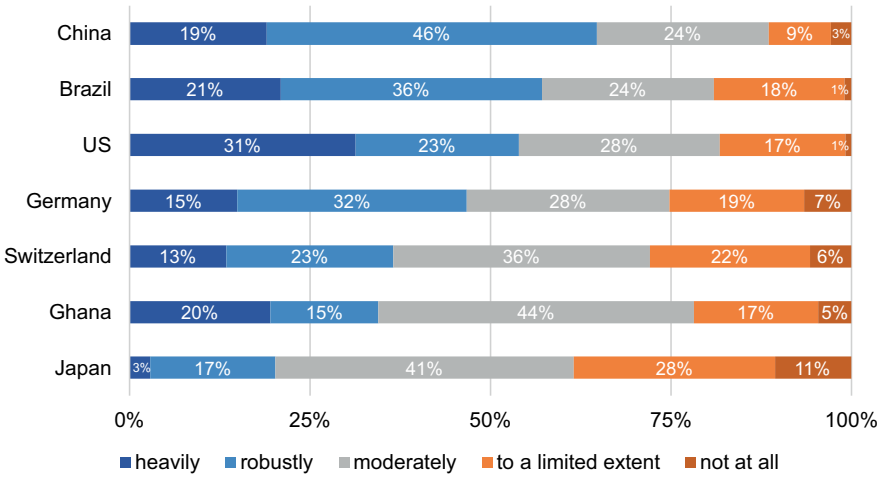

Fig. 62: Q16. How would you assess the enforcement of consumer data protection within companies in your country? It is enforced ...

Table 94: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' assessments of the enforcement of consumer data protection within companies.

	Japan	Switzerland	Ghana	Germany	Brazil	US
Switzerland	0.079					
Ghana	0.023*	1.000				
Germany	0.003**	1.000	1.000			
Brazil	< 0.0005***	0.078	0.358	0.577		
US	< 0.0005***	0.028*	0.200	0.247	1.000	
China	< 0.0005***	0.003**	0.036*	0.092	1.000	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 95: Effect sizes for significant differences in respondents' assessments of the enforcement of consumer data protection within companies.

Contrast		*r*
Japan	Brazil	0.38
	China	0.46
	Ghana	0.23
	Germany	0.26
	US	0.39
Switzerland	China	0.26
	US	0.21
Ghana	China	0.22

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

Japan can thus be characterized as a country with "low perceived corporate enforcement," while China can be classified as a country with "high perceived corporate enforcement" (see Fig. 63), as Chinese corporate enforcement ratings significantly surpassed those of three other countries (Japan, Switzerland, and Ghana). The remaining countries—the United States, Brazil, Germany, Ghana, and Switzerland—are best classified as intermediate cases, with the United States leaning more strongly toward the countries with high perceived corporate enforcement. By contrast, Ghana and Switzerland leaned slightly more toward the countries with low perceived corporate enforcement.

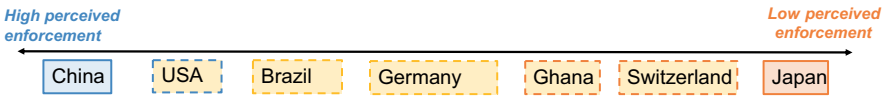

Fig. 63: Scale of perceived enforcement of consumer data protection within companies.

3.6 Sufficiency of current regulations to prevent the misuse of consumer data

We also asked respondents to rate the sufficiency of their country's current regulations to prevent the corporate misuse of consumer data, using the same five-point scale as in previous sections (*sufficient – rather sufficient – neutral – rather insufficient – insufficient*). A Kruskal-Wallis test showed significant differences across the surveyed countries in this regard, $H(6) = 65.619$, $p < 0.0005$. Fig. 64 shows that, in most countries (China, Brazil, the United States, and Germany), a majority of respondents considered current regulations to be *sufficient* or *rather sufficient* to ensure that companies did not misuse consumers' personal data for purposes other than those stated. In Ghana, 50 % of professionals held this view. Regulations were considered to be *sufficient* or *rather sufficient* to counteract the misuse of consumer data by companies in the United States (67 % of respondents), Brazil (68 %), and China (71 %) in particular. It is noteworthy that the United States was the country where the biggest proportion of respondents (40 %) considered regulations to be *sufficient* (not just *rather sufficient*).

In contrast, in Switzerland and Japan, only a minority believed that regulations were *sufficient* or *rather sufficient* to prevent the corporate misuse of consumer data (47 % and 29 % respectively). Notably, Japan was the only country where a greater proportion of people believed regulation to be *insufficient* or *rather insufficient* (43 %) than those who believed it to be *sufficient* or *rather sufficient* (29 %). Indeed, Japanese respondents' sufficiency ratings were significantly lower than those given by respondents in all other countries ($p < 0.0005$ or $p = 0.017$, depending on the contrast; see Table 96). These differences amounted to medium-to-large effects for the contrasts with Brazil ($r = 0.40$), China ($r = 0.44$), and the United States ($r = 0.43$); a medium effect for the contrast Japan-Germany ($r = 0.31$); and a small-to-medium effect for the remaining contrasts (see Table 97). Swiss respondents' ratings were significantly lower than those given by Brazilian ($p = 0.024$, $r = 0.22$), Chinese ($p = 0.012$, $r = 0.23$), and US respondents ($p = 0.001$, $r = 0.28$). These differences all constituted small-to-medium effects.

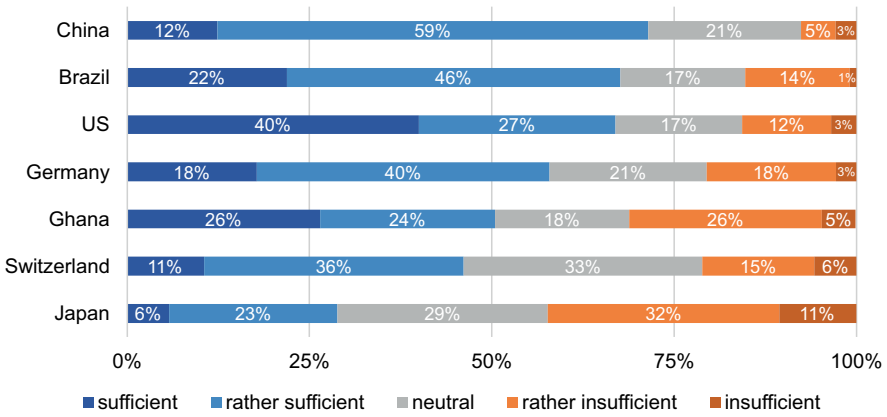

Fig. 64: Q18. Current regulation in my country is ... to ensure that companies do not misuse consumers' personal data for purposes other than those stated.

Table 96: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' assessments of the sufficiency of their country's regulations to prevent the corporate misuse of data.

	Japan	Switzerland	Ghana	Germany	Brazil	China
Switzerland	0.017*					
Ghana	0.017*	1.000				
Germany	< 0.0005***	0.930	1.000			
Brazil	< 0.0005***	0.024*	0.930	0.930		
China	< 0.0005***	0.012*	0.930	0.930	1.000	
US	< 0.0005***	0.001**	0.088	0.083	0.930	0.580

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 97: Effect sizes for significant differences in respondents' assessments of the sufficiency of their country's regulations to prevent the corporate misuse of data.

Contrast		*r*
Japan	Switzerland	0.23
	Brazil	0.40
	China	0.44
	Germany	0.31
	Ghana	0.24
	US	0.43
Switzerland	Brazil	0.22
	China	0.23
	US	0.28

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

4 Impact of data protection and informational privacy regulations

The survey items presented in this section were designed to examine what professionals thought about the impact of their country's data protection and informational privacy regulations on

- the relationship between data protection and the degree of freedom enjoyed by companies to use data (customer orientation, ability to innovate, cooperation with other companies, transnational data flow);
- bureaucracy, the amount of information that must be processed, the professional and flexible handling of data, and privacy management; and
- fundamental rights, digitalization, and their overall effect.

4.1 … on companies with regard to customer orientation, innovation, and cooperation

Respondents were first asked to indicate their agreement with several statements concerning the impact of their country's data protection and informational privacy regulations on companies. They were asked whether they believed that their countries' regulations still allowed companies to

(1) tailor their products and services to consumers' needs;

(2) develop new products and services;
(3) cooperate with other companies in their country;
(4) cooperate with companies in other countries with essentially equivalent data protection and informational privacy regulations; and
(5) cooperate with companies in other countries, no matter how they regulate data protection and informational privacy.

For all statements, we found significant cross-cultural differences between respondents' levels of agreement ($p < 0.0005$; see Table 98). In the following, we will examine these differences in more detail for each statement.

Table 98: Output of Kruskal-Wallis tests regarding cross-cultural differences in respondents' agreement with statements concerning the impact of their country's regulation of data protection and informational privacy on companies. Regulation still allows companies …

	H	*df*	*p*
(1) to tailor their products and services to consumers' needs	69.77	6	< 0.0005***
(2) to develop new products and services	66.55	6	< 0.0005***
(3) to cooperate with other companies in your country	62.18	6	< 0.0005***
(4) to cooperate with companies in other countries with essentially equivalent data protection and informational privacy regulations	106.93	6	< 0.0005***
(5) to cooperate with companies in other countries, no matter what their regulation of data protection and informational privacy is	65.49	6	< 0.0005***

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Fig. 65 below shows that, in all countries but Japan, a majority agreed that their country's data protection and informational privacy regulations still allowed companies to tailor products and services to consumers' needs. Agreement was highest (84–88 % of respondents) in China, Brazil, and the United States. In fact, in the United States, half of respondents (50 %) strongly agreed that this was the case, which was the greatest proportion of respondents in any country. This contrasts with Japan, where only a minority of 45 % agreed. This was also the country where the largest proportion of respondents (37 %) neither agreed nor disagreed. Indeed, Japanese respondents exhibited significantly lower agreement than respondents in all other countries ($p < 0.0005$ each; see Table 99) except for Switzerland ($p = 0.107$). Whereas the contrasts with Brazil and the United States amounted to medium-to-large effects ($r = 0.42$, $r = 0.44$), the remaining contrasts amounted to medium effects (with r ranging from 0.31 to 0.35; see Table 100 below). Moreover, Swiss respondents agreed significantly less with the statement than US respondents ($p < 0.0005$) and

Brazilian respondents (p = 0.002), which constituted medium and small-to medium effects (r = 0.30, r = 0.27). Finally, despite the high combined percentage answering with *strongly agree* or *somewhat agree*, Chinese respondents exhibited significantly lower agreement than US respondents (p = 0.009), another small-to-medium effect (r = 0.23).

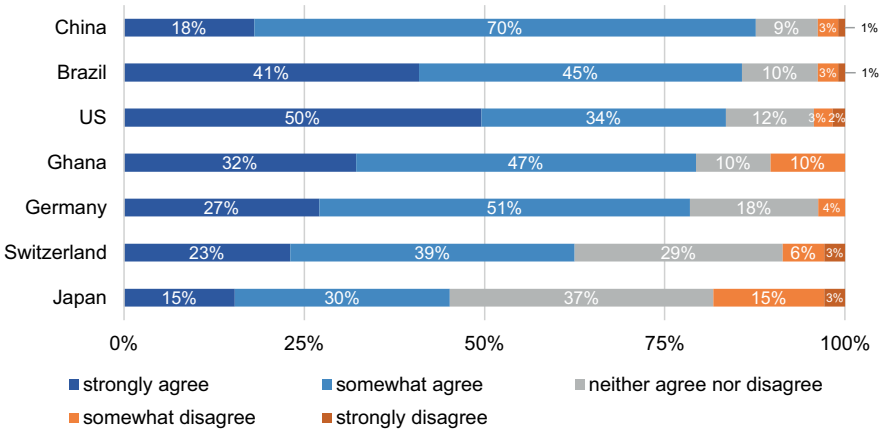

Fig. 65: Q19r1. Do you agree or disagree that the regulation of data protection and informational privacy in your country still allows companies to tailor their products and services to consumers' needs?

Table 99: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' agreement with the statement that their country's regulation of data protection and informational privacy still allows companies to tailor their products and services to consumers' needs.

	Japan	Switzerland	Germany	Ghana	China	Brazil
Switzerland	0.107					
Germany	< 0.0005***	0.260				
Ghana	< 0.0005***	0.260	1.000			
China	< 0.0005***	0.260	1.000	1.000		
Brazil	< 0.0005***	0.002**	0.260	0.626	0.107	
US	< 0.0005***	< 0.0005***	0.050	0.240	0.009*	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 100: Effect sizes for significant differences in respondents' agreement with the statement that their country's regulation of data protection and informational privacy still allows companies to tailor their products and services to consumers' needs.

Contrast		*r*
Japan	Brazil	0.42
	China	0.35
	Germany	0.32
	Ghana	0.31
	US	0.44
Switzerland	Brazil	0.27
	US	0.30
China	US	0.23

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

A similar pattern emerged when we considered statement (2). As shown in Fig. 66 below, a majority in all countries but Japan agreed that the regulation of data protection and informational privacy in their country still allowed companies to develop products and services. Again, agreement was highest in China and the United States (83–87 %), and, once more, the United States was the country where the greatest proportion of respondents strongly agreed with this statement (47 %, i.e., around half of respondents). Japan, where only a minority of 46 % agreed, was again the country where the largest proportion of respondents (34 %) neither agreed nor disagreed. Accordingly, Japanese respondents once more exhibited significantly lower agreement than respondents in all other countries ($p < 0.0005$ and $p = 0.008$; see Table 101) except for Switzerland ($p = 0.697$). These contrasts mostly amounted to medium effects (with r ranging from 0.31 to 0.40, see Table 102), while the contrast Japan-Germany constituted a small-to-medium effect ($r = 0.24$). Moreover, this time Swiss respondents' agreement with the statement was significantly lower than that of respondents in almost all other countries (with p ranging from < 0.0005 to 0.038; see Table 101) except for Japan and Germany ($p = 0.697$, $p = 0.751$). These contrasts amounted to or approached a medium effect size regarding the United States ($r = 0.32$) and China ($r = 0.29$), while the contrasts with Brazil and Ghana constituted small-to-medium effects ($r = 0.27$, $r = 0.21$). Furthermore, German respondents exhibited significantly lower agreement with the statement than US respondents ($p = 0.008$), another small-to-medium effect ($r = 0.23$).

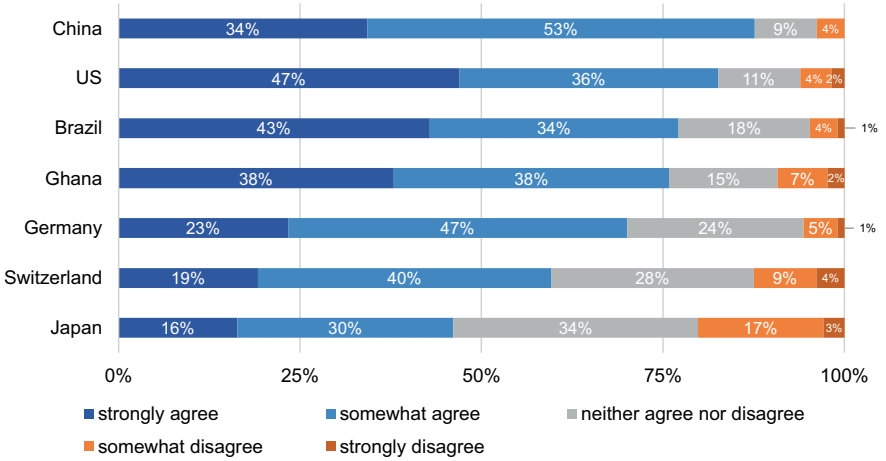

Fig. 66: Q19r2. Do you agree or disagree that the regulation of data protection and informational privacy in your country still allows companies to develop new products and services?

Table 101: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' agreement with the statement that their country's regulation of data protection and informational privacy still allows companies to develop new products and services.

	Japan	Switzerland	Germany	Ghana	Brazil	China
Switzerland	0.697					
Germany	0.008*	0.751				
Ghana	< 0.0005***	0.038*	0.751			
Brazil	< 0.0005***	0.002**	0.116	1.000		
China	< 0.0005***	< 0.0005***	0.052	1.000	1.000	
US	< 0.0005***	< 0.0005***	0.008*	0.878	1.000	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 102: Effect sizes for significant differences in respondents' agreement with the statement that their country's regulation of data protection and informational privacy still allows companies to develop new products and services.

Contrast		*r*
Japan	Brazil	0.36
	China	0.40
	Germany	0.24
	Ghana	0.31
	US	0.40
Switzerland	Brazil	0.27
	China	0.29
	Ghana	0.21
	US	0.32
Germany	US	0.23

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

Let us now turn to the statements about the possibility for cooperation among companies (statements [3]–[5]). Fig. 67 below summarizes the results pertaining to respondents' agreement with the statement that the regulation of data protection and informational privacy still allows companies to cooperate within their country. Here, we see the trend observed for the previous two statements reproduced: Once more, a majority in all countries but Japan agreed with the statement. Agreement was highest in Brazil and China (80–82 %). Although "only" 72 % of respondents in the United States demonstrated agreement, it was again the country where the greatest proportion of respondents strongly agreed with the statement (37 %, i.e., more than a third of respondents). Japan was once more the odd one out: Here, only a minority of 42 % agreed with the statement, and, again, Japan was the country where the largest proportion of respondents (37 %) neither agreed nor disagreed. Pairwise Wilcoxon rank-sum tests confirmed Japan's special status: Japanese respondents' agreement was significantly lower than that of respondents in all other countries ($p < 0.0005$ each) except Switzerland ($p = 0.108$). These contrasts amounted to medium-to-large effects for China ($r = 0.44$) and Brazil ($r = 0.42$), and either constituted or approached a medium effect size for the remaining three countries (with r ranging from 0.29 to 0.37; see Table 104). Moreover, Swiss respondents' agreement with the statement was significantly lower than that of Brazilian, Chinese, and US respondents (with p ranging from 0.004 to 0.043; see Table 103). This difference was small-to-medium regarding China and Brazil ($r = 0.25$ each) and small regarding the United States ($r = 0.20$).

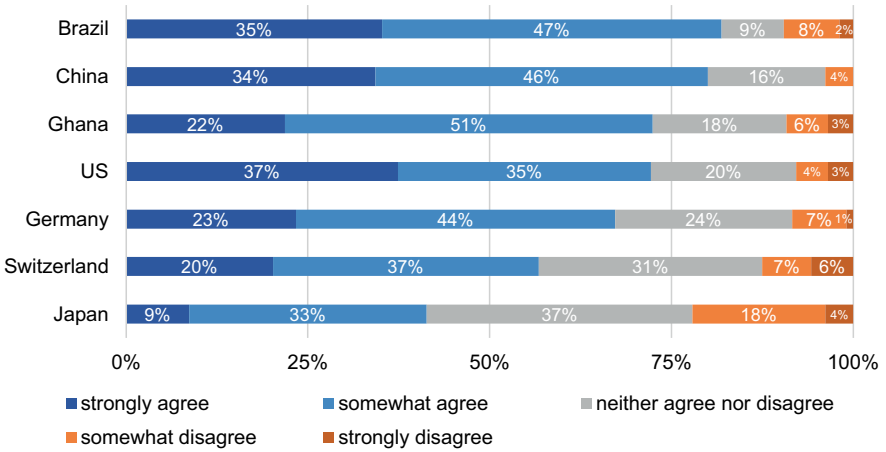

Fig. 67: Q19r3. Do you agree or disagree that the regulation of data protection and informational privacy in your country still allows companies to cooperate with other companies in your country?

Table 103: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' agreement with the statement that their country's regulation of data protection and informational privacy still allows companies to cooperate with other companies in their country.

	Japan	Switzerland	Germany	Ghana	US	China
Switzerland	0.108					
Germany	< 0.0005***	0.850				
Ghana	< 0.0005***	0.715	1.000			
US	< 0.0005***	0.043*	0.673	0.850		
China	< 0.0005***	0.004**	0.221	0.376	1.000	
Brazil	< 0.0005***	0.005*	0.221	0.361	1.000	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 104: Effect sizes for significant differences in respondents' agreement with the statement that their country's regulation of data protection and informational privacy still allows companies to cooperate with other companies in their country.

Contrast		*r*
Japan	Brazil	0.42
	China	0.44
	Germany	0.29
	Ghana	0.31
	US	0.37
Switzerland	Brazil	0.25
	China	0.25
	US	0.20

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

But what about international cooperation between companies? Fig. 68 below shows that in all countries but Japan and Switzerland, a majority agreed that the regulation of data protection and informational privacy in their country still allowed for cooperation with companies in other countries with equivalent regulations (statement [4]). Agreement was highest in China and the United States (82–85 %). The United States was again the country where the greatest proportion of respondents strongly agreed with the statement (46 %, i.e., around half of respondents). By contrast, in Japan, only a minority of about one-third (32 %) agreed. Again, this was the country where the largest proportion of respondents (40 %) neither agreed nor disagreed, and it was the only country where most respondents chose not to indicate agreement or disagreement. In Switzerland, just under half (48 %) agreed, whereas about one-third (32 %) chose the neutral option. Accordingly, Japanese and Swiss respondents' agreement was significantly lower than that of respondents in the remaining five countries ($p < 0.0005$ for all contrasts involving Japan; for the contrasts involving Switzerland, p ranged from < 0.0005 to 0.043; see Table 105). Whereas the contrasts Japan-China and Japan-United States amounted to large effects ($r = 0.54$, $r = 0.51$), the contrasts Switzerland-China and Switzerland-United States constituted medium-to-large effects ($r = 0.41$, $r = 0.42$). The remaining contrasts involving Japan were medium effects (with r ranging from 0.34 to 0.39; see Table 106 below). The contrasts Switzerland-Brazil and Switzerland-Germany were small-to-medium effects ($r = 0.28$, $r = 0.22$), and the contrast Switzerland-Ghana was a small effect ($r = 0.20$). Moreover, both German and Ghanaian respondents' agreement was significantly lower than that of US and Chinese respondents (with p ranging from

0.002 to 0.025; see Table 105 below), a small-to-medium effect in each case (with r ranging from 0.21 to 0.26; see Table 106 below).

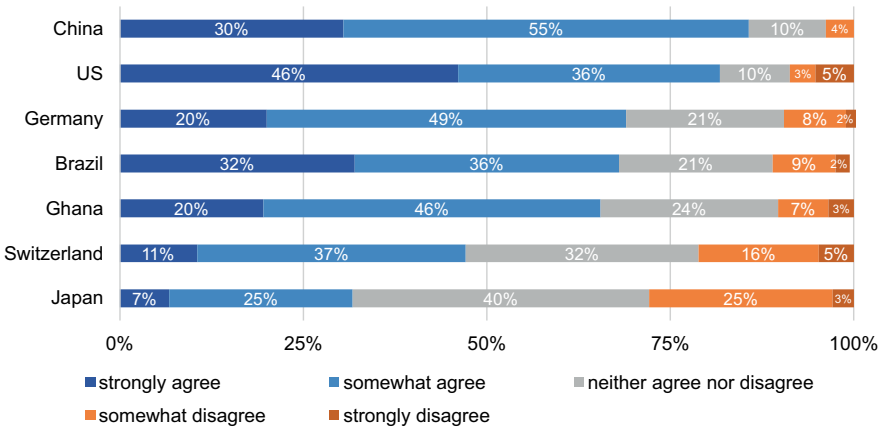

Fig. 68: Q19r4. Do you agree or disagree that the regulation of data protection and informational privacy in your country still allows companies to cooperate with companies in other countries with essentially equivalent regulation of data protection and informational privacy?

Table 105: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' agreement with the statement that their country's regulation of data protection and informational privacy still allows companies to cooperate with companies in other countries with essentially equivalent data protection and informational privacy regulations.

	Japan	Switzerland	Ghana	Germany	Brazil	China
Switzerland	0.292					
Ghana	< 0.0005***	0.043*				
Germany	< 0.0005***	0.013*	0.785			
Brazil	< 0.0005***	0.001**	0.764	0.764		
China	< 0.0005***	< 0.0005***	0.021*	0.025*	0.764	
US	< 0.0005***	< 0.0005***	0.002**	0.002**	0.142	0.764

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 106: Effect sizes for significant differences in respondents' agreement with the statement that their country's regulation of data protection and informational privacy still allows companies to cooperate with companies in other countries with essentially equivalent data protection and informational privacy regulations.

Contrast		*r*
Japan	Brazil	0.39
	China	0.54
	Germany	0.36
	Ghana	0.34
	US	0.51
Switzerland	Brazil	0.28
	China	0.41
	Germany	0.22
	Ghana	0.20
	US	0.42
Ghana	China	0.22
	US	0.26
Germany	China	0.21
	US	0.25

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

The last statement (5) concerned cooperation with companies in any country, regardless of how it regulates data protection and informational privacy. Here, we see a repetition of the pattern observed for the previous statement. Fig. 69 below shows that in all countries but Japan and Switzerland, a majority agreed that the regulation of data protection and informational privacy in their country still allowed for cooperation with companies in other countries regardless of how data protection and informational privacy are regulated there. Agreement was again highest in the United States and China (72–77 %). The United States was again the country where the greatest proportion of respondents strongly agreed with the statement (37 %). By contrast, in Japan, only a minority of about one-third (35 %) agreed. Once more, Japan was the country where the largest proportion of respondents (37 %) neither agreed nor disagreed—and again, it was the only country where most respondents chose not to indicate agreement or disagreement. In Switzerland, just under half (46 %) agreed, whereas about one-third (34 %) opted for the neutral answer. Japanese respondents' agreement was significantly lower than that of respondents in all other countries ($p < 0.0005$ and $p = 0.044$; for details, see Table 107 below) except Switzerland ($p = 0.693$). Whereas the contrast Japan-United States amounted to a

medium-to-large effect (r = 0.44), most of the remaining contrasts either constituted or approached a medium effect size (with r ranging from 0.29 to 0.37; see Table 108, p. 134). The contrast Japan-Ghana was a small effect (r = 0.21). However, Swiss respondents' agreement was only significantly lower than that of Brazilian, Chinese, and US respondents (with p ranging from < 0.0005 to 0.014; see Table 107). This difference amounted to a medium effect regarding US respondents (r = 0.35) and a small-to-medium effect regarding Brazilian and Chinese respondents (r = 0.23, r = 0.26). Finally, Ghanian respondents agreed significantly less with the statement than US respondents (p = 0.002, r = 0.27), another small-to-medium effect.

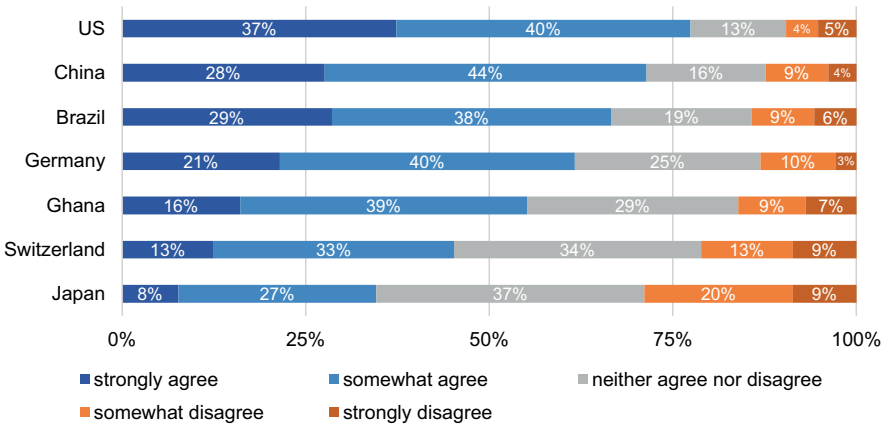

Fig. 69: Q19r5. Do you agree or disagree that the regulation of data protection and informational privacy in your country still allows companies to cooperate with companies in other countries, no matter what their regulation of data protection and informational privacy is?

Table 107: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' agreement with the statement that their country's regulation of data protection and informational privacy still allows companies to cooperate with companies in other countries, regardless of how they regulate data protection and informational privacy.

	Japan	Switzerland	Ghana	Germany	Brazil	China
Switzerland	0.693					
Ghana	0.044*	0.870				
Germany	< 0.0005***	0.099	0.870			
Brazil	< 0.0005***	0.014*	0.478	0.870		
China	< 0.0005***	0.002**	0.158	0.870	0.870	
US	< 0.0005***	< 0.0005***	0.002**	0.053	0.568	0.795

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 108: Effect sizes for significant differences in respondents' agreement with the statement that their country's regulation of data protection and informational privacy still allows companies to cooperate with companies in other countries, regardless of how they regulate data protection and informational privacy.

Contrast		*r*
Japan	Brazil	0.33
	China	0.37
	Germany	0.29
	Ghana	0.21
	US	0.44
Switzerland	Brazil	0.23
	China	0.26
	US	0.35
Ghana	US	0.27

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

4.2 ... on bureaucracy, privacy management, and information overload

Respondents were then asked to indicate their agreement with several statements concerning the impact of their country's regulation of data protection and informational privacy on bureaucracy, information overload, the professional handling of data by companies, and consumers' privacy management. They were asked whether they believed their country's regulations

(1) created too much bureaucracy for the state;
(2) created too much bureaucracy for companies;
(3) created too much bureaucracy for consumers
(4) created information overload for consumers;
(5) had led to companies handling data more professionally; and
(6) enabled consumers to easily manage their privacy needs.

For all statements, we found significant cross-cultural differences in respondents' agreement ($p < 0.0005$; see Table 109). In the following, we will examine these differences in more detail for each statement.

Table 109: Output of Kruskal-Wallis tests regarding cross-cultural differences in respondents' agreement with statements concerning the impact of their country's regulation of data protection and informational privacy on different actors. Regulation …

	H	*df*	*p*
(1) creates too much bureaucracy for the state	36.41	6	< 0.0005***
(2) creates too much bureaucracy for companies	37.71	6	< 0.0005***
(3) creates too much bureaucracy for consumers	30.12	6	< 0.0005***
(4) creates information overload for consumers	49.21	6	< 0.0005***
(5) has led to a more professional handling of data by companies	80.52	6	< 0.0005***
(6) enables consumers to easily manage their privacy needs	75.34	6	< 0.0005***

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Let us first consider statements (1)–(3), which relate to the impact on bureaucracy for various actors. Fig. 70 shows that, in most countries, a majority agreed that data protection and informational privacy regulations created too much bureaucracy for the state. The exceptions were Switzerland and Japan, where only a minority agreed with the statement (44 % each). While the largest proportion of respondents agreed in China (77 %), followed by the United States and Germany (69 % and 67 % respectively), the United States was the country where the greatest proportion of participants strongly agreed (43 %). However, Japanese and Swiss respondents' agreement was significantly lower than that of US and Chinese respondents (with p ranging from < 0.0005 to 0.004; see Table 110 below). Moreover, Brazilian respondents agreed to a significantly lesser extent with the statement than US respondents (p = 0.011). All these differences amounted to small-to-medium effects (with r ranging from 0.23 to 0.29; see Table 111 below), with the contrast between Japan and the United States approaching a medium effect size.

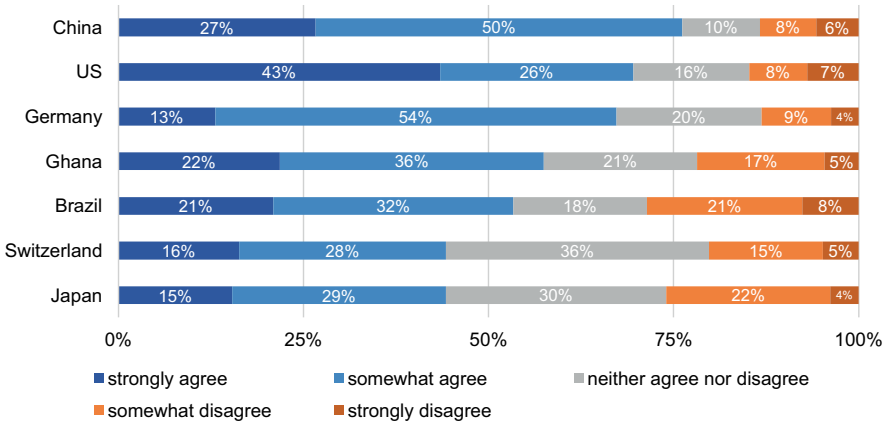

Fig. 70: Q20r1. The regulation of data protection and informational privacy in my country creates too much bureaucracy for the state.

Table 110: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' agreement with the statement that their country's regulation of data protection and informational privacy creates too much bureaucracy for the state.

	Japan	Switzerland	Brazil	Germany	Ghana	China
Switzerland	1.000					
Brazil	1.000	1.000				
Germany	0.147	0.296	1.000			
Ghana	1.000	1.000	1.000	1.000		
China	0.002**	0.004**	0.086	0.394	0.407	
US	< 0.0005***	0.001**	0.011*	0.067	0.096	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 111: Effect sizes for significant differences in respondents' agreement with the statement that their country's regulation of data protection and informational privacy creates too much bureaucracy for the state.

Contrast		*r*
Japan	China	0.27
	US	0.29
Switzerland	China	0.25
	US	0.27
Brazil	US	0.23

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

As shown in Fig. 71, in most countries, the majority agreed that data protection and informational privacy regulation created too much bureaucracy for companies. Again, the exceptions were Switzerland and Japan, where only a minority agreed with the statement; in Switzerland, this was just under half (49 %). Agreement was lowest in Japan at 46 %. Again, it was in China (77 %) that most respondents agreed, followed by the United States (62 %) and Germany and Ghana (59 % and 57 % respectively). This time, however, China was the country where the greatest proportion of participants strongly agreed (42 %). Accordingly, China was the country that stood out here, with Chinese respondents exhibiting significantly greater agreement than respondents in all other countries (with p ranging from < 0.0005 to 0.005; see Table 112) except the United States ($p = 0.514$). These differences amounted to medium effects for the contrasts involving Japan ($r = 0.35$), Switzerland ($r = 0.32$), and Ghana ($r = 0.31$); and to small-to-medium effects for the contrasts involving Brazil ($r = 0.26$) and Germany ($r = 0.25$; see also Table 113).

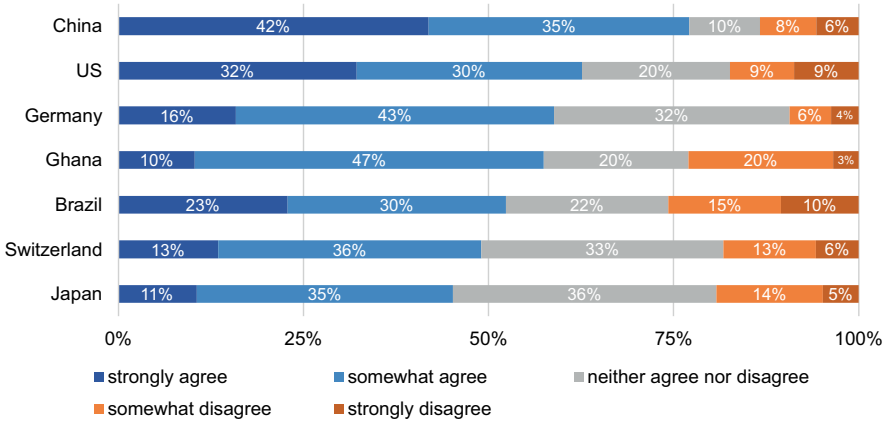

Fig. 71: Q20r2. The regulation of data protection and informational privacy in my country creates too much bureaucracy for companies.

Table 112: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' agreement with the statement that their country's regulation of data protection and informational privacy creates too much bureaucracy for companies.

	Japan	Switzerland	Brazil	Ghana	Germany	US
Switzerland	1.000					
Brazil	1.000	1.000				
Ghana	1.000	1.000	1.000			
Germany	0.326	1.000	1.000	1.000		
US	0.055	0.233	0.779	0.418	1.000	
China	< 0.0005***	< 0.0005***	0.004**	< 0.0005***	0.005*	0.514

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 113: Effect sizes for significant differences in respondents' agreement with the statement that their country's regulation of data protection and informational privacy creates too much bureaucracy for companies.

Contrast		*r*
China	Brazil	0.26
	Germany	0.25
	Ghana	0.31
	Japan	0.35
	Switzerland	0.32

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

The pattern observed for the first two statements was also reproduced for statement (3), which concerned the impact on bureaucracy for consumers. Again, a majority in all countries but Switzerland and Japan agreed with the statement (see Fig. 72). In Switzerland and Japan, only a minority agreed that the regulation of data protection and informational privacy created too much bureaucracy for consumers, with just under half agreeing in Switzerland (49 %). Agreement was lowest in Japan at 36 %, and highest in China (66 %), followed by Brazil and the United States (64 % and 63 % respectively). It is noteworthy that Japan was also the only country where most respondents opted for the neutral answer. The United States was the country where the greatest proportion of participants strongly agreed (34 %). The country that stood out most noticeably was Japan, where respondents agreed significantly less with the statement than respondents in all other countries except Switzerland and Ghana, with p ranging from < 0.0005 to 0.025 (see Table 114). These differences mostly amounted to small-to-medium effects (with r ranging from 0.22 to 0.28; see Table 115), except for the contrast Japan-China, which constituted a medium effect ($r = 0.33$). Moreover, Swiss respondents' agreement was significantly lower than that of Chinese respondents, another small-to-medium effect ($p = 0.048$, $r = 0.21$).

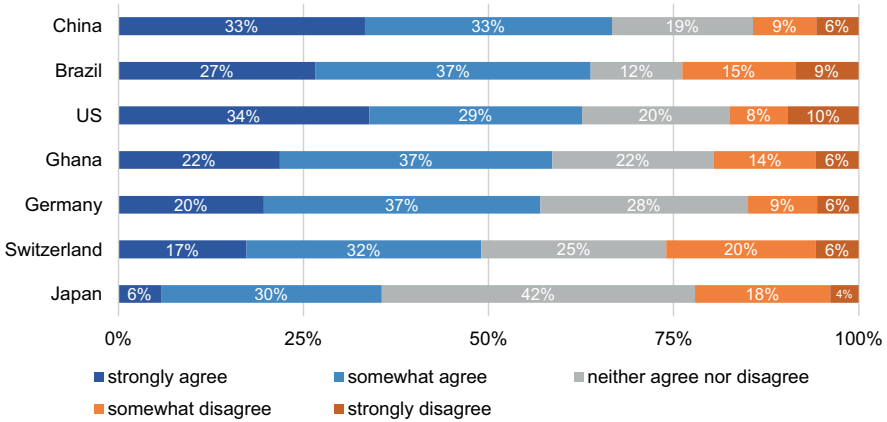

Fig. 72: Q20r3. The regulation of data protection and informational privacy in my country creates too much bureaucracy for consumers.

Table 114: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' agreement with the statement that that their country's regulation of data protection and informational privacy creates too much bureaucracy for consumers.

	Japan	Switzerland	Germany	Ghana	Brazil	US
Switzerland	1.000					
Germany	0.025*	1.000				
Ghana	0.059	1.000	1.000			
Brazil	0.017*	1.000	1.000	1.000		
US	0.001**	0.206	1.000	1.000	1.000	
China	< 0.0005***	0.048*	0.842	1.000	1.000	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 115: Effect sizes for significant differences in respondents' agreement with the statement that their country's regulation of data protection and informational privacy creates too much bureaucracy for consumers.

Contrast		*r*
Japan	Brazil	0.23
	China	0.33
	Germany	0.22
	US	0.28
Switzerland	China	0.21

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

The next statement (4) concerned information overload for consumers. As shown in Fig. 73 below, a majority in most countries agreed that data protection and informational privacy regulations overloaded consumers with information. The exceptions were Ghana and Japan, where only a minority agreed with the statement, with just under half agreeing in Ghana (47 %). Agreement was lowest in Japan at 28 % and highest in China (69 %), followed by the United States (68 %) and Germany (63 %). It is noteworthy that Japan was again the only country where most respondents opted for the neutral answer. Moreover, China was the country where the greatest proportion of participants strongly agreed (33 %) with the statement. Accordingly, the two countries that stood out the most were Japan and China. While Japanese respondents exhibited significantly lower agreement than respondents in three countries (China, Germany, and the United States; $p < 0.0005$ each), Chinese respondents agreed significantly more with the statement than respondents in four countries did (in addition to Japan, Ghana, Switzerland, and Brazil, with p ranging from 0.011 to 0.049; see Table 116). The differences involving Japan amounted to a medium effect size (with r ranging from 0.40 to 0.33; see Table 117), while the three remaining contrasts involving China were of a small-to-medium effect size regarding Ghana and Switzerland ($r = 0.25$, $r = 0.23$), and of a small effect size regarding Brazil ($r = 0.20$).

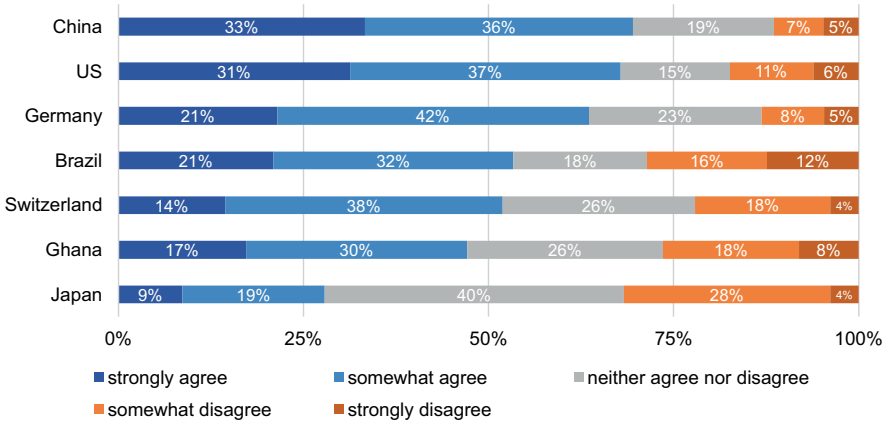

Fig. 73: Q20r4. The regulation of data protection and informational privacy in my country creates too much information overload for consumers.

Table 116: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' agreement with the statement that their country's regulation of data protection and informational privacy overloads consumers with information.

	Japan	Ghana	Switzerland	Brazil	Germany	US
Ghana	0.421					
Switzerland	0.054	1.000				
Brazil	0.224	1.000	1.000			
Germany	< 0.0005***	0.242	0.421	0.635		
US	< 0.0005***	0.057	0.086	0.173	1.000	
China	< 0.0005***	0.011*	0.016*	0.049*	0.692	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 117: Effect sizes for significant differences in respondents' agreement with the statement that their country's regulation of data protection and informational privacy overloads consumers with information.

Contrast		*r*
Japan	China	0.40
	Germany	0.33
	US	0.35
China	Brazil	0.20
	Ghana	0.25
	Switzerland	0.23

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

Statement (5) asked about the impact of regulation on corporate data handling. The pattern observed for statements (1)–(3) was again reproduced in Fig. 74, which shows that, in most countries, a majority agreed that data protection and informational privacy regulations had led to companies handling data more professionally. The exceptions were—once again—Switzerland and Japan, where only a minority agreed with the statement, with just under half agreeing in Switzerland (46 %). At 39 %, agreement was once more lowest in Japan, which was, again, the only country where most respondents opted for the neutral option (42 %). China led once more with the highest level of agreement (78 %), followed by Brazil (77 %) and the United States (76 %). This time, however, Brazil was the country where the greatest proportion of participants strongly agreed (38 %). China, Brazil, and the United States quite clearly stood in contrast to the remaining countries: Agreement in these three countries was significantly higher than that of Japanese, Swiss, Ghanaian, and German respondents (with p ranging from < 0.0005 to 0.033; see Table 118). Moreover, Japanese and Swiss respondents exhibited significantly lower agreement than German respondents ($p = 0.003$, $p = 0.033$). The contrasts involving Japan and Switzerland stood out in that they mostly amounted to medium effects (with r ranging from 0.35 to 0.40; see Table 119, p. 145), with the contrast between Japan and China even constituting a medium-to-large effect ($r = 0.43$). Only the contrasts Japan-Germany and Switzerland-Germany amounted to just a small-to-medium and a small effect ($r = 0.26$, $r = 0.20$). The remaining contrasts were mostly small-to-medium effects (with r ranging from 0.21 to 0.25; see Table 119), and the contrast between the United States and Germany only amounted to a small effect ($r = 0.20$).

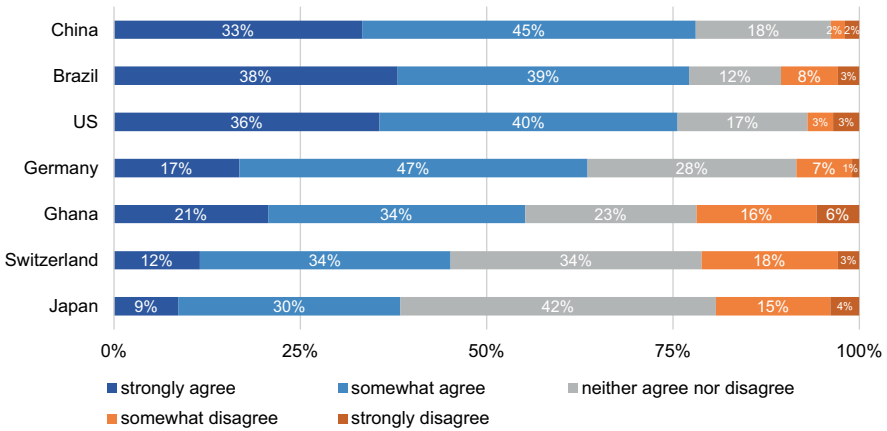

Fig. 74: Q20r5. The regulation of data protection and informational privacy in my country has led to a more professional handling of data by companies.

Table 118: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' agreement with the statement that their country's regulation of data protection and informational privacy has led to companies handling data more professionally.

	Japan	Switzerland	Ghana	Germany	US	Brazil
Switzerland	1.000					
Ghana	0.469	1.000				
Germany	0.003**	0.033*	1.000			
US	< 0.0005***	< 0.0005***	0.010*	0.033*		
Brazil	< 0.0005***	< 0.0005***	0.009*	0.024*	1.000	
China	< 0.0005***	< 0.0005***	0.006*	0.023*	1.000	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 119: Effect sizes for significant differences in respondents' agreement with the statement that their country's regulation of data protection and informational privacy has led to companies handling data more professionally.

Contrast		*r*
Japan	Brazil	0.40
	China	0.43
	Germany	0.26
	US	0.40
Switzerland	Brazil	0.35
	China	0.37
	Germany	0.20
	US	0.35
Germany	Brazil	0.21
	China	0.21
	US	0.20
Ghana	Brazil	0.25
	China	0.25
	US	0.24

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

The last statement (6) concerned the impact of regulation on consumers' ability to manage their privacy needs (see Fig. 75 below). We again see a familiar pattern repeated: Whereas a majority in most countries agreed that the regulation of data protection and informational privacy enabled customers to easily manage their privacy needs, only a minority were of this opinion in Japan and Switzerland (though in Switzerland, this was just under half of respondents, at 45 %). As with the other statements, agreement was lowest in Japan (30 %) and highest in China (77 %). The United States followed at 73 % and Brazil at 70 %. The United States was again the country where the greatest proportion of participants strongly agreed (37 %). Strikingly, Japan was once again the only country where most respondents opted for a neutral answer. Japan thus stood out in that Japanese respondents' agreement was significantly lower than that of respondents in all other countries (with p ranging from < 0.0005 to 0.009; see Table 120) except for Switzerland ($p = 0.631$). Whereas the contrasts with China and the United States amounted to medium-to-large effects ($r = 0.46$, $r = 0.43$) and the one with Brazil to a medium effect ($r = 0.34$), the remaining contrasts (with Germany and Ghana) constituted small-to-medium effects ($r = 0.28$, $r = 0.25$, see also Table 121). Moreover, Swiss respondents exhibited significantly lower agreement

than Brazilian, Chinese, and US respondents ($p = 0.004$, $p < 0.0005$, and $p < 0.0005$ respectively). These differences were of a medium effect size regarding China and the United States ($r = 0.37$, $r = 0.34$) and a small-to-medium effect size regarding Brazil ($r = 0.25$). Chinese respondents also significantly surpassed German and Ghanian respondents in terms of their agreement with the statement ($p = 0.014$, $p = 0.045$), a small-to-medium effect in each case ($r = 0.22$, $r = 0.21$). Finally, German respondents agreed significantly less with the statement than US respondents, which amounted to a small effect ($p = 0.028$, $r = 0.20$).

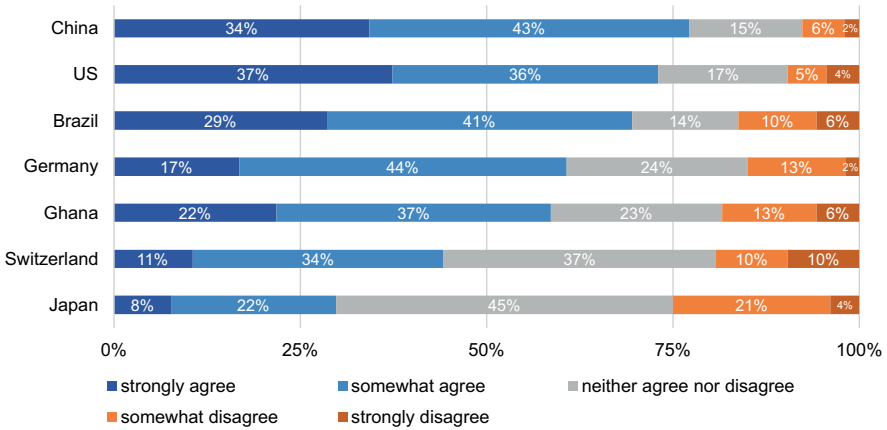

Fig. 75: Q20r6. The regulation of data protection and informational privacy in my country enables consumers to easily manage their privacy needs.

Table 120: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' agreement with the statement that their country's regulation of data protection and informational privacy enables consumers to easily manage their privacy needs.

	Japan	Switzerland	Ghana	Germany	Brazil	US
Switzerland	0.631					
Ghana	0.009*	0.360				
Germany	0.001**	0.172	1.000			
Brazil	< 0.0005***	0.004**	0.740	0.659		
US	< 0.0005***	< 0.0005***	0.072	0.028*	0.740	
China	< 0.0005***	< 0.0005***	0.045*	0.014*	0.740	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 121: Effect sizes for significant differences in respondents' agreement with the statement that their country's regulation of data protection and informational privacy enables consumers to easily manage their privacy needs.

Contrast		*r*
Japan	Brazil	0.34
	China	0.46
	Germany	0.28
	Ghana	0.25
	US	0.43
Switzerland	Brazil	0.25
	China	0.37
	US	0.34
Germany	China	0.22
	US	0.20
Ghana	China	0.21

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

4.3 ... on fundamental rights, digitalization, and overall impact

Respondents were then asked to evaluate
(1) the sufficiency of their country's regulations on data protection and information privacy to protect the fundamental rights of individuals;
(2) the impact of their country's regulation on digital development and the implementation of digital innovations; and
(3) the overall impact of their country's data protection and information privacy regulations.

For all these ratings, we found significant differences across the examined countries ($p < 0.0005$; see Table 122). In the following, we will examine these differences in more detail for each rating.

Table 122: Output of Kruskal-Wallis tests regarding cross-cultural differences in respondents' evaluations of the impact of their country's regulation of data protection and information privacy.

	H	*df*	*p*
(1) Evaluation of the regulation's sufficiency to protect the fundamental rights of individuals	64.00	6	< 0.0005***
(2) Evaluation of the regulation's impact on digital development and the implementation of digital innovations	106.87	6	< 0.0005***
(3) Evaluation of the regulation's overall impact	59.97	6	< 0.0005***

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Fig. 76 shows that, in almost all countries, a majority regarded the regulation of data protection and informational privacy as *sufficient* or *rather sufficient* to protect the fundamental rights of individuals. The exception was Japan, where only a minority of 26 % believed this to be the case. In fact, Japan was the only country where a higher proportion of respondents (34 %) regarded regulation as *insufficient* or *rather insufficient* in this respect. In contrast, the proportion of respondents who believed that the regulation of data protection and informational privacy was *sufficient* or *rather sufficient* to protect individuals' fundamental rights was greatest in Brazil and China (74 % and 73 % respectively), followed by the United States (69 %). The United States was the country where the greatest proportion of participants (38 %) regarded the regulation of data protection and informational privacy as *sufficient* (not just *rather sufficient*) in this respect. Japan's special status was also confirmed by statistical tests: Japanese sufficiency ratings were significantly lower than those given by respondents in all other countries (with p ranging from < 0.0005 to 0.004; see Table 123). This difference was medium-to-large regarding China (r = 0.47), Brazil (r = 0.44), and the United States (r = 0.41); medium regarding Germany (r = 0.35); and small-to-medium regarding Ghana (r = 0.29) and Switzerland (r = 0.26; see Table 124). Moreover, respondents from Switzerland perceived the regulation of data protection and informational privacy to be significantly less sufficient to protect individuals' fundamental rights than respondents from the United States (p = 0.029, r = 0.21), another small-to-medium effect.

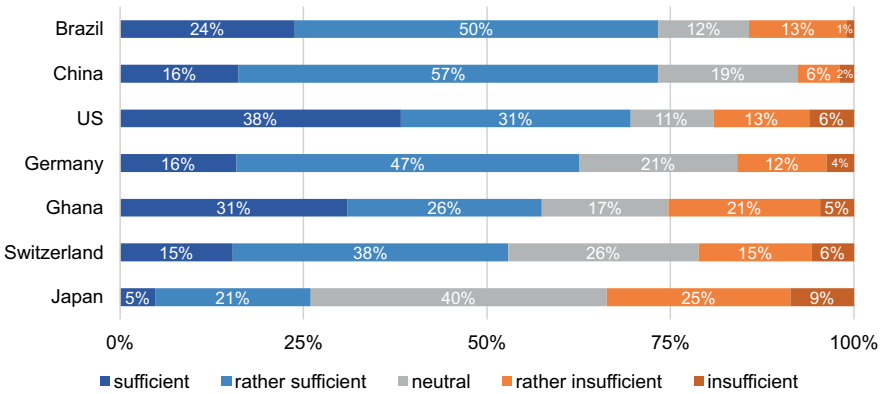

Fig. 76: Q21. In your expert opinion, the current regulation of data protection and informational privacy in your country is ... to protect the fundamental rights of individuals.

Table 123: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' assessments of the sufficiency of their country's regulations to protect individuals' fundamental rights.

	Japan	Switzerland	Ghana	Germany	China	Brazil
Switzerland	0.004**					
Ghana	0.001**	1.000				
Germany	< 0.0005***	1.000	1.000			
China	< 0.0005***	0.107	1.000	1.000		
Brazil	< 0.0005***	0.071	1.000	0.822	1.000	
US	< 0.0005***	0.029*	1.000	0.241	1.000	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 124: Effect sizes for significant differences in respondents' assessments of the sufficiency of their country's regulations to protect individuals' fundamental rights.

Contrast		*r*
Japan	Brazil	0.44
	China	0.47
	Germany	0.35
	Ghana	0.29
	Switzerland	0.26
	US	0.41
Switzerland	US	0.21

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

Moving on to rating (2), we see that a majority in most countries believed that the regulation of data protection and informational privacy had a *positive* or *very positive* impact on digital development and the implementation of digital innovations (see Fig. 77 below). The exceptions were Japan and Switzerland, where only a minority believed this to be the case. In Switzerland, this figure was just under half (45 %), and in Japan it was less than one-third (30 %). In Japan, most respondents (47 %) believed that the regulation of data protection and informational privacy had a neutral effect on digital development and the implementation of digital innovations. In contrast, the proportion of respondents who believed that the regulation of data protection and informational privacy had a *positive* or *very positive* effect in this respect was greatest in China (79 %), followed by the United States and Brazil (74 % each). Japan clearly stood out as it was the country where ratings were significantly lower than those of all other countries ($p < 0.0005$ each) except for Switzerland ($p = 0.068$). These differences amounted to a large effect for China ($r = 0.52$), approached a large effect size for the United States ($r = 0.49$) and Brazil ($r = 0.47$), and amounted to medium effects for Germany ($r = 0.35$) and Ghana ($r = 0.30$). Furthermore, Swiss respondents' assessments were significantly less positive than those made by respondents in Brazil, China, and the United States ($p < 0.0005$ each), a medium effect in each case (see Table 126, p. 152).

The assessments given by respondents in China and the United States not only differed significantly from those made by Japanese and Swiss respondents. In both countries, respondents assessed the impact of data protection and informational privacy regulations on digital development and the implementation of digital innovations significantly more positively than respondents in Ghana and Germany did (with p ranging from 0.001 to 0.009; see Table 125). While the contrast between

China and Ghana approached a medium effect size (r = 0.29), the remaining contrasts were small-to-medium effects (see Table 126).

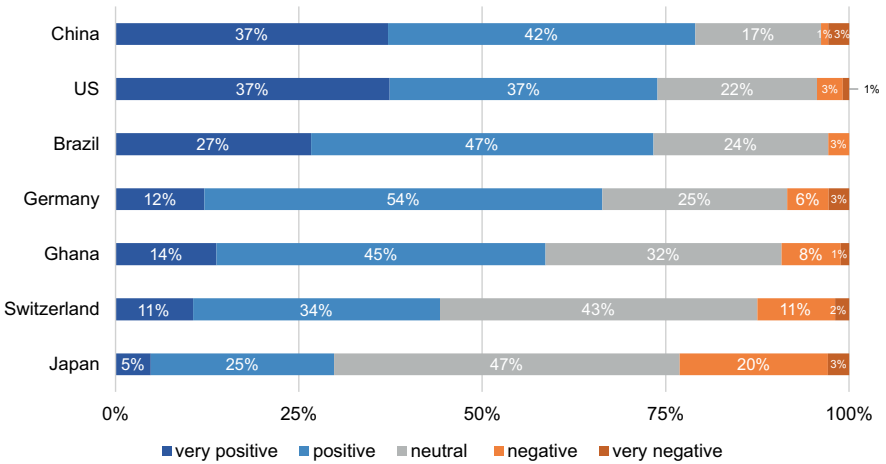

Fig. 77: Q22. In your expert opinion, the regulation of data protection and informational privacy in your country has a ... effect on digital development and the implementation of digital innovations.

Table 125: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' assessments of the impact of the data protection and informational privacy regulation on digital development and the implementation of digital innovations.

	Japan	Switzerland	Ghana	Germany	Brazil	US
Switzerland	0.068					
Ghana	< 0.0005***	0.347				
Germany	< 0.0005***	0.063	1.000			
Brazil	< 0.0005***	< 0.0005***	0.055	0.117		
US	< 0.0005***	< 0.0005***	0.004**	0.009*	0.857	
China	< 0.0005***	< 0.0005***	0.001**	0.002**	0.510	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 126: Effect sizes for significant differences in respondents' assessments of the impact of data protection and informational privacy regulation on digital development and the implementation of digital innovations.

Contrast		*r*
Japan	Brazil	0.47
	China	0.52
	Germany	0.35
	Ghana	0.30
	US	0.49
Switzerland	Brazil	0.32
	China	0.39
	US	0.36
Ghana	China	0.29
	US	0.25
Germany	China	0.26
	US	0.22

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

As regards the final rating, Fig. 78 shows that, in four out of seven countries (China, the United States, Brazil, and Germany), a majority believed that, overall, the regulation of data protection and informational privacy had a positive impact. In Japan, Ghana, and Switzerland, however, only a minority believed this to be the case. In Switzerland and Ghana, this was just under half (44 % each), while in Japan, it was about one-third (34 %). In these three countries, most respondents believed that the regulation of data protection and informational privacy had a neutral impact. The proportion of respondents who believed it had a positive impact was greatest in China (76 %), followed by the United States (71 %) and Brazil (64 %). Japan was the country that stood out the most: Japanese ratings were significantly less positive than Chinese, US, Brazilian, and German ratings ($p < 0.0005$ and $p = 0.048$, depending on the contrast; see Table 127). This difference amounted to a medium-to-large effect for China ($r = 0.41$), a medium effect for the United States ($r = 0.37$), approached a medium effect size for Brazil ($r = 0.29$), and amounted to a small-to-medium effect for Germany ($r = 0.20$; see also Table 128). Like the Japanese ratings, both the Ghanaian and Swiss ratings were significantly less positive than those provided by Chinese ($p < 0.0005$ each) and US respondents ($p = 0.002$ each). Both contrasts with China amounted to medium effects ($r = 0.32$ for Ghana, $r = 0.31$ for Switzerland), while the contrasts Ghana-United States and Switzerland-United States amounted to

small-to-medium effects (r = 0.27 and r = 0.26). Another country that exhibited significantly less positive ratings than China was Germany (p = 0.011), which constituted a small-to-medium effect (r = 0.23).

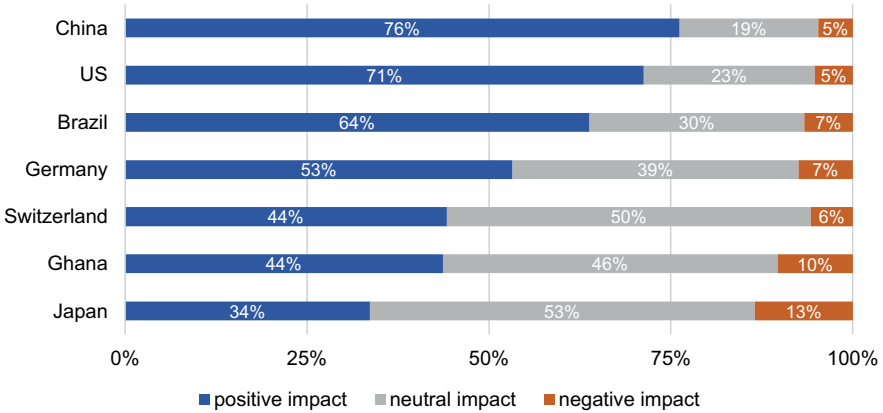

Fig. 78: Q23. Overall, the regulation of data protection and informational privacy in your country has a ...

Table 127: *P* values of pairwise Wilcoxon rank-sum tests regarding respondents' assessments of the overall impact of data protection and informational privacy regulation in their country.

	Japan	Ghana	Switzerland	Germany	Brazil	US
Ghana	1.000					
Switzerland	0.429	1.000				
Germany	0.048*	1.000	1.000			
Brazil	< 0.0005***	0.082	0.111	1.000		
US	< 0.0005***	0.002**	0.002**	0.082	1.000	
China	< 0.0005***	< 0.0005***	< 0.0005***	0.011*	0.448	1.000

Note. Significance codes: '***' < 0.0005 '**' < 0.005 '*' < 0.05. Significant effects are shaded grey.

Table 128: Effect sizes for significant differences in respondents' assessments of the overall impact of data protection and informational privacy regulation in their country.

Contrast		*r*
Japan	Brazil	0.29
	China	0.41
	Germany	0.20
	US	0.37
Ghana	China	0.32
	US	0.27
Switzerland	China	0.31
	US	0.26
Germany	China	0.23

Note. Following Cohen (1988), $r = 0.10$ is to be considered a small effect, $r = 0.30$ a medium effect, and $r = 0.50$ a large effect.

IV Summary of findings and comparison with consumer views

1 Introduction

In this section, we will summarize the main results of our survey of data protection professionals from Brazil, China, Germany, Ghana, Japan, Switzerland, and the United States and compare them with consumer views wherever we have been able to draw on relevant, large-scale comparative surveys of our selected countries. Such surveys were compiled and analyzed in detail in Wawra (2023a; 2023b). We therefore will not elaborate on them again here and will only include overall results in the following. Ghana was not included in any of these surveys, so we conducted our own survey there in 2022 (for details, see Thir & Wawra 2023). This survey will be used to compare professionals' attitudes with those of consumers in that country. Although we also compiled a cultural country report for Switzerland that details consumer attitudes toward privacy and data protection issues there (see Thir et al. 2023), we must always exclude the country from the cross-cultural analyzes here. This is because Switzerland was not part of any of the international studies we consulted, other surveys in the country seemed too disparate to be used for comparison, and we could not survey consumers in the country ourselves to generate comparable data. Wherever we have found statistically significant differences in our results between one country and most or all other countries, thus reflecting significant cultural differences, we have mentioned it again below.

2 Cross-cultural trends

This section summarizes the common cross-cultural trends identified in our survey of data protection professionals in Brazil, China, Germany, Ghana, Japan, Switzerland, and the United States regarding cultural attitudes toward data protection and data disclosure issues in the fields of data autonomy (2.1.) and the data power of companies (2.2.).

2.1 Data autonomy

A majority of data protection professionals across *all* seven countries agree (at least somewhat) that

https://doi.org/10.1515/9783111458366-004

– consumers should be able to decide for themselves about the disclosure of their personal data; and
– they can do so in their country.

The statistically significant differences in agreement between countries (which were found here between Japan, Switzerland, and China on the one hand and all other countries on the other regarding the first point; and between Japan and Switzerland on the one hand and all other countries on the other regarding the second point) are therefore due to differences in the strength of agreement with these points rather than differences as to whether respondents tended to agree or disagree on them.

Moreover, a majority of professionals in all countries but Brazil and the United States believed that consumers in their country could *always* make self-determined decisions about the disclosure of their personal data. This trend was exceptionally strong in China, where respondents were significantly more likely to hold this view than in all other countries. By contrast, Brazilian respondents were significantly less likely to hold this view than respondents in three other countries (China, Germany, and Switzerland), with a majority of them not believing that this was the case. They believed that the following factors restricted consumers' data autonomy:
– secret data collection by companies,
– insufficient information provided by companies,
– data transfers to third parties without users' consent,
– digital data theft,
– data leaks,
– lack of options not to disclose,
– consumers not taking enough time to inform themselves about what happens to their data, and
– consumers being unaware of the consequences of data disclosure.

US professionals were undecided: Half of them said there were some restrictions, the other half said there were no restrictions at all.

In the light of rapidly advancing technological innovations such as "[m]achine learning, artificial intelligence, algorithm-based personalization, and neuroscience" (Wertenbroch et al. 2020, 429; summarizing André et al. 2018), it was surprising that most professionals did not see any deficits or restrictions with regard to the data autonomy of consumers in their country. Such developments are increasingly challenging the basic principle that people should be able to decide for themselves and retain control over what data they want to share with whom and when.

2.2 The data power of companies

Professionals across *all* countries were also largely in agreement about how they preferred companies to handle consumer data. The following "recommendations" can be taken as cross-cultural blueprints for good data processing practice:

Companies should

- only be allowed to collect personal data from consumers with their consent;
- always provide options to delete personal data so that consumers can erase their personal data at any time if they change their mind about data disclosure;
- always explicitly state what consumers' personal data will be used for; and
- always have to request consumers' consent once more when using their data for purposes not previously stated.

These practices were particularly important to professionals in Ghana and Brazil, who showed significantly stronger agreement with these points than respondents in most other countries (Japan, Switzerland, Germany, and China; for Ghana, this list also included the United States).

But what about professionals' assessments of how companies actually handle consumer data in their countries? A majority of professionals in all countries surveyed had trust in at least healthcare providers and financial services companies to use consumers' personal data in the right way. Professional and lay assessments corresponded cross-culturally for healthcare providers (see Thir & Wawra 2023, 16; Wawra 2023b, 77).[21] In Brazil and Germany, laypeople's assessments diverged from those in other countries with regard to financial services companies: In a representative survey conducted by Ipsos (2019, 18, 19, 20), only a minority of respondents in Brazil and Germany expressed trust in financial services companies, while a majority showed confidence in them in the other countries (see Thir & Wawra 2023, 16; Wawra 2023b, 77). An explanatory factor in this finding could be that Germans consider financial data to be much more sensitive than members of other cultures do, as a survey of people from Germany, China, and the United States conducted by Trepte and Masur (2016) has shown (see also Wawra 2023a, 183). Unfortunately, there has been no comparable study contrasting Brazil with the other countries we investigated. An even more differentiated picture emerges when looking at other industries, as will be detailed below.

Besides these cross-cultural trends, there is far more cultural variation with regard to other topics related to data disclosure, as we will discuss in the following.

---

21 Please note again that, here and in the following, Switzerland had to be excluded from the comparisons with laypeople's assessments as we did not have suitable data for a comparative analysis (see above).

3 Cultural differences

There is—in part considerable—cultural variation regarding data protection and disclosure issues in the fields of data autonomy (1), data sensitivity (2), the data power of companies (3), and the impact of data protection and informational privacy regulations (4).

3.1 Data autonomy

A majority of professionals

- in all countries except Japan and China *strongly* (!) agreed that consumers should have the possibility to make self-determined decisions about the disclosure of their personal data. In China, a majority *somewhat* agreed (61 %) and an additional 34 % *strongly* agreed (i.e., 95 % in total). In Japan, however, only 79 % agreed (33 % *somewhat* and 46 % *strongly*). Moreover, the number of neutral answers (18 %) was exceptionally high in Japan compared with the other countries. Both China and Japan exhibited significantly lower agreement than most other countries (Brazil, Germany, Ghana, and the United States);
- in all countries except Ghana and Japan considered the legislation in their country to be *sufficient* or *rather sufficient* to guarantee consumers' data autonomy. Indeed, professionals in those two countries rated the sufficiency of their country's legislation significantly lower than respondents in the other five countries did. At the same time, a majority of Ghanaian and Japanese professionals did not see any deficits in the overall data autonomy of consumers in their countries (see above). However, they did find fault with the data power of certain industries (see section IV.3.3).
- in China, Switzerland, and Japan saw no need to adjust current data protection and informational privacy regulations for any data type (e.g., health data, financial data, etc.). In Germany, this view was held by exactly half of respondents. In Ghana, the United States, and Brazil, only a minority felt this way. The country that stood out the most was Brazil, where this sentiment was significantly less prevalent than in all countries except the United States.[22] By contrast, Chinese professionals were significantly more likely to be completely satisfied with cur-

22 A large majority of Brazilian respondents (72 %) advocated to increase the regulation of data protection and informational privacy for certain data types. A majority of US and Ghanaian professionals (64 % and 54 % respectively) held the same view. There was, however, no majority in any country that opted for stricter (or weaker) regulations for a specific data type. We therefore have not repeated the findings for specific data types here. These can be found in chapter III.1.2.1.

rent regulations regarding all data types (and thus to see no need for adjustment in this respect) than half the other countries (Brazil, the United States, and Ghana).

- in all countries except the United States and Brazil saw no need to adjust current data protection and informational privacy regulations for any data-disclosure context (e.g., using smartphone apps, disclosing data to foreign governments, etc.). The country that stood out the most in this respect was, again, Brazil, where professionals were significantly less likely to be completely satisfied (and thus see no need for adjustment) in this regard than in all countries except the United States.[23] US respondents also stood out, as they were significantly less likely to be completely satisfied than respondents in half the other countries (China, Germany, and Japan.)
- in all countries except the United States, Ghana, and Brazil saw no need to adjust current data protection and informational privacy regulations for any data collection purpose (e.g., law enforcement, medical research, marketing, etc.). Once more, Brazilians stood out the most, being significantly less likely to hold this view than respondents in most other countries (China, Japan, Germany, and Switzerland).[24] Similarly, US professionals were significantly less likely to feel this way than respondents in half the other countries (China, Japan, and Germany). By contrast, Chinese professionals were significantly more likely to be completely satisfied with current regulations concerning any data collection purpose than half the other countries (Brazil, the United States, and Ghana).
- in all countries except Ghana, the United States, and Brazil saw no need to adjust current data protection and informational privacy regulations for any industry. Brazil was once again the country that stood out the most, with professionals there significantly more likely to see a need for adjustment in this respect than professionals from *all* other countries except the United States.[25]

---

23 A majority of Brazilian and US professionals (58 % each) advocated to increase the regulation of data protection and informational privacy in certain data disclosure contexts. Again, however, there was no majority in any country that opted for stricter (or weaker) regulations in a specific data disclosure context. We therefore have not repeated the findings for specific contexts here. These can be found in chapter III.1.2.2.

24 A majority of Brazilian (53 %), US (53 %), and Ghanaian (52 %) professionals advocated to increase the regulation of data protection and informational privacy for certain data collection purposes. Again, however, there was no majority in any country that opted for stricter (or weaker) regulations for a specific data collection purpose. We therefore have not repeated the findings for specific purposes here. These can be found in chapter III.1.2.3.

25 A majority of Brazilian (66 %) professionals advocated to increase the regulation of data protection and informational privacy in certain industries. A majority of US (57 %) and Ghanaian (54 %) professionals held the same view. Again, however, there was no majority in any country that opted

Chinese professionals were once again significantly more likely to see no such need than half the other countries (Brazil, the United States, and Ghana).

We have thus identified low-satisfaction countries and high-satisfaction countries when it comes to the current state of data protection and informational privacy regulation. The former are countries in which a majority of professionals saw a need to adjust current regulations in all four categories surveyed (data types, contexts of data disclosure, data collection purposes, and industries) and where professionals were significantly more likely to hold this opinion than respondents in at least half the other countries regarding at least two categories. These countries were Brazil and the United States.

By contrast, China is a high-satisfaction country, as a clear majority of Chinese professionals were content with current regulations in all four categories surveyed, and respondents in China were usually significantly more likely to hold this opinion than respondents in half the other countries.

The remaining countries—Germany, Ghana, Japan, and Switzerland—are intermediate cases. Ghana leaned more toward the low-satisfaction countries, as a majority of Ghanaian professionals saw a need for adjustment in three out of four categories. However, across all four categories, Ghanaian respondents were significantly more likely to hold this opinion than respondents from only two countries at most. Thus, Ghana still classifies as an intermediate case.

In Japan, Switzerland, and Germany, a majority of professionals (albeit smaller majorities than in China) were content with current regulations in three or four categories. Switzerland was a true in-between case as it differed significantly from only a single country (Brazil) regarding all four categories. Germany and Japan leaned more toward the high-satisfaction countries because, for two or three categories, German and Japanese respondents were significantly more likely to be content with current regulations than respondents from two or three countries.

Furthermore, a majority of professionals

– in all countries except Ghana considered consumers to be *very* or *rather aware* of how data protection and informational privacy are regulated. This trend was particularly strong in the United States and China, where professionals rated consumer awareness significantly higher than professionals in most other countries did (Ghana, Japan, Brazil, and Switzerland for China; for the United States, this list also included Germany);

---

for stricter (or weaker) regulations for a specific industry. We therefore have not repeated the findings for specific industries here. These can be found in chapter III.1.2.4.

– in all countries except Switzerland and, in particular, Japan thought that consumers were doing enough to protect their personal data. However, just under half the professionals in Switzerland held this opinion. Accordingly, it was Japanese professionals' assessments of consumers' data protection literacy that stood out here, as they were significantly less positive than in *all* other countries.

The professionals' overwhelmingly positive assessments of consumers' awareness of data protection and informational privacy regulations in their countries do not always correspond to consumers' self-reports. Thus, Japanese, US, Brazilian, and Chinese professionals may have overestimated their populations' data literacy in this respect, as representative surveys reveal. German and Ghanaian consumers are the only ones who predominantly report being very or somewhat aware of these regulations, while a majority of respondents from other countries say that they are not very or not at all aware (see Thir & Wawra 2023, 13; Wawra 2023a, 187; CIGI-Ipsos 2019b, 281). The discrepancy between professionals' assessments and consumers' self-evaluations is particularly large in Japan, where 84 % of consumers reported not being very aware or at all aware of these regulations (CIGI-Ipsos 2019b, 281; Wawra 2023a, 187), whereas only 54 % of Japanese data protection professionals considered laypeople to be very or rather aware of them. However, it is equally plausible that consumers in these countries may have underestimated their awareness of data protection and informational privacy regulations. In Ghana, consumers may have overestimated their data protection literacy in this respect (for further discussion, see V.3.5): In contrast to Ghanaian professionals' overall negative assessment, a majority in our own survey of the Ghanaian population reported being very or somewhat aware of the rules in their country (Thir & Wawra 2023, 13). Regarding the question of whether consumers were doing enough to protect their data, self-evaluations and professional assessments corresponded in all the countries surveyed (Thir & Wawra 2023, 13; CIGI-Ipsos 2019b, 283)—though there were no self-reporting data available for China and, as always, Switzerland.

3.2 Data sensitivity

The overall distribution of mean sensitivity ratings across all 33 data categories in each country shows that the ratings given by US professionals tended to be the highest, followed—in descending order—by Germany, China, Ghana, Switzerland, Brazil, and Japan. It is noteworthy that Japanese professionals gave significantly lower mean sensitivity ratings than most other countries (the United States, China, Germany, and Switzerland), while US respondents gave significantly higher ones than

respondents in three other countries (Japan, Switzerland, and Brazil). Moreover, Japan's data protection law lists the fewest sensitive data categories—i.e., five—compared with the other countries. At the same time, US state laws (CPRA and VCDPA) have the most sensitive data categories—i.e., 16 (see Wawra 2023a, 180).

3.3 Data power of companies and governments

3.3.1 Trust

A majority of professional respondents from all countries surveyed trusted shipping/delivery, telecommunications, and media companies, search and social media sites, and retailers to use consumers' personal data in the right way, except professionals from

- Switzerland with regard to telecommunications companies;
- Switzerland and Japan with regard to shipping/delivery companies and retailers selling goods and services;
- Switzerland, Ghana, and Japan with regard to media companies; and
- Switzerland, Germany, Ghana, Japan with regard to search and social media sites.

Thus, search and social media sites were the industry that was not trusted by a majority of professionals in four out of seven countries. This industry received significantly lower trust ratings than most other industries in Japan, Ghana, and Switzerland. Similarly, media companies received significantly lower trust ratings in Japan and Ghana than most other industries. Thus, those two industries deserve particular attention.

Let us now compare the professionals' assessments with the level of trust that laypeople have in different industries to correctly handle of consumer data. Across *all* countries surveyed except China, consumers overwhelmingly do not have a great deal or fair amount of trust in media companies or search and social media sites to handle their data correctly (see Thir & Wawra 2023, 16; Wawra 2023b, 77; Ipsos 2019, 18, 19, 20). Thus, professionals' views were in line with laypeople's views in this respect in Ghana and Japan, as they were in Germany regarding search and social media sites, but not regarding media companies. In addition, there is a mismatch between professionals' and laypeople's views' of both industries in the United States and Brazil, where, in contrast to laypeople, a majority of professionals trusted those two industries to use consumer data correctly.

Furthermore, in *all* countries but China and Ghana, consumers overwhelmingly do not have a great deal or fair amount of trust in shipping/delivery, telecommunications companies, or retailers. Thus, there is a mismatch between laypeo-

ple's and professionals' trust in these industries in the United States, Brazil, and Germany, where a majority of professionals trusted these industries. The same discrepancy can be found for Japan regarding telecommunications companies.

Turning to trust in governments, our survey shows that a majority of professional respondents from all countries had trust in their national and foreign governments, except professionals from

- Japan with regard to their own government. Japanese trust ratings in this respect were significantly lower than those in three other countries (China, the United States, and Germany). The country that stood out the most here, however, was China, where trust in the national government was significantly higher than in all other countries except the United States. US trust ratings were second highest and significantly surpassed those of three other countries (Japan, Switzerland, and Brazil).
- Japan and Switzerland with regard to foreign governments. Japanese professionals had significantly lower trust in them than respondents from all other countries, while Swiss respondents had significantly lower trust than respondents from three other countries (Ghana, the United States, and China).

In addition, in all countries except Ghana, professionals' trust in the national government to handle personal data correctly was significantly higher than their trust in foreign governments.

Again, let us examine how these trends compare to those observed regarding consumers' views in the respective countries. In *none* of the countries studied, except Ghana and Switzerland[26] with regard to their own governments (see Thir & Wawra 2023, 15; Thir et al. 2023, 43), did a majority of consumers express a great deal or fair amount of trust in their national government or foreign governments regarding the correct handling of consumer data (Wawra 2023b, 74).[27] Professionals' and consumers' assessments in this regard are thus in line regarding their own governments in Ghana, Japan, and Switzerland, and in relation to foreign governments in Japan.

Corresponding to professionals' assessments, in all countries for which we could find suitable data but Ghana, consumers' trust in their own government is

26 Please note that Ghana and Switzerland were not included in the Ipsos 2019 survey, in which the other countries were directly compared. We therefore refer to our own survey on Ghana and to other surveys that were conducted in Switzerland on this topic. Thus, it is not possible to directly compare the surveys, but they provide a good indication of consumers' attitudes in those countries.
27 Please note that there are no comparable data that express Chinese people's attitudes toward their national government and no suitable data for comparison regarding Swiss people's attitudes toward foreign governments.

overwhelmingly higher in this regard than in foreign governments (see Thir & Wawra 2023, 15; Wawra 2023b, 74; Ipsos 2019, 20).

We can thus identify high-trust countries when it comes to the correct use of personal data, i.e., countries in which all industries[28] were trusted a great deal or a fair amount by a majority of *professional* respondents. These countries are the United States, China, and Brazil. China is also a high-trust country in terms of consumer assessments, while the other two countries are not (see above).

Japan and Switzerland, in contrast, can be categorized as low-trust countries in this regard: A majority of professionals considered most industries untrustworthy when it came to the correct use of personal data. This is in line with the assessments given by Japanese consumers (see above); however, there are no data for Switzerland that could be used for a comparison.

Germany and Ghana are in-between cases. If we were to only consider how many of the seven surveyed industries were trusted by a majority of respondents, both countries would have to be regarded as rather high-trust countries, since professionals in both countries trusted the overwhelming majority of industries to handle consumer data correctly. Thus, German professionals only distrusted search and social media sites, which Ghanaian professionals also distrusted in addition to media companies. Again, this is not how consumers feel (see above). When considering the statistical significance of cross-cultural differences in trust in various industries to handle consumer data correctly, however, German trust ratings prove to be more similar to those of low-trust countries than those of high-trust countries. Ghanian trust ratings are more similar to those of high-trust countries.

3.3.2 Compliance

A majority of professionals in China and the United States considered compliance with the regulation of consumer data protection and informational privacy to be *sufficient* or *rather sufficient* in *all* the industries surveyed.

A majority of Brazilian professionals also assessed compliance as *sufficient* or *rather sufficient* across all industries except retailers, regarding which they were undecided (50 % considered compliance there to be *sufficient* or *rather sufficient*).

Professionals from all countries except Japan were satisfied with compliance in the healthcare and finance sectors.

Professionals from Japan, Ghana, and Switzerland were the most critical about compliance in their countries: Only a minority of

28 Please note that trust ratings of national and foreign governments were not included in the analysis upon which a country's categorization as either a high-trust or low-trust country is based.

- Ghanaian and Swiss professionals rated compliance as *sufficient* or *rather sufficient* in all the sectors surveyed except the healthcare sector and financial services companies;
- Japanese professionals rated compliance as *sufficient* or *rather sufficient* across *all* industries. A majority of respondents from Japan even explicitly said that compliance was *insufficient* or *rather insufficient* for search and social media sites as well as media companies.

While a majority of German professionals were satisfied with compliance in the healthcare and financial sectors, German respondents were undecided with regard to telecommunications companies and retailers (50 % considered compliance to be *sufficient* or *rather sufficient*), and only a minority assessed the compliance of shipping/delivery companies, search and social media sites, and media companies as *sufficient* or *rather sufficient*.

Brazil, China, and the United States can thus be categorized as countries with high perceived compliance, i.e., compliance with the regulation of consumer data protection and informational privacy was considered *sufficient* or *rather sufficient* by a majority of respondents in (almost) all the industries surveyed.

Japan and Switzerland are countries with low perceived compliance, i.e., compliance with the regulation of consumer data protection and informational privacy was not considered *sufficient* or *rather sufficient*" by a majority of respondents in (almost) all industries surveyed. Based on how many of the seven industries surveyed were considered compliant by a majority of respondents, Ghana also falls in this category. However, when considering the statistical significance of cross-cultural differences in perceived compliance, Ghana occupies more of an in-between position between the countries with high and low perceived compliance, albeit leaning more toward the latter. Germany is a truly intermediate case between these two categories.

3.3.3 Enforcement

The enforcement of consumer data protection by the national government was considered heavy/robust by a majority of professionals in all countries except Ghana and Japan. Japan stood out the most, where government enforcement was considered significantly weaker than it was by respondents in all other countries except Ghana. In Ghana, government enforcement was perceived to be significantly weaker than it was in three other countries (China, Brazil, and the United States). Accordingly, both are countries with low perceived government enforcement. By contrast, China is a country with high perceived government enforcement, based both on significant differences with other countries and the fact that an exceptionally high pro-

portion of respondents (75 %) assessed government enforcement as either heavy or robust.

Enforcement by private parties and within companies was seen as heavy or robust by a majority of professionals in Brazil, China, and the United States. Brazil and China stood out in particular regarding enforcement by private parties, which was perceived to be significantly stronger in those countries than in most other countries (Japan, Switzerland, Ghana, and Germany). Accordingly, both countries can be categorized as countries with high perceived enforcement regarding private parties. By contrast, Japanese professionals perceived enforcement by private parties to be significantly weaker than respondents in *all* other countries did and can thus be characterized as a country with low perceived enforcement in this respect.

Japan also stood out regarding the perceived enforcement of consumer data protection within companies, which was significantly weaker there than in all countries except Switzerland. Japan can thus also be classified as a country with low perceived corporate enforcement. By contrast, China is a country with high perceived corporate enforcement based on significant differences to other countries.

3.3.4 Levels of consumer data protection

A majority of professionals in China and the United States evaluated the levels of consumer data protection in *all* industries surveyed as *sufficient* or *rather sufficient*.

Brazilian professionals were (rather) satisfied as well, except with consumer data protection in the retail sector.

Ghanaian and Swiss professionals only considered data protection in the healthcare and financial services industries to be *sufficient* or *rather sufficient*.

For Japanese respondents, the only industry that provided satisfactory (i.e., *sufficient* or *rather sufficient*) data protection for consumers was the healthcare sector. Moreover, Japanese professionals were the only ones who predominantly considered data protection on search and social media sites and media companies in their country to be *insufficient* or *rather insufficient*.

Germany occupied the middle ground: Professionals there assessed data protection as *sufficient* or *rather sufficient* in most industries surveyed, i.e., healthcare, finance, shipping/delivery companies, and retailers. They were undecided (50 %) with regard to telecommunications companies, and the majority of professionals were not convinced of the sufficiency of search and social media sites and media companies.

The United States, China, and Brazil can thus be categorized as high-satisfaction countries, as a majority of respondents considered the level of consumer data protection satisfactory for (almost) all industries surveyed there. This contrasts with our findings of cross-cultural differences in satisfaction based on professionals' as-

sessments of whether adjustments need to be made to current consumer data protection and informational privacy regulations in their countries (see IV.3.1). According to those findings, the United States and Brazil ought to be classified as low-satisfaction countries.

Based on professionals' assessments of consumer data protection levels, Japan and Switzerland are low-satisfaction countries. There, only one or two industries were considered satisfactory by a majority of respondents in terms of the levels of consumer data protection they provide. The same was true for Ghana. Thus, based on this criterion alone, Ghana is also one of the low-satisfaction countries. However, when considering the statistical significance of cross-cultural differences in perceived levels of consumer data protection, Ghana occupies more of an in-between position between high- and low-satisfaction countries. Germany is another intermediate case, though in contrast to Ghana, it leaned slightly more toward the high-satisfaction countries.

Finally, a majority of professionals in China, Brazil, the United States, and Germany regarded current regulation to be *sufficient* or *rather sufficient* to prevent the corporate misuse of consumer data. In Ghana, this figure was exactly 50 % of respondents. In Switzerland and Japan, however, only a minority held this view. It is particularly noteworthy that Japan was the sole country where respondents expressing the view that regulation was *insufficient* or *rather insufficient* outnumbered those who considered it *sufficient* or *rather sufficient*. Accordingly, Japanese sufficiency ratings for this item were significantly lower than those given by respondents in all other countries, while Swiss ratings were significantly lower than US, Brazilian, and Chinese ratings. This item thus further corroborates the finding that Japan and Switzerland are low-satisfaction countries when it comes to the level of consumer data protection provided.

3.4 Impact of data protection and informational privacy regulations

3.4.1 … on companies with regard to customer orientation, innovation, and cooperation

In all countries, except Japan,[29] a majority of professionals agreed that data protection and informational privacy regulations in their country still allowed companies to

29 However, the majority in Japan did not say that current regulations (somewhat) hindered companies to do these things. A considerable number of Japanese respondents took a neutral stance (see above).

– tailor their products and services to consumers' needs;
– be innovative, i.e., develop new products and services; and
– cooperate with other companies in their country.

Regarding all of these points, Japanese professionals exhibited significantly lower agreement than respondents from all other countries except Switzerland. Swiss respondents also stood out in that they exhibited significantly lower agreement than professionals from most other countries (the United States, China, Brazil, and Ghana) regarding the second point and significantly lower agreement than respondents from three other countries (China, Brazil, and the United States) regarding the last point.

A majority of professionals across all countries surveyed except Switzerland and Japan[30] also agreed that data protection and informational privacy regulations in their country still allowed companies to cooperate with companies in other countries

– with essentially equivalent data protection and informational privacy regulations,
– no matter how they regulate data protection and informational privacy.

On both points, Japanese professionals exhibited significantly lower agreement than respondents from all other countries except Switzerland. Swiss respondents also agreed significantly less than all other countries except Japan regarding the first point, while they exhibited significantly lower agreement than professionals from three other countries (the United States, China, and Brazil) on the second point. By contrast, Chinese and US respondents agreed significantly more strongly with the first point than respondents from most other countries (Japan, Switzerland, Ghana, and Germany).

Thus, overall, a majority of respondents in all countries tended to agree with these statements, apart from respondents in Japan and, sometimes, Switzerland. Japan clearly stood out the most, since for all questions, Japanese respondents exhibited the lowest agreement (followed by Swiss respondents) and significantly lower agreement than all countries but Switzerland. Switzerland was most similar to Japan in that, for two questions, only a minority agreed with the given statement; Switzerland and Japan did not differ significantly from each other for any of the five questions; and for all but the first question, Swiss agreement was significantly lower

30 However, the majority in Switzerland and Japan did not say that current regulations were *insufficient* or *rather insufficient* in this respect either. A considerable number of Japanese and Swiss respondents took a neutral stance (see above).

than that of respondents from three to five other countries (these always included the United States, China, and Brazil; Ghana was included twice, Germany once).

Finally, it is noteworthy that China was *always* one of the countries with the highest proportion of agreement, usually together with the United States and sometimes (also) Brazil. Moreover, the United States *always* had the greatest proportion of respondents who strongly agreed. For four out of five questions, US respondents agreed to a significantly greater extent than respondents from three to four other countries. These always included Japan and Switzerland, and sometimes Ghana, Germany, or China.

3.4.2 … on bureaucracy, privacy management, and information overload

In all countries but Japan and Switzerland,[31] a majority of professionals agreed that the regulation of data protection and informational privacy

- had created too much bureaucracy for the state, for companies, and for consumers. US respondents in particular believed that regulation created too much bureaucracy for the state, significantly more so than respondents in three other countries did (Japan, Switzerland, and Brazil). However, regarding excessive bureaucracy for companies, it was Chinese professionals who stood out the most, agreeing significantly more strongly with the statement than respondents in all countries but the United States. Japanese professionals believed significantly less strongly that regulation caused excessive bureaucracy for consumers than professionals from most other countries (China, the United States, Brazil, and Germany);
- had led to companies handling data more professionally. Japanese and Swiss respondents agreed significantly less with this statement than respondents from most other countries (China, Brazil, the United States and Germany). By contrast, this sentiment was particularly strong among US. Chinese, and Brazilian respondents, significantly more so than in most other countries (Japan, Switzerland, Ghana, and Germany). This is in line with their status as high-satisfaction countries regarding the levels of consumer data protection offered in various industries (see IV.3.3.4);
- enabled consumers to easily manage their privacy needs. Chinese and US respondents in particular believed this to be the case, significantly more so than respondents from three to four other countries (Japan, Switzerland, and Ger-

31 However, the majority in Japan and Switzerland did not say that current regulations had the (somewhat) opposite impact either. A considerable number of Japanese and Swiss respondents took a neutral stance (see above).

many; for China, this list also included Ghana). Japanese respondents agreed significantly less with this statement than respondents from all countries but Switzerland, and Swiss respondents agreed significantly less than respondents from three countries (China, the United States, and Brazil).

The majority of professionals from all countries but Ghana and Japan thought that the regulation of data protection and informational privacy overloaded consumers with information. This sentiment was particularly strong among Chinese respondents, significantly more so than for respondents in most other countries (Japan, Ghana, Switzerland, and Brazil).

In sum, Japanese respondents exhibited the lowest amount of agreement with all these statements, generally followed by Swiss respondents.[32] They exhibited significantly lower agreement with half of the statements than most other countries (China, the United States, Brazil, Germany, and, in one instance, Ghana as well) and, for one statement, significantly lower agreement than half the other countries (China, the United States, and Germany). By contrast, China was *always* among the countries with the highest proportion of respondents who agreed (usually together with the United States and sometimes [also] Brazil).[33] Chinese respondents agreed with four out of six statements to a significantly greater extent than respondents from most other countries. These always included Japan, Switzerland, and Ghana.[34] For three out of six statements, the United States had the greatest proportion of respondents who strongly agreed, and US respondents agreed with three out of six statements (not necessarily the same ones) to a significantly greater extent than respondents from three to four other countries. These always included Japan and Switzerland.[35]

3.4.3 … on fundamental rights, digitalization, and overall effect

The majority of professionals from all countries surveyed but Japan considered the current regulation of data protection and informational privacy to be *sufficient* or *rather sufficient* to protect the fundamental rights of individuals. The majority of Japanese professionals, however, did not think that they were inadequate either, with

32 Switzerland is indeed the country that is most similar to Japan in that Switzerland and Japan did not differ significantly from each other on any of the statements.

33 The US came in second place four times and in third place twice, and was thus always among the top three.

34 Germany was included three times; Brazil was included twice.

35 Germany was included twice; Brazil and Ghana were each included once.

many of them (40 %) giving a neutral answer (see above). Their sufficiency ratings were significantly lower than those given by respondents from *all* other countries.

Professionals overwhelmingly stated that the regulation of data protection and informational privacy was having a *positive* or *very positive* impact on digital development and the implementation of digital innovation in their countries. Japan and Switzerland were the exceptions. However, even in Japan and Switzerland, only a small minority believed that current regulations had *negative* or *very negative* effects in this respect. Considerable numbers of Japanese and Swiss respondents took a neutral stance (43 % of Swiss professionals, 47 % of Japanese professionals; see above). Accordingly, Japanese respondents' assessments were significantly less positive than those given by respondents in all other countries except Switzerland, and Swiss respondents' assessments were significantly less positive than those made by respondents in three other countries (China, the United States, and Brazil). The most positive assessments were provided by Chinese and US respondents, significantly more than in most other countries (Japan, Switzerland, Ghana, and Germany).

Overall, a majority of professionals from China, the United States, Brazil, and Germany expressed the opinion that the regulation of data protection and informational privacy had a positive impact. For Brazil and China, this corresponded to consumers' assessments. German consumers overwhelmingly saw a neutral (50 %) or negative (10 %) impact. The United States was not part of this survey (see Cisco 2021, 10). In the present survey, Chinese and US professionals stood out as their assessments were significantly more positive than those of respondents in three to four other countries (Japan, Ghana, Switzerland; for China, this list also included Germany).

The majority of Japanese professionals (53 %) thought that the regulation of data protection and informational privacy had a neutral impact, as did 50 % of Swiss professionals. The number of neutral answers was also rather high in Ghana (46 %) and made up the largest proportion of the three answer options. It is noteworthy that Japanese professionals' assessments were significantly less positive than those given by respondents in most other countries (China, the United States, Brazil, and Germany). In contrast, Japanese consumers overwhelmingly believed that their privacy laws had a positive impact. Switzerland was not part of that survey (see Cisco 2021, 10). In our own survey in Ghana, a majority of consumers attested a neutral impact to data protection and privacy regulations in their country (only about one-third saw a positive effect) (Thir & Wawra 2023, 13). Thus, while the results for professionals and consumers are more or less in agreement for Ghana, this is not the case for Japan.

In sum, a majority of professionals in most countries evaluated their country's regulation of data protection and information privacy as positive/sufficient with re-

spect to the aspects surveyed. These countries *always* included China, the United States, Brazil, and Germany.[36] Japan is a noteworthy exception as, for all three ratings, only a minority of professionals evaluated the regulation as positive/sufficient.[37] Moreover, Japanese respondents always gave the lowest ratings, generally followed by Swiss (and once by Ghanaian) respondents.[38] For *all* ratings, they assessed regulation as significantly less positive/less sufficient than most other countries did. These countries always included China, the United States, Brazil, and Germany.[39] By contrast, the United States, China, and Brazil always took the top three places in terms of the proportion of *positive* or *very positive*, or *sufficient* or *rather sufficient* ratings. For two out of three evaluations, China was the country with the highest proportion of positive assessments (following Brazil very closely for the third one). In these two cases, Chinese and US evaluations were significantly more positive than those in three to four other countries (Japan, Ghana, Switzerland, and Germany).

36 Ghana was included twice, Switzerland only once.

37 This was also the case for Switzerland in two out of three cases and for Ghana in one case.

38 Switzerland was indeed most similar to Japan in that, for two out of three ratings, only a minority evaluated regulation as positive or very positive. Switzerland and Japan did not differ significantly from each other on these two ratings.

39 This included all of the countries in one case.

V Discussion of factors influencing data disclosure

1 Introduction

When we started our interdisciplinary research project, our overarching research question was: What influences people's data disclosure behavior and are there cultural differences in this regard? In the cultural part of the project, we generally took a macro research perspective and examined our topic on a societal or national level. The objective was to gain informed insights based on large data sets and to generate an overview of eight privacy cultures (for an introduction, see Wawra 2022). We first approached our research question from the perspective of consumers, resulting in eight country reports (see Howe 2022; Kessel 2022; Thir & Wawra 2023; Thir et al. 2023; Wawra et al. 2022a; 2022b; 2022c; 2022d) and two comparative discussions of consumers' perceptions of the key aspects influencing data disclosure in our eight countries (see Wawra 2023a; 2023b).

Here, we took a complementary approach to the consumer perspective and looked into data protection professionals' views on the regulation of data protection as well as the governmental and corporate practices that framed data disclosure in their countries. In this chapter, we will return to our basic research question and the macro level. On the basis of our work in the project, we will begin by proposing an integrative model that aims to summarize the main factors that can play a role in people's disclosure behavior (V.2). We will then focus on the most fundamental of these factors, cultural privacy norms and values, and discuss their explanatory potential for each of our selected countries (V.3). We will selectively consider other factors in our Data Disclosure Model as well when they appear to be particularly relevant to the survey results in the countries for which there is little research on basic privacy orientations.

2 Data disclosure model

The causes of people's attitudes toward privacy and their ensuing data disclosure behavior are manifold, multifactorial, intertwined, and can be found on multiple levels. With our Data Disclosure Model (DDM), which we outline below, we aim to offer an integrative perspective on data disclosure. It can be applied to all sorts of data disclosure situations in both on- and offline contexts. It generalizes beyond the concrete data disclosure scenario. It should be kept in mind that the real impact of the individual factors, their force, and direction of influence (promoting or hindering data disclosure) depend on the actual disclosure situation. Our model aims to provide a comprehensive overview of the many potential factors that can influence

https://doi.org/10.1515/9783111458366-005

people's data disclosure behavior, structuring them and demonstrating their interdependence. It can be used as a starting point for theoretical and empirical studies on data disclosure.

The *individual* is at the center of any data disclosure situation and therefore the key element in our model (individual or micro level). Aggregated individual behavior informs collective behavior that defines *cultures* (collective or macro level). Let us therefore start with the role of the individual in our Data Disclosure Model (1), before we explain the other factors (2–14) that can have an impact on disclosure:

(1) In offline and online contexts alike, individuals can either be *aware* of the fact that they are disclosing data or not. In offline contexts, for example, we automatically disclose data about ourselves as soon as we interact with somebody else. Others learn about our body features, language, clothing, etc., and can use those data to draw conclusions about us. Online, individuals are not always aware of the fact that, when they surf the internet, for instance, they are disclosing data about themselves while they are being automatically tracked if they have not taken precautions to prevent this from happening. It thus varies in both contexts whether individuals as *data owners consciously or unconsciously* (see below) share data and how much (if at all) they reflect on the fact that they are potentially disclosing data beforehand. Whether data disclosure is preceded by (more or less intense) conscious deliberation or whether it is performed without thinking about it (see Ackermann et al. 2021; Kim et al. 2015; Wawra 2022) depends on the concrete disclosure situation and on the individual themselves. Data disclosure in general is influenced by an individual's specific *personality traits, dispositions, knowledge,* and *skills* (see, e.g., Ghose et al. 2022; Robinson 2018; Wawra 2022; Zhang et al. 2021). A very introverted person is likely to have an inherently lower predisposition toward sharing data to begin with. In addition, *sociodemographic factors* such as age, gender, and education can affect a person's disclosure behavior (see Anaraky et al. 2021; Trepte & Masur 2017; Herbert et al. 2020). Furthermore, a person who has more *data protection literacy* is likely to be more aware of disclosure and to have more technical means at their disposal to protect their data (if they want to), particularly in online contexts. Data protection literacy has an (a) *epistemological* and a (b) *procedural* component that should be distinguished from each other. Data protection literacy thus encompasses (a) "people's awareness and knowledge of data protection, privacy rules and policies" and (b) "the skills they [report to] have, and the measures they [say they] take to protect their personal data" (Wawra 2022, 9).[40]

40 Please note that the impact of the legal context (9) on data disclosure is closely linked to an individual's data protection literacy.

All of these factors can reinforce each other but may also work against each other in a disclosure situation. It will therefore always vary individually whether somebody exerts considerable or minimal cognitive effort, i.e., takes the high or low route of cognitive effort.[41] It is to be expected that the more problematic (see below) an individual considers a disclosure situation to be in terms of privacy and data protection issues (depending on the factors mentioned above), the more likely and thorough conscious deliberation will be.

The personality traits of the data owner develop in the interaction between the individual and their social and cultural environment (meso [institutional] and macro level). At the same time, individuals' actions can change or transform that environment (see, e.g., Hedström & Swedberg's [1998] model of social mechanisms).[42] The influence is therefore mutual or bidirectional.

(2) Thus, *cultural (privacy) values and norms* that are based on formative historical influences (see, e.g., V.3.7 on how Germany's Nazi past impacted the country's privacy orientation) are factors that also have to be weighed in when taking a comprehensive look at data disclosure. This factor in data disclosure potentially influences all of the factors in data disclosure cited here.

(3) Another important factor than can affect individuals' disclosure behavior is whether they consider the use of, for example, a particular offline or online service or digital application that collects data to be a *necessity* or a *choice*: The greater the urgency to use the service or application in question, the more likely a data owner will be to disclose even sensitive data.

(4) However, the individual's perception of the *sensitivity of the data* they are about to disclose can still play an important role in data disclosure (assuming the individual is aware of the disclosure). Some studies even claim that the more sensitive the data, the less influence other factors have on an individual's disclosure behavior (see, e.g., Ackermann et al. 2021). Again, this only applies to situations in which individuals are aware that they are disclosing data that they perceive as more or less sensitive. How sensitive somebody perceives certain data to be depends above all on their personality traits, sociodemographic factors (1), and cultural privacy values and norms (2), as well as the following factors, which can also influence disclosure behavior in general:

(5) Individuals' *past experiences with data disclosure*, pertaining to certain kinds of data (4), disclosure contexts (8–14), and data recipients (7) in particular also potentially impact their data sharing practices.

---

41 Whereas high-effort decisions involve "a rational choice that makes full use of all available information, … low-effort processes are based on mental shortcuts like heuristics and stereotypes to save cognitive energy" (Richthammer & Widjaja 2023, 43; drawing on Petty & Cacioppo 1986).

42 This model is based on Coleman's (1986) macro-micro-macro model.

(6) *Privacy concerns and risks*: The greater the concerns and risks someone associates with data disclosure in a specific situation, influenced by all the factors mentioned so far as well as those that are to follow, the less pronounced their inclination to disclose data will be.
(7) The *data recipient* is also key to disclosure: It depends on the data owner's (1) trust in and past experience (5) with them, as well as on
(8) The *purpose of the (potential) data collection*:
    a. Disclosure is more likely if it aligns with the data recipient's (7) business or mission in the eyes of the data owner (see Ackermann et al. 2021; Wawra 2022): Skepticism about disclosure is very likely to be less pronounced if a healthcare provider asks for health data than if a dating app asks for them.
    b. The (expected) *benefit* of the data collection to the data owner (1)—assuming they are aware of the data collection—can also have an impact on disclosure: The more beneficial the data use seems to someone, the more likely they are to disclose. For example, if they believe that contributing to a research project that aims to develop a better corona vaccine is an important cause, they will be more likely to disclose data for the greater social good—that is, altruistic motives and societal benefits can play a role (see, e.g., Thir et al. 2023). Clearly, the perception of such benefits can vary across cultures, exemplifying how cultural values and norms (2) play a role in data disclosure behavior.
(9) The *legal context*: First of all, we have to distinguish between "law in books" and "law in action": Whereas law in books "describes all written-down laws, regulations and written legal customs," law in action refers to

> how … [the law] is actually applied and practiced in society. … [It] is also concerned with the effect of laws on actual people in the real world as well as the impact of legal frameworks and societal interpretations of the rule-of-law. (Puaschunder 2022, 1)

In our survey, we focused on the part of law in action that looks at people's perceptions of informational privacy and data protection regulations. Both, actual legislation (law in books) and people's interpretations of it (law in action) can influence data disclosure. Legislation (law in books) provides a framework for data disclosure as it defines, for example, which data may be collected and by whom. It also has an impact in that it may, for instance, allow tracking or profiling. This also regularly leads to data disclosure of which individuals are often unaware when they surf the internet or use certain online applications and services (1).

Regarding law in action we can differentiate further between "assured" and "self-determined privacy" (see Richthammer & Widjaja 2024): The better a person believes (a) their data to be protected by *assured privacy*—i.e., *legislation*,

institutional practices, and default settings—or the better they perceive (b) their *self-determined privacy* to be—i.e., the options they have to protect their data themselves and their ability do so—the lower their perceived privacy concerns and risks (6) and, thus, the more likely they will be to disclose. Individuals' perceptions of all aspects of both kinds of privacy depend on their data protection literacy (1). The perception of assured and self-determined privacy can also be influenced by all the factors mentioned so far and by those that follow.

(10) The *media coverage and media framing* of privacy-related issues (including, e.g., debates on informational privacy and data protection) can also play a role in a data disclosure situation, as media content and its framing contributes to the formation of opinions. In a recent representative online survey of 1,021 respondents in Germany, for example, a majority of 63 % (in comparison to 72 % in 2018) reported that current news about data protection breaches made them pay more attention to protecting their personal data (DDV/Acxiom 2022, 28).

(11) The *communication* of privacy and data protection issues in the concrete (potential) data collection situation or the lack thereof is another factor with a potential impact on data disclosure that must be taken into account. An explicit guarantee, for example, that the data will not be shared with third parties can weigh in favor of disclosure. Thus, the *transparency* or *opaqueness* of communication can be relevant. Moreover, the *intelligibility* and *accessibility of the message* must be considered as well (i.e., the length and complexity of the message), as it is paramount for the party requesting the data that the data owner interprets the message as intended. Communication should therefore be easy to process, i.e., clear, unambiguous, not longer than necessary, and orderly (see, e.g., in particular Grice's [1975] maxims of manner and quantity). Furthermore, the *tone* (positive/negative, emotional/factual) can affect how the message is processed and interpreted by the data owner and which conclusion they will draw.

(12) *Time* is another relevant factor in this context: In addition to formative historical experiences (2), current or recent events related to privacy issues and data protection can influence people's willingness to share. Shortly after a data scandal has become public (10), people can be more sensitive to the potential risks of data disclosure. If a data recipient (7), however, has recently been acknowledged by experts for the way it protects privacy in leading media (10), for example, an individual who received that information will potentially be more open to disclosing their data to that recipient.

(13) The *place* of the (potential) disclosure situation is important as well: Is the data being disclosed, e.g., online or offline, on social media, or at a doctor's office? The place influences data protection because it above all affects how easily data can be shared and passed on to third parties.

(14) Finally, the *type of disclosure* can be crucial in a data disclosure situation: Is it (non-, pseudo-, or semi-)anonymous? This has even been identified by Ackermann et al. (2021) as the single most decisive determinant in disclosure (see also Wawra 2022). The *mode* of data exchange—visual or verbal communication (spoken/written), recorded/non-recorded—and its implications for data storage and potential data misuse is also relevant. It will thus make a difference whether data are revealed, e.g., orally to a data recipient (7) without being recorded or whether they can be stored and easily passed on to others (e.g., pictures on WhatsApp [13]).

All of these factors can have an impact on how people view and perceive data protection and informational privacy and how they practice data disclosure. The factors can be summarized in the following formula,[43] which can be used to capture any data disclosure context (see Fig. 79): Who (7) wants to collect what kind of data (4) in which cultural (2), legal (9), and media context (10) from whom (1)—under which circumstances (necessity or free choice) (3), with which past experiences (5), and which concerns (6)—in what form (14), in which way (11), when (12), where (13), for what purpose (8), and with what effect (i.e., disclosure or non-disclosure)?

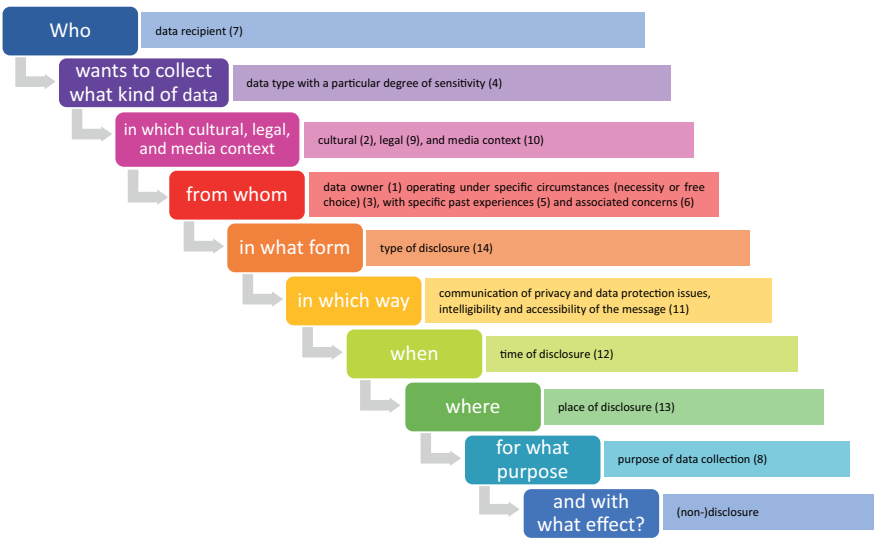

Fig. 79: Data disclosure formula.

43 The formula is based on Lasswell's (1964 [1948]) model of (mass) communication: "Who says what in which channel to whom with what effect?" (37). The numbers in brackets indicate the primary or key factor(s) for each part of the question.

It is important to note again that individual data disclosure behavior cannot generally be explained by any one of the factors cited above (1–14) alone. Nor do all factors have the same impact in all data disclosure situations. The specific, individual data disclosure situation determines which of the factors come into play at all, which ones become particularly relevant, and with what force (if any) they influence a data owner's disclosure behavior.

Continuing to investigate these influencing factors and their interconnectedness is a worthwhile endeavor. We have seen that the factors that can influence data disclosure range from daily events to historical imprints that shape cultural (privacy) values and norms (see DDM [2]). As the latter are more difficult to grasp, we would like to dedicate the following chapter to them.

3 Cultural privacy orientations

3.1 Introduction

In this part of our exploration, we will primarily be taking a closer look at the sociocultural values and norms that underlie data protection, information privacy, and data disclosure and the historical influences that have shaped them (see V.2, DDM [2]). This will allow us to stay on the macro level of our analysis and to thereby identify the different cultural approaches to privacy that have led to different cultural concepts of privacy and variations in the value attributed to it. These specific "privacy mentalities" also have an influence on how control over personal data is regulated in a country, i.e., by privacy laws and regulations (V.2, DDM [9]), how strong basic trust or mistrust tends to be vis-à-vis specific institutions (V.2, DDM [7]) when it comes to sharing personal data, and who has the most data power. They thus have a fundamental influence on above all data protection and privacy legislation (macro level) as well as institutional practices (meso level) in this regard. Looking into culturally specific concepts of and approaches to privacy opens up further, extensive prospects for future research projects. We can only sketch selected aspects for the countries we have surveyed here.

The focus in this chapter is to make the historical influences on cultural privacy mentalities more tangible and to discuss their potential to help explain our survey findings. Basic privacy orientations are part of the broader cultural context of data disclosure and can help to explain the different assessments of and approaches to informational privacy, data protection, and data disclosure that are reflected in aggregated survey data. In the course of our study, research on basic cultural privacy norms and values proved to be more substantial for some of the countries we studied than for others. Therefore, we have selectively included other particularly rele-

vant factors of our Data Disclosure Model for the latter countries (see V.2) to help explain survey results.

China and Japan have repeatedly attracted our attention, with survey results that deviate significantly from those of the other countries (see IV). We will therefore start with a discussion of their basic approaches to privacy in more detail in the following sections (V.3.2 and V.3.3), before turning to Brazilian, Ghanaian, Swiss, German, and US privacy mentalities (V.3.4–3.8). It should be kept in mind that we are mainly attempting to capture cultural privacy values and norms (V.2, DDM [2]), or "privacy orientations," on a macro level here (see also Wawra 2022).

3.2 China

China stands out among the countries we investigated, first of all, because the Chinese legal system bears scant resemblance to the principle of the *rule of law* in liberal democracies (Oud 2023) that is characteristic of the other six countries in our research sample. According to the United Nations (cited in Oud 2023), the *rule of law* constitutes

> a principle of governance in which all persons, institutions and entities, public and private, including the State itself, are accountable to laws that are publicly promulgated, equally enforced and independently adjudicated, and which are consistent with international human rights norms and standards.

Thus, within a rule of law system,

> laws provide meaningful restraints on state power … , every person is subject to the law and no one is above it. In liberal democracies, the rule of law is associated with civil and political rights and implies a separation of powers. (Oud 2023)

In contrast to this, the Chinese Communist Party (CCP) understands the *rule of law* as "'law-based governance' or ruling the country in accordance with the law" (*fazhi* or *yifazhiguo* in Chinese) (Oud 2023). That is, the law operates under the guidance and oversight of the CCP, which regards it as an instrument for upholding "stability and order" and for legitimizing and sustaining governance by the CCP (Oud 2023). This specific Chinese approach has also been characterized as "rule by law" (see, e.g., Van Norman Law 2017; Kempken 2021; Chin 2023). While the basic idea of the *rule of law* is that all people, including the rulers or members of government of a country, are equal before and subject to the law (see above and, e.g., Van Norman Law 2017), *rule by law* "sees the governing authority as somehow being above the law, and has [*sic*] the power to create and execute law where they find it to be convenient …" (Van Norman Law 2017). As such, governments and other authorities use

this strategy to influence the conduct of individuals as well as large segments of the population within a country, typically with the aim of convincing individuals (either on a psychological level or coercively) to support controversial political choices (see Van Norman Law 2017). We see *rule by law* in practice in China, "where courts, police and prosecutors are controlled by the Communist Party and where the constitution—which guarantees freedom of speech and religion, among other liberties—has been shunted aside when it conflicts with party interests" (Chin 2023). In accordance with this, China has been characterized as having "[e]xtractive political institutions," i.e., "power [is concentrated] in the hands of a narrow elite and … few constraints [are placed] on the exercise of this power" (Acemoglu & Robinson 2012, 95). It has also been described as a "single-party authoritarian state" (Zapletal & Barter 2021). China's omnipotent Communist Party "controls the entire state bureaucracy, the armed forces, the media, and large parts of the economy," with citizens' political liberty and involvement in political decision-making rather limited (Acemoglu & Robinson 2012, 487). In line with all of this, China's data policy has been characterized as "state-controlled" (Wang 2020, 662). In this regard, we have to distinguish between the state's approach to data protection vis-à-vis private actors on the one hand and the state on the other. China's approach is "state-controlled" in that, in the end, it is the state, i.e., the CCP (see above), that determines and controls data protection legislation and practice. While individuals' data are not protected against state intrusion, they are (better) secured against intrusion by other actors —foreign governments and companies (see Pernot-Leplay 2020, 107). The characterization of China's data policy as "state-controlled" is also consistent with Gao's (2023) categorization of the country as one that follows a "security paradigm" in terms of data regulation (708, 711). This implies that China puts national security first: Individual rights and commercial aspects are subordinate to bracing the state against threats from within and without (see Gao 2023, 722). Behind this lies a concern that the "legitimacy of the ruling regime" and the "country's political and social stability" are at risk (Gao 2023, 724). This approach is rather protectionist and critical of the free transnational flow of data (see Gao 2023, 727–728).

Further aspects that set China apart from the other countries we studied, and that are also relevant to help explain our survey findings, have already been discussed in detail in the context of our analyses of consumers' attitudes toward data protection and privacy issues (see Wawra 2023a, 190–192; 2023b, 59–61). We will therefore just briefly summarize some of these aspects here. First, China introduced "a digital sociotechnical credit system that rewards and sanctions the economic and social behaviors of individuals and companies" (Chen &, Grossklags 2022), which has been characterized as "the most ambitious experiment in digital social control ever undertaken" (Bartsch & Gottske 2018). Such social credit scoring systems (SCS) pose the risk of "large-scale systematic violations of privacy and human rights" (Kissel-

burgh & Beever 2022, 412). This can readily be observed in the Chinese context: The Chinese SCS evaluates citizens' "trustworthiness" based on various types of information (e.g., medical, financial, and insurance data but also information gathered through video surveillance in public spaces) in the form of a score and applies penalties accordingly. These penalties include prohibiting citizens from working in government and public organizations, travel restrictions, excluding children from private educational institutions, and publicly releasing citizens' scores online (Kisselburgh & Beever 2022, 412). In other words, "the stakes of large-scale state surveillance include significant loss of freedoms of movement, employment, education, and reputation …" (Kisselburgh & Beever 2022, 412). Chinese citizens can gain credits in this system by, for example, "[p]raising the government on social media" (Bartsch & Gottske 2018). In addition, China comes last on the Internet Privacy Index,[44] which reflects its lack of measures to safeguard citizen's online privacy.

Furthermore, Chinese culture has been characterized as

- a society in which people are "less protective of [their own as well as other's] personal space and privacy" than people from other cultures (Scroope & Evason 2017);
- being quite accepting of "quite loud public demeanours," which are common and may include publicly displaying one's feelings, conversing within proximity of others close enough for them to hear, singing, or dancing without concern for people nearby (Scroope & Evason 2017);
- still being influenced by Confucianism, which "promotes the acceptance of hierarchies, which are seen as natural and necessary" (Wawra 2023b, 60; drawing on Scroope & Evason 2017) for "harmonious, stable relations between individuals and … society," i.e., *li*, "social cohesiveness" (Scroope & Evason 2017). Confucianism thus teaches "respect [for] the law and authority" and the maintenance of harmony in society, for which "national unity and cooperation" are regarded as crucial in the Chinese cultural context (Scroope & Evason 2017).

In addition, we have to consider the possibility that Chinese respondents may have (preemptively) self-censored their answers, as China is characterized by censorship and restrictions on free speech (see Grant 2020; Zhicheng 2018). Indeed, "[i]nformation posted by [Chinese] citizens can be censored or blocked. Major offenses result in arrests" (Grant 2020). What is more, "… in contrast to the other countries, surveillance measures by the government are particularly common and elaborated in China, and the Chinese are used to them and have no other option than to accept them"

44 "A high privacy score means the country takes steps to protect information shared online. The higher the score, the more protected the information" (Grant 2020).

(Wawra 2023, 59). Consequently, Chinese respondents' answers might not always reflect what they really think for fear of negative consequences (see Wawra 2022, 191–192)—not least because of the SCS (see above), which discourages citizens from criticizing their government.

All of these factors can help explain China's status as a high-satisfaction country regarding the regulation of data protection and informational privacy in our survey (see IV.3.1), and why Chinese professionals

- agreed to a significantly greater degree than respondents from all other countries that consumers in their country can *always* make self-determined decisions about the disclosure of their personal data (see IV.2.1);
- agreed significantly less than respondents from most other countries with the proposition that consumers should be able to decide for themselves about the disclosure of their personal data (see IV.2.1);
- expressed the highest trust in most institutions we included in our survey (industries as well as domestic and foreign governments) regarding the correct use of consumer data (see IV.3.3.1) as well as exceptionally high trust in their own government (significantly more than respondents in all other countries except the United States).

China's privacy profile is also relevant in order to better understand its outstanding aggregated rating (across all industries surveyed) and consequential categorization as a country with high trust, high perceived compliance, high perceived enforcement,[45] and high satisfaction with regard to the level of consumer data protection provided (see IV.3.3.1–4). Another relevant factor in this respect is the Chinese legal context, for "Chinese law provides for extensive means of [data] protection in the private sector. In fact, China provides for the highest assured and overall level of privacy protection in this ranking" (Sonnenberg 2024, 77). Moreover, along with the United States, "China provide[s] for the most intensive/intrusive enforcement system [of the seven countries we investigated], both when it comes to theoretical possibilities and actual activities of enforcement" (Sonnenberg 2024, 76).

China's privacy profile also helps to explain why Chinese professionals evaluated the overall impact of their country's data protection and informational privacy regulations rather favorably (see IV.3.4.3), as they did the impact of regulation on companies (see IV.3.4.1), the professional handling of data by companies (see IV.3.4.2), consumers' ability to easily manage their privacy needs (see IV.3.4.2), individuals' fundamental rights, and digitalization (see IV.3.4.3). Chinese professionals,

45 With regard to all three types of consumer data protection enforcement surveyed, i.e., government enforcement, corporate enforcement, and enforcement by private parties.

however, evaluated its impact more critically in terms of consumer information overload as well as bureaucracy for the state, companies, and consumers, which a majority deemed excessive. Regarding bureaucracy for companies and information overload for consumers, Chinese respondents were significantly more critical than professionals from most other countries. A reason for their generally negative evaluations of bureaucracy and information overload could be a fatalistic attitude: Respondents may have been aware that individuals' informational privacy was not held in high regard in their country and that personal data would be collected, processed, and analyzed by the government no matter what the regulations said (see the discussion of China's *rule by law* above). Bureaucracy relating to data and privacy is therefore just cosmetic and does not really contribute to consumers' privacy protection. It merely causes additional work and processing overload for consumers but is of no benefit.

Another, related, East Asian conception of privacy that differs greatly from Western approaches is the Japanese one, which we will discuss in the following section.

3.3 Japan

Japanese culture has been characterized as "pragmatic" (Scroope 2021), and it seems that this mindset also extends to the Japanese approach to privacy (see Wawra 2023a), with concerns about privacy rights having generally been low in the country (see Orito & Murata 2005; Hiramatsu 1993). This is also reflected in the Japanese language: Privacy has often been said to be "a foreign concept to the Japanese" (Cullen 2008, 2) and an import from the West. Japanese does not have a word for privacy with exactly the same meaning as the English word; *puraibashi* has been imported as a loan word, but for the Japanese it often has other implications than for Westerners, such as the ability to "arbitrarily reject interference by others" (Orito & Murata 2005).

It has been argued that "there are related concepts of 'secret,' and 'forbidden' matters in the Japanese language, but that the concept of privacy itself is different in the Japanese tradition" (Cullen 2008, 2; summarizing Mizutani et al. 2004). Miyashita (2009) describes "the Japanese culture of privacy as 'privacy effected by the public'" (278). He continues:

> One famous motto of Japanese culture is "devoting oneself to the public, sacrificing one's private interests" (*messhi-hoko*). We have a long tradition of sacrificing private interests for the public good. For example, there is the history of *Bushi-do* (the Way of the Warrior), under which samurai fight not for their own interest, but for that of the Shogun (General), the head of the community. "Devoting oneself to the public, sacrificing one's private interests" is thus a virtue in Japanese culture. (Miyashita 2009, 278)

Thus, in Japan, what is considered "private" and "public" has been dictated by a communitarian culture (Miyashita 2009, 278). "[G]roup mentality" is important, and there is a widespread view that "a well-rounded character is attained by learning to be cooperative with others" (Orito & Murata 2005). Buddhism has been described as very influential in this regard as well in that it teaches the individual to subordinate themselves to the collective (see Cullen 2008, 2). Rice agriculture has also been cited as a factor with some impact, as "growing rice requires a collective decision-making process" (Orito & Murata 2005; Hayashi 1984).

Traditionally, the Japanese have lived in "close proximity to family and neighbours," which has led to a culture of politely ignoring what has been "observed or overheard inadvertently" (Cullen 2008, 2) and "self-imposed restraint in relation to the privacy of others" (Cullen 2008, 3). Consequently, one could argue that privacy regulations have not been regarded as something deserving of immediate attention (see Cullen 2008, 3; Mizutani et al. 2004). Another important aspect of traditional Japanese culture is that "harmony and trusted human relations" are seen as being in opposition to "privacy and individualism," and the public is seen as an "open, impartial" domain that stands in contrast to "the partial, secret, selfish domain" (Cullen 2008, 3; Nakada & Tamura 2005). Privacy can therefore evoke rather negative connotations in Japanese society. Orito & Murata summarize the impact of this privacy orientation on a fundamental Japanese data disclosure mentality as follows:

> [I]nsistence on the right to privacy as "the right to be let alone" indicates a lack of cooperativeness as well as an inability to communicate with others. The right to privacy, understood as "the individual's right to control the circulation of information concerning him or her," is considered a shameful excess of mistrust in relation both to cooperative society and to those who collect, store, share, and use personal data. Consequently, the sense of a right to privacy is foreign and less important to Japanese society than it is in Western societies. (Orito & Murata 2005)

Orito & Murata (2005) draw the following conclusions:

- In Japan, the safeguarding of privacy appears to operate only at the surface level;
- the socio-cultural context in Japan is not conducive to the adoption of initiatives aimed at safeguarding privacy and personal information; and
- the probability of Japanese attitudes toward safeguarding privacy and personal data aligning with Western standards is low.
- Hence, one cannot assert that the perception of privacy as a fundamental right is held globally.

This basic privacy orientation can explain why the preferred modus operandi of the Japanese government has been described as "self-regulation in relation to information and data privacy" (Cullen 2008, 3). The government tends to refrain from issuing

privacy and data protection regulations (if it is not more or less forced to do so due to international pressure), leaving it to the market instead. Today, Japan "emphasizes the importance of data as an economic commodity and protects a narrower range of personal information" (Wang 2020, 669). In the Japanese Constitution, there are no "explicit references to the right of privacy or data protection" (Wang 2020, 669), and the APPI, Japan's "most significant … data privacy legislation" (Wang 2020, 669) "places more significant emphasis on the economic salience of data than the EU" (Wang 2020, 670). Wang quotes from an interview with Murata, who says that Japanese law is "not for privacy, but pro-economy," concluding that "Japan primarily views privacy as a commodity for business opportunities" (Murata 2019; as cited in Wang 2020, 670). Unsurprisingly, these views clash with the European conceptualization of privacy (see V.3.7), which is why, rather than importing the GDPR in accordance with the so-called "Brussel's effect" (see V.3.6), Japan has taken a "cooperative data privacy" approach regarding the EU (Wang 2020, 662). The latter "provides a precedent for parties seeking to benefit from the economic salience of data flows, but are concerned about the societal and cultural implications of the Brussels Effect" (Wang 2020, 689). In other words, it allows Japan to be classified as a country with an adequate level of data protection from the EU's point of view without compromising its own cultural values regarding data protection and informational privacy.

The aspects mentioned above can help explain why, in our survey, Japan and China were the only countries where the majority did not *strongly* agree that consumers should be able to make self-determined decisions about the disclosure of their personal data. In addition, Japan had the lowest percentage of respondents (79 %) altogether who agreed (strongly or somewhat) that consumers should have autonomy over their data disclosure decisions (followed by Switzerland at 92 % [!]). In addition, the number of neutral answers (18 %) was exceptionally high in Japan in comparison to the other countries (see IV.3.1). Accordingly, Japanese respondents' agreement with the statement was significantly lower than in most countries surveyed.

This cultural privacy orientation also offers an explanation for the survey finding that Japanese professionals' mean sensitivity ratings were overall comparatively low and significantly lower than for most other countries (the United States, China, Germany, and Switzerland) (see IV.3.2). It also helps explain why Japanese law defines the fewest data categories as sensitive compared to the other countries (see IV.3.2 and Wawra 2023a, 180). Japan's pragmatic privacy mentality is also reflected in consumers' awareness of their country's data protection and privacy rules: Comparing the results for Brazil, China, Germany, Japan, Russia, and the United States, Japan ranks last, with only 16 % reporting they were very or somewhat aware of the rules (CIGI-Ipsos 2019b, 281; Wawra 2023, 187). This underlines the lower importance the Japanese place on privacy regulation. The noticeably high frequency with which substantial percentages of professional respondents gave neu-

tral answers in our survey on data protection and informational privacy issues also seems to reflect this pragmatic Japanese approach to privacy regulation (see III.4).

Japanese data protection professionals seemed to be at least partly (self-)aware of this "laissez-faire" approach to privacy in their country, as they assessed legislation in Japan as significantly less sufficient to guarantee consumers' data autonomy than respondents in almost all other countries did (see IV.3.1). Similarly, they agreed significantly less than professionals in almost all other countries that data protection and informational privacy regulation enables consumers to easily manage their privacy needs (see IV.3.4.2) and considered it the least and significantly less sufficient to protect the fundamental rights of individuals than respondents from all other countries (see IV.3.4.3). However, overall, they did not see any deficits in the data autonomy of Japanese consumers, and Japan occupied the midfield of countries regarding the perceived necessity of making adjustments to current data protection and informational privacy regulations, even leaning more toward the high-satisfaction countries in this regard (see IV.3.1). Thus, there seems to be some awareness that Japan regulates consumers' data autonomy less than other countries, though this is not necessarily seen as something that needs to be changed by professionals. This is in accordance with the characteristically low Japanese concern for privacy matters outlined above. It is also reflected in Japanese professionals' rather impartial stance toward the overall impact of their country's data protection and informational privacy regulations, which the majority assessed as *neutral*. Most respondents gave the same assessment of the impact of Japanese regulation on digital development and the implementation of digital innovations. It is noteworthy, however, that these assessments were the least positive in cross-cultural comparison and were significantly less positive than those given by most other countries (see IV.3.4.3).

In accordance with this supposed awareness of the pragmatic Japanese approach to privacy, Japanese professionals also assessed the measures adopted by consumers to protect their data as significantly less sufficient than the professionals in *all* other countries did (see IV.3.1). Interestingly, however, a majority considered Japanese consumers to be (very or rather) aware of data protection and informational privacy regulations (see IV.3.1). Having said that, Japanese professionals may have overestimated consumers' data protection literacy in this respect, for Japanese consumers' self-assessments in this regard were considerably less positive: A vast majority reported that they were not very or at all aware of these regulations (CIGI-Ipsos 2019b, 281; Wawra 2023a, 187). This is more in line with the pragmatic approach to privacy mentioned above.

Japanese professionals' awareness of their culture's pragmatic approach to privacy was also reflected in their (rather critical) assessments of

– the level of consumer data protection (in which respect Japan is a low-satisfaction country; see IV.3.3.4);

- corporate compliance with the regulation of consumer data protection and informational privacy (in which respect Japan is a country with low perceived compliance; see IV.3.3.2); and
- the corporate handling of consumer data (in which respect Japan is a low-trust country) and the government handling of consumer data in Japan (see IV.3.3.1);

as well as their rather neutral assessments of the overall impact of the regulation of data protection and informational privacy in their country (see IV.3.4.3).

The results of our survey of how Japanese professionals assess the impact of their country's regulation of data protection and information privacy on bureaucracy is also in line with Japan's pragmatic approach to privacy. Japanese professionals agreed least that regulation overloads consumers with information (significantly less so than respondents from three other countries) and that it causes too much bureaucracy for the state, companies, and consumers. Regarding bureaucracy for consumers, they held this opinion to a significantly lower degree than professionals from most other countries (see IV.3.4.2). However, when considering information obligations for data handlers, the aspects of the legal context that are probably most closely related to perceptions of the information overload and bureaucracy associated with data protection, Japan ranks in the middle of the seven countries surveyed rather than at the bottom (see Sonnenberg 2024). In other words, the level of bureaucracy associated with informational privacy protection in Japan is likely rather moderate and not significantly less than in most other countries.

It is more difficult to explain why Japanese professionals assessed the impact of their country's data protection and informational privacy regulations on companies as significantly less positive than respondents from other countries regarding customer orientation, innovation, and national as well as international cooperation, with many taking a neutral stance in this respect (see IV.3.4.1). The high number of neutral answers is in line with the Japanese culture's pragmatic approach to privacy. If, however, Japanese privacy law is indeed, as stated above, "not for privacy, but pro-economy" (Murata 2019; as cited in Wang 2020, 670), one would expect a more positive assessment of Japan's regulations in this regard. By contrast, the finding that Japanese professionals agree the least and significantly less than respondents from most other countries that regulation in their country has led to companies handling data more professionally supports the idea that Japan follows a pro-economy privacy approach (see IV.3.4.2).

Finally, let us turn to the enforcement of data regulation in Japan. In contrast to the European approach to enforcement (see V.3.7), the Japanese approach relies on "soft power," i.e., "reputation." The "fear of violating social norms" and thereby losing "social trust and business reputation" is particularly strong in Japan (Miyashita 2011, 233; as cited in Wang 2020, 679). Therefore, "reputational value serves as an im-

portant enforcement mechanism … , particularly for data breaches" (Wang 2020, 679). This has been attributed to "shame culture" (Fujiwara 2019) and a "culture of apology" (Miyashita 2009, 279). Both accentuate "the significance of community reputation in Japan" (Wang 2020, 681; Fujiwara 2019):

> [W]hen a business leaks a large amount of personal information, the harm suffered is not the loss of control of personal information, but rather the disruption in its relationship with customers and the community. … [B]usinesses which have leaked customers' information tend to apologize in advertisements placed in newspapers, and they are often willing to compensate without court orders. (Miyashita 2009, 279)

This cultural background is reflected in professionals' assessments of the enforcement of data protection and informational privacy in their country. Japan is a country with low perceived government enforcement, low perceived corporate enforcement, and also low perceived enforcement by private parties (see IV.3.3.3). This is in accordance with the Japanese tendency to rely more on "soft" than on "hard power" (i.e., legal punishment; see V.3.7).

Having explored the privacy values and norms in the two Asian countries in our sample, we will now turn to South America and take a look at some typical aspects of Brazilian culture that could have explanatory potential for the results of our survey.

3.4 Brazil

Our findings regarding Brazilian respondents were rather ambivalent: While they expressed dissatisfaction with certain aspects of how informational privacy is safeguarded in their country, they assessed others quite positively. For example, while their assessments of consumers' ability to always make self-determined decisions about personal data disclosure were relatively negative in cross-cultural comparison (see IV.2.1), they were generally quite trusting regarding the corporate handling of personal data, with Brazil qualifying as a high-trust country in this respect (see IV.3.3.1). In the following, we will first discuss selected aspects of Brazilian culture, in particular Brazilian legal culture, before discussing how those aspects may help explain some of our findings.

One cultural concept that is particularly relevant to our discussion of findings and the Brazilian legal context is *jeitinho,* which is a widespread "problem-solving strategy" in Brazilian culture (Ferreira et al. 2012, 321). It constitutes a "special way to solve a problem or a difficult or prohibited situation … [that involves] finding a creative solution for dealing with situations, whether in the form of conciliation, cunningness, or skill" (Barbosa 2006, 41; as cited in Akira Miura et al. 2019, 1). Exam-

ples include jumping a long queue by spotting a friend and asking to join them or getting out of a traffic ticket by bribing a police officer (see Ferreira et al. 2012). Ferreira et al. (2012) identify three key factors in *jeitinho*: "Corruption, Creativity, and Social Norm Breaking" (335). Similarly, Pilati Rodrigues et al. (2011) identify seven central facets of *jeitinho*, namely "sympathy, harm to others, malandragem, disregard for social rules, innovative processes, power relation, and compensation" (32).[46] The rule and norm-breaking component of the construct raises the question of *jeitinho*'s relationship with the Brazilian legal context. Zimmermann (2009) discusses *jeito*[47] (i.e., *jeitinho*) as one aspect of the substantial divide between law in books and law in action (see V.2) in Brazil, which can be traced back to the country's significant legalism. As Rosenn observes,

> [t]he Brazilian legal culture is highly legalistic; that is, the society places great emphasis upon seeing that all social relations are regulated by comprehensive legislation. There is a strong feeling that new institutions or practices ought not be adopted without a prior law authorizing them. … Brazil has reams of laws and decrees regulating with great specificity seemingly every aspect of Brazilian life, as well as some aspects of life not found in Brazil. It often appears that if something is not prohibited by law, it must be obligatory. (Rosenn 1971, 528)

This has resulted in "a superabundance of regulatory legislation" as well as a lack of regulatory adaptability in Brazil, which contributes to *jeito*; the latter can be understood as "a legalistic response" to these issues (Rosenn 1971, 529). Alongside legalism, another aspect of Brazilian legal culture conducive to *jeitinho* is its excessive formalism (see Rosenn 1971; Duarte 2006). Research has shown that *jeitinho* is used in Brazil to navigate bureaucratic inefficiencies (see Duarte 2006; see also Ferreira et al. 2012). Using *jeitinho* in response to unreasonable legislation or the "absurdities of bureaucracy" is well accepted in Brazil, with "the bypassing of legal norms ha[ving] become more the rule rather than the exception" (Zimmermann 2009, 22–23). In fact, *jeitinho* is so widespread that Brazilians consider it an integral component of their cultural identity (see Duarte 2005; as cited in Zimmermann 2009, 22), which is reflected in the saying "o pais do jeitinho," or "the land of jeitinho" (Barbosa 2006; as cited in Ferreira et al. 2012, 331).

Let us now contextualize our findings in the light of these considerations. According to our analysis, Brazil qualifies as a low-satisfaction country regarding the current regulation of data protection and informational privacy, with a majority of respondents advocating to increase the regulation of data protection and informa-

46 *Malangdragem* can be translated as "deception or trickery" (Porto & Pilati 2021, 22).

47 The diminuitive *jeitinho* derives from this word, which translates as "skill," "talent," "style," or "way" (Cambridge Dictionary 2024). *Jeito* is used by some authors in a similar sense as *jeitinho* (see also Pilati Rodrigues et al. 2011).

tional privacy for certain data types, contexts of data disclosure, purposes of data collection, and industries (see IV.3.1). This seems surprising given that the regulatory intensity of Brazil's data protection law (Lei Geral de Proteção de Dados Pessoais, LGPD) is similarly high to that of the EU's GDPR (see Sonnenberg 2024, 78). However, this finding may be due to the highly legalistic character of Brazilian legal culture. As noted above, there is a strong expectation of comprehensive legislation in Brazil, which explains why the Brazilian professionals in our survey tended to advocate to intensify their country's data protection and informational privacy regulations even further. This also explains why they exhibited particularly strong agreement with statements regarding the regulation of data handling by companies (see the cross-cultural blueprints for good data processing practice in IV.2.2).

Another remarkable finding was that Brazil qualified as a country with high perceived corporate compliance with the regulation of consumer data protection and informational privacy (see IV.3.3.2). This finding is surprising given the ubiquity of *jeitinho* in Brazil, which might prompt the expectation that actual compliance would be rather low. However, this could be explained by how we framed the relevant question in our survey: Respondents were not asked whether compliance was high or low in certain industries; rather, they were asked to indicate whether they thought compliance was sufficient or insufficient. It is possible that, given the widespread acceptance of *jeitinho* in Brazil, respondents expect and accept limited compliance with data protection and informational privacy regulations (especially given that they typically engender a substantial amount of bureaucracy) and thus regard compliance as *sufficient*. Extensive regulation and the acceptance of *jeitinho* may also explain why Brazilian respondents were generally satisfied with the level of consumer data protection in various industries, with Brazil qualifying as a high-satisfaction country in this regard (see IV.3.3.4).

Furthermore, *jeitinho* can be cited as a key factor for why, despite Brazil's intense regulatory scheme, Brazilian respondents had comparatively positive assessments of the impact of Brazilian data protection and privacy regulations on companies' ability to innovate, cooperate with other companies, and tailor products and services to consumers' needs (see III.4.1 and IV.3.4.1). Evidently, existing regulations were not regarded as too restrictive, as *jeitinho* creates additional leeway in the Brazilian legal system.

Despite Brazilians' awareness and acceptance that people in their country bend legal rules, they seem to have at least some confidence in the overall effectiveness of their legal system, for

> they have … inherited, via Portugal, the … belief or hope that positive laws can eventually function as panaceas for every sort of social disease. This hope maintains that one day everybody will suddenly start respecting the existing laws, and when the "miracle" suddenly happens,

> these laws will finally solve all the country's social problems. (Zimmermann 2009, 17; drawing on Rosenn 1998, 54)

This "faith" in or hope for the (eventual) effectiveness of the legal system might explain why Brazilian respondents in our survey still believed (to a comparatively strong degree) that regulation in their country had improved corporate data handling (IV.3.4.2), why they assessed its overall impact and its impact on digitalization rather positively (in cross-cultural comparison as well; see IV.3.4.3), and why their assessments of its sufficiency to protect the fundamental rights of individuals was also rather positive (see III.4.3 and IV.3.4.3). By contrast, their assessments of consumers' ability to *always* make self-determined decisions about personal data disclosure was rather negative both in cross-cultural comparison and in absolute terms (see IV.2.1), indicating that this issue remains an area with room for improvement in Brazil.

Although Brazilians seem to retain faith in their legal system despite *jeitinho*, it has been argued that the phenomenon negatively affects Brazilians' trust in both other people and institutions. As pointed out by Porto & Pilati (2021), "Brazilians tend to have a distrust bias, perceiving their co-citizens as advantage-takers who use deception and cunningness strategies and break social norms to obtain personal gains" (25). This bias is evident in the results of the World Value Survey, which found that Brazilians largely distrust other people and exhibit relatively low trust in various institutions such as the police, the government, and political parties (see Porto & Pilati 2021; Wawra et al. 2022d). According to Porto & Pilati (2021), the tendency to distrust is encouraged by the prevalence of scam tactics in Brazil, which illustrate the *malandragem* aspect of *jeitinho*. Furthermore, corruption scandals occur frequently, and rule-breaking organizations are infrequently penalized, resulting in great personal tragedies (e.g., the Brumadinho dam disaster in 2019), while governmental and non-governmental organizations fall short in fulfilling their commitments to the public (see Porto & Pilati 2021, 28). The Brazilian media regularly report on such fraudulent behavior (see Porto & Pilati 2021, 28), which is therefore very present in the consciousness of the Brazilian public (see also V.2 [9]).

It is therefore rather surprising that, according to our survey data, Brazil qualifies as a high-trust country regarding the corporate use of personal data. This reflects the professional perspective and stands in contrast to findings for consumers (see IV.3.3.1; Wawra et al. 2022d), which are in line with the distrust bias described above. It is difficult to explain why our findings regarding professionals differ from consumers' perceptions (and the general sentiment of distrust in Brazilian culture) in this regard. One possible explanation could be that, because they have an insider perspective on how companies or other institutions process consumer data, professionals may be less susceptible to the influence of negative media coverage, which possibly contributes to consumers' suspicions regarding corporate data handling.

Another noticeable finding in the present study is that private enforcement was rated as comparatively strong in Brazil, which means that it can be classified as a country with high perceived enforcement in this respect (see IV.3.3.3). This is in line with Sonnenberg's (2024) assessment of private enforcement in the Brazilian context, which he links to Brazilians' litigiousness (70–71).[48]

In the following section, we will take a closer look at Ghana's basic privacy orientation.

3.5 Ghana

According to The Culture Factor Group (2024),[49] Ghana can be classified as a collectivist culture, which is in line with the philosophy of *Ubuntu*, a worldview prevalent throughout Africa (see, e.g., Adjei et al. 2024; Kamwangamalu 1999; Olinger et al. 2007). One key principle of *Ubuntu* is "communalism," that is, "the interest of the individual is subordinate to that of the group" (Kamwangamalu 1999, 27). The Akans, Ghana's largest ethnic group, which make up almost half the country's population (Ghana Statistical Service 2022, 30), capture this worldview using the term "*biakoyɛ* (unity is strength) or wo yɔnko da ne wo da (i.e., what affects one affects all)" (Adjei et al. 2024, 165). The central virtues of the latter are "universal vulnerability and collective responsibility" (Adjei et al. 2024, 165).

How do these cultural values relate to people's privacy orientations? According to Hofstede et al. (2010, 126), while "[t]he right to privacy is a central theme in many individualist societies," such as Germany or Switzerland (The Culture Factor Group 2024), it "does not find the same sympathy in collectivist societies, where it is seen as normal and right that one's in-group can at any time invade one's private life" (Hofstede et al. 2010, 126). As the most collectivistic culture of all the seven countries that we surveyed (The Culture Factor Group 2024), and considering the prevalence of the Ubuntu worldview in Ghana, there could be an expectation that Ghanaian respondents would show less interest in privacy than the others (see also Agyei-Bekoe 2013). This, however, is not what we found in the present study: Just like in all the other countries, the vast majority of Ghanaian professionals advocated for consumer data autonomy (see IV.2.1). Moreover, the cross-cultural blueprints for good corporate data processing practice (see IV.2.2) were found to be particularly impor-

48 Sonnenberg (2024, 70) cites Armour & Schmidt (2017, 5), Takahashi (2019, 94 et seq.), and Deffenti (n.d.) in this regard.

49 The Culture Factor Group is a consultancy specializing in cultural analytics and strategy. It was established in 1985 with the help of Prof. Geert Hofstede, a pioneer in the field of comparative cultural studies, and draws heavily on his work and related research.

tant to Ghanaian (alongside Brazilian) professionals. Ghanaian professionals also stood out (alongside their Japanese colleagues) when it came to assessing the sufficiency of their country's legislation to guarantee consumers' data autonomy, which only a minority regarded as *sufficient* or *rather sufficient* (with many taking a neutral stance), resulting in a rather low rating in cross-cultural comparison. We also found that Ghana leaned more toward the low-satisfaction countries regarding the current regulation of data protection and informational privacy. Thus, in the present survey, Ghanaian professionals' concerns about data protection and informational privacy were by no means lower than in the other countries—quite the contrary. In addition, they were not entirely satisfied with the extent of the current regulation of data protection and informational privacy in their country.

If not on the basis of collectivism, how can these findings be explained? One possible explanation is that Western notions of privacy and their connection to the individualism/collectivism dichotomy may not be apt to capture Ghanaians' understanding of privacy and the value they attribute to it. Thus, while the majority of Ghanaian regional languages (such as Twi, Ewe, and Ga) lack an exact equivalent for the notion of privacy (Elul 2022, 49), Twi, for example, has several words for privacy-related concepts, such as *Asisɛm* (*secret*, literally *hidden information*, which is used for "any occurrence or information that should not be disclosed publicly" [Elul 2022, 50]) and *Ahintasem*, which is connected to "privacy or discreteness as a social expectation" (Elul 2022, 50), signifying that one should keep something to oneself rather than uttering it aloud (see Elul 2022, 50). Elul (2022) lists someone's home address, pregnancy status, or income as possible examples of *Ahintasem*, explaining that "it is culturally acceptable to hide (and even lie about) these details" (50). This shows that Ghanaian culture has its own notions of and expectations regarding what might be termed "privacy" in Western contexts that are linked to "politics of indirectness and discreteness within Ghana" (Elul 2022, 50), a frequently observed characteristic of Ghanaian culture (for an overview of scholarly work in this area, see Elul 2022, 25). Elul (2022) gives examples of how this indirectness is mirrored in local language use (48), concluding that it "is a lingual manifestation of privacy and its social virtues: it protects one's reputation, relieves collective tensions, and prevents confrontation or shame" (49). From this point of view, concerns about privacy are by no means absent from Ghanaian culture. Rather, it seems that privacy is conceptualized differently than in Western societies. In light of these considerations, our findings regarding Ghanaian professionals' concerns about data protection and informational privacy and their limited satisfaction with the extent of current regulations seem far less surprising.

Moreover, recent historical events and their presence in the Ghanaian media (see V.2, [9]) may provide an additional explanation for Ghanaian professionals' evident concerns about data protection. Ghana has a history of cybercrime (see Agyei-

Bekoe 2013) and has experienced a steady increase in its frequency in recent years.[50] The issue of cybersecurity has featured regularly in the Ghanaian media[51] and entered public awareness not least when cyberattacks on electricity companies in Ghana caused disruptions to the Ghanaian electricity supply for days in 2021 and 2022 (Positive Technologies 2023). Political action to combat this problem included the founding of the national Cyber Security Authority (CSA) in 2020 (see Ministry of Communications and Digitalisation, Ghana 2022) and the establishment of an annual National Cybersecurity Awareness Month in Ghana (Cyber Security Authority Ghana 2021; see also Essah 2018; Bonney 2023) to raise awareness among Ghanaians of cybersecurity issues. Efforts in this regard have also been made by the Ghanaian media (see, e.g., Adu 2023; Awiah 2017; Johnson 2023).

While such measures may eventually improve Ghanaians' data protection literacy, at least regarding the issue of cybersecurity, they are evidently still deemed necessary by the Ghanaian government and media, suggesting that data protection literacy in Ghana is still underdeveloped. This explains why the Ghanaian professionals in our survey assessed the general data protection literacy of consumers in their country as comparatively low (see IV.3.1). This stands in contrast to our finding that a majority of Ghanaian consumers believe that they are very or somewhat aware of the regulation of data protection and informational privacy in their country (Thir & Wawra 2023). It is possible that Ghanaian respondents may have been unaware of what knowledge they still lacked in this respect, thus overestimating their own data protection literacy. Another possible explanation lies in the nature of our sample (Thir & Wawra 2023): Most respondents (79 %) came from urban regions; however, the urban-rural ratio is far more even in the general Ghanaian population (57 % vs. 43 %; Ghana Statistical Service 2022, 4). It is possible that the urban Ghanaian population does indeed possess greater data protection literacy than the average Ghanaian population, leading to higher self-professed levels of data protection literacy in our survey.

Despite the Ghanaian government's efforts mentioned above, Ghana still qualified as a country with low perceived government enforcement in our survey (see IV.3.3.3). One might expect the enforcement of data protection and informational privacy regulations to be comparatively low in Ghana as the Ghanaian Data Protec-

50 Cybercrime increased in Ghana by about 480 % from 2016 (116 cases) to 2018 (558 cases; The Ghana Report 2019). In October 2019, the Cybercrime Incident Reporting Points of Contact (PoC) was launched in Ghana, and within a year, 11,550 cybercrime incidents had been recorded (Ghana Chamber of Telecommunications 2020; see also Ennin & Mensah 2019; 2022; Mensah 2023).

51 See several articles and opinion pieces published in the online version of *The Daily Graphic*, the most widely circulated Ghanaian daily newspaper (Kuehnhenrich, 2012): Adu (2023); Awiah (2017); Bruce (2022); Cephas (2023); Dotse (2023); Essah (2018); see also Johnson (2023) in *Modern Ghana*.

tion Commission is understaffed and adequate applicants are scarce (Hoffmann 2022, 19). Moreover, as noted by Hoffmann (2023), fines for non-compliant data processors in Ghana are rather low in international comparison. This could also be why most Ghanaian professionals overall said that the regulation of data protection and informational privacy had a neutral impact in their country (see IV.3.4.3).

In the following two sections, we will discuss the privacy orientations of the two European countries in our sample—first Switzerland (see V.3.6) and then Germany (see V.3.7).

3.6 Switzerland

Switzerland is a country that in many ways stands out among its European neighbors, first and foremost due to its politically "neutral" status. It is thus part of neither the EU nor the European Economic Area (EEA). According to Morris & White (2011), Switzerland's ongoing disinclination to join the EU goes back to "a historic identity that the Swiss perceive is threatened by membership in the EU" (104). Having experienced repeated threats to its sovereignty in past centuries and relying on the idea of neutrality as a unifying common ground among its linguistically diverse population, "the Swiss … fear losing their identity as a neutral nation, but also direct democracy and federalism, which are seen as uniquely Swiss institutions" by becoming an EU member state (Morris & White 2011, 107). Swiss skepticism toward the EU continues to this day, with only about 15 % of Swiss respondents in support of Switzerland joining the European Union in 2019 (according to an analysis by Smartvote, referred to in Watson 2022). Given these reservations toward "outside control," it is unsurprising that Swiss professionals in our survey stood out (alongside Japanese respondents) in terms of their comparatively low trust in foreign governments to use of consumer data correctly (see IV.3.3.1).

However, it is not immediately obvious why Switzerland qualifies as a low-trust country (see IV.3.3.1), a country with low perceived compliance with regard to informational privacy and data protection regulation (see IV.3.3.2), and a low-satisfaction country regarding the level of consumer data protection offered (see IV.3.3.4). Switzerland is a politically and economically very stable country, and is also perceived as such by its population: When asked to name three things that symbolize Switzerland, one-third of Swiss respondents (34 %) named security and stability (Credit Suisse 2022, 12), and an overwhelming majority of Swiss respondents trust Switzerland's political system (82 %) and legal system (87 %) (data collected in 2021; Federal Statistical Office 2023). Moreover, Bewes (2010) describes Switzerland as a very trusting culture (109–111), which is corroborated by a finding that a majority (59 %) believe that most people can be trusted (EVS/WVS 2022, 189). However, this level of

trust does not seem to extend to companies: 65 % of Swiss respondents reported having little or no confidence at all in major companies (EVS/WVS 2022, 289). Moreover, as regards data protection and informational privacy specifically, we found that the Swiss tend to place greater confidence in the national government than in the private sector (see Thir et al. 2023). All this is in line with our finding that data protection professionals tend to place limited trust in companies to handle consumer data correctly and are critical of their compliance with existing data protection and informational privacy regulations (with Switzerland thus qualifying as a low-trust country and a country with low perceived compliance). Swiss professionals' low satisfaction with the level of consumer data protection in place in their country, however, could be explained by the fact that our survey data was gathered just a few months before the revised data protection law in Switzerland came into force. This means that our respondents probably had the old data protection law in mind when filling in the survey. In contrast to the revised data protection law, the old law did not yet mention consumer protection (see Sonnenberg & Hoffmann 2022, 3). This may also explain why Swiss respondents agreed comparatively little with the statement that the regulation of data protection and informational privacy had led to companies handling data more professionally and enabled consumers to easily manage their privacy needs (see IV.3.4.2)

The data collection period (and the fact that Swiss respondents thus had the old rather than the new data protection law in mind) may also explain why they often assessed the consequences of data protection and informational privacy regulation comparatively negatively, for example, regarding both national and international cooperation among companies (see IV.3.4.1). The need to uphold "unhindered business relations between Switzerland and EU countries" is a central theme in debates surrounding data protection in Switzerland (Sonnenberg & Hoffmann 2022, 2 [emphasis omitted]). Consequently, data protection legislation in Switzerland has "been intricately linked to developments in the European Union" (Sonnenberg & Hoffmann 2022, 1). With the passing of the GDPR in the EU, Switzerland naturally experienced considerable pressure to adapt its data protection laws accordingly, which constitutes a prime example of what Bradford (2019) more generally terms the "Brussels effect" (Sonnenberg & Hoffmann 2022, 2; see also Hennemann 2021), i.e., "the EU commanding significant regulatory power beyond its borders" (Sonnenberg & Hoffmann 2022, 2). However, while the GDPR came into force in 2016 and has been applied since 2018 (European Commission n.d.), the revised Swiss Data Protection Act (Datenschutzgesetz, DSG) and the associated Data Protection Ordinance (Datenschutzverordnung, DSV) only took effect recently, in September 2023 (see Federal Assembly of the Swiss Confederation 2020; Swiss Federal Council 2022), that is, with considerable delay (considering that the DSG has been in development since 2017; see Sonnenberg & Hoffmann 2022, 1). Swiss respondents' negative assessments

of the data protection and informational privacy regulations in place in their country at the time of the survey may thus reflect the fact that they had not yet been updated to reflect the GDPR.

If the old regulation did truly hinder collaboration between companies, it will inevitably have had a detrimental impact on digital innovation and development as well. This might explain why Swiss professionals' assessments of the impact of data protection and informational privacy regulations on digital development and the implementation of digital innovation were rather neutral (as was their overall assessment) and comparatively negative. This could also be why they agreed significantly less than respondents in most other countries that the current regulation allowed for corporate innovation. Moreover, the delayed commencement of the new regulation may have created the impression among respondents that Switzerland was falling behind in terms of data protection legislation and thus opportunities for cooperation and innovation compared to other countries.

In contrast, Swiss professionals assessed the impact of Swiss data protection and informational privacy regulations on bureaucracy for the state, companies, and consumers comparatively positively (see IV.3.4.2). These favorable perceptions may likewise have been at least in part due to the data collection period, as the old data protection law in Switzerland imposed significantly fewer information obligations than the new legislation does (see Bühlmann & Reinle 2020), thus possibly keeping bureaucracy in check, at least compared to the new law. Moreover, it is possible that Swiss respondents may have unconsciously compared their own data protection law to the GDPR, which has also received media coverage in Switzerland due to its indirect (see above) and direct influence on Switzerland.[52] This media coverage has sometimes highlighted the bureaucracy-intensive character of the GDPR[53] (see also V.2, [9]). Consequently, Swiss respondents may have perceived their own data protection laws to be comparatively less burdensome when juxtaposed with the GDPR.

After this overview of the lesser-known privacy orientations in five of the countries that were part of our survey, we will now take a closer look at the rather well-researched general European, and specifically German, as well as US privacy norms and values.

---

52 The GDPR is applicable to the corporate handling of EU citizens' data in Switzerland.

53 See, e.g., an interview with Swiss legal expert Martin Steiger in Orizet (2019), where Steiger states that "until now, the GDPR has first and foremost not contributed to more data protection for the persons concerned but has caused more bureaucracy for all who process personal data" [our translation].

3.7 Germany (Europe)

Within the European cultural context, privacy has primarily been conceptualized as "an aspect of dignity" (Whitman 2004, 1161).[54] Within this concept, privacy is mainly related to "respect," "personal dignity," and to an individual's "rights to control [their] public image" (Whitman 2004, 1161 [emphasis omitted]). It has often been said that the European privacy focus on dignity is rooted in the European experience of fascism and, in particular, of Germany's Nazi past: "Having experienced the horrific indignities of the 1930s and 1940s, continental societies, Europeans say, have mended their ways. Europe has dignity today because Europe was traumatized seventy years ago" (Whitman 2004, 1165). Aden likewise emphasizes the influential role that Germany's history has played in this respect: "[D]ata protection has been of particular relevance in the German context—not only against the backdrop of rapidly evolving information technology, but also of the historical experiences with political regimes collecting information in order to oppress citizens" (Aden 2021, 119).

During the Nazi regime, the Gestapo (*Geheime Staatspolizei*, Secret State Police) collected information "about Jewish citizens, political opponents, and members of other groups targeted by racist prosecution" with the goal of intimidating, silencing, imprisoning and even murdering them (Aden 2021, 121). They mainly relied on the methods of surveillance and denunciation. During the Cold War, spying was also commonplace in the former German Democratic Republic (GDR) and in Soviet-dominated states in Eastern Europe, ensuring that citizens toed the line with party policies and did not pose any threat to the authoritarian regimes. In the GDR, the Stasi (*Ministerium für Staatssicherheit*, Ministry for State Security) monitored citizens, particularly those who were considered to be critical of the state (Aden 2021, 121).

These oppressive state surveillance systems were very effective at invading and annihilating people's privacy—even in the pre-digital era. It has been argued that these historical experiences of personal data abuse have increased German citizens' vigilance regarding their privacy vis-à-vis the state (see Aden 2021, 121; Freude & Freude 2016, 86). Recent surveys seem to confirm this: According to a representative survey of 1,065 respondents commissioned by the Max-Planck-Institute and the University of Bristol (Kozyreva et al. 2020, 4), Germans have serious concerns about data protection: 82 % of those surveyed reported being very or partly concerned about the protection of their data (Kozyreva 2020, 5). In a recent survey of 12,263 Europeans, considerably more German respondents (45 %) reported being

54 Whitman (2004) here draws conceptually on Post's (2001) concepts of privacy.

concerned about data protection in 2019, in light of advancing technological and digital developments, than the average across the 28 EU member states (36 %) (Osterwinter & Wortmann 2020, 3). This heightened concern is also reflected in German consumers' awareness of their country's data protection and privacy rules. Comparing survey results for Brazil, China, Germany, Japan, Russia, and the United States, Germany was the only country in which a majority (59 %) said that they were very or somewhat aware of these rules (CIGI-Ipsos 2019b, 281; Wawra 2023, 187).

The unforgettable historical lessons mentioned above, learned from Germany in particular but also from former Soviet-dominated states, have found their way into data regulation and data protection in European legislation. The view of privacy as a part of human dignity has led to the establishment of a European "privacy paradigm" that considers the protection of personal data to be a fundamental right (see Gao 2023, 718–719): "European legal sources tend to view control over personal data as an inherent aspect of individual dignity" (McGeveran 2016, 967; quoted after Wang 2020, 668). The Charter of Fundamental Rights of the European Union safeguards "privacy and data protection" (Rustad & Koenig 2019, 373; quoted after Wang 2020, 668), and "other European constitutional documents and treaties also name privacy as a crucial right" (Wang 2020, 668; see McGeveran 2016, 967; Rustad & Koenig 2019, 377).

Thus, within the European cultural context, the primary focus is not on ensuring the maximum exploitation of data for commercial purposes—as in the US trade paradigm (see V.3.8)—or on safeguarding the system of government—as in the Chinese security paradigm (see V.3.2)—but on protecting the rights of the individual. Wang (2020) comes to a similar conclusion when comparing the EU to Japan, stating that the "most significant difference between the EU approach and the Japanese approach to privacy is that the EU considers data protection and privacy to be fundamental rights, viewing those rights as a more dominant rationale for regulation than economic incentives" (668).

Our survey findings confirm Wang's observation: German professionals' assessments of the sufficiency of current data protection and privacy regulations to protect individuals' fundamental rights was significantly more positive than those of Japanese professionals (see IV.3.4.3). However, this was also true when comparing Japanese professionals' assessments with those of professionals in all other countries. Though a majority of German professionals considered current regulations to be *sufficient* or *rather sufficient* in this regard, their assessments were not significantly more positive than those of the respondents in the remaining countries (except for Japanese respondents' assessments; see III.4.3). This was despite the focus on individuals' fundamental rights in European privacy legislation, with the GDPR explicitly "protect[ing] fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data" (GDPR 2016, Art. 1[2]). This exemplifies how law in books may not always correspond to (perceptions of) law in action. One

explanation for this finding could be that respondents from different countries have different interpretations of what constitutes a data subject's fundamental rights, perhaps viewing them as less closely tied to privacy than in the European context, leading to more positive assessments in the other countries.

Former German chancellor Angela Merkel (The Economist 2018; as cited in Wang 2020, 662) describes the European approach to privacy as being in between the two opposing poles of China's "state-controlled" approach (see V.3.2) and the United States' "privatized" approach (see V.3.8). Fortunately, this approach does not appear to hinder German companies in their capacity to innovate, customize their products and services to meet consumer demands, or engage in domestic and international collaborations with other companies, at least according to German professionals' assessments of the current data protection and informational privacy regulations (see IV.3.4.1). They also assessed the impact of this approach on digital development and the implementation of digital innovations quite positively (see IV.3.4.3), though significantly less positively than Chinese and US professionals (III.4.3).

According to Whitman (2004), the main violator in the European understanding of privacy described above is the media (1161). Our own and others' findings concur with this observation: Both German professionals and German consumers trusted media companies and search and social media sites the least to use consumers' personal data correctly of all industries investigated.[55] While this tendency was not exclusive to Germany, our comparison of German consumers with those surveyed in Brazil, China, Japan, Russia, and the United States[56] revealed that German consumers represented the smallest minority expressing confidence in these two industries to use their data correctly (see III.3.2.1 & IV.3.3.1; Wawra 2023b, 77; Ipsos 2019, 20).

Europe's characteristic skepticism toward the media regarding privacy issues is also reflected in German professionals' negative assessments of the levels of consumer data protection provided by media companies and search and social media sites, which was considered *sufficient* or *rather sufficient* by only a minority and in which both industries ranked lowest (see III.3.4.1 & IV.3.3.4). While neither tendency is exclusive to Germany, these trends are particularly noteworthy as, overall, satisfaction with the level of corporate consumer data protection was relatively high in Germany, with Germany leaning toward the high-satisfaction countries in this respect (see IV. 3.3.4).

In line with Europeans' suspicions of the media, compliance with the national regulation of consumer data protection and informational privacy by media compa-

55 However, there was still a majority of professionals who expressed trust in media companies in this context, while only a minority said they trusted search and social media sites.

56 Ghana was not part of the survey.

nies and search and social media sites was assessed similarly negatively by professionals in our survey (see III.3.3.1, IV.3.3.2). Moreover, Germany was the only country where both industries received significantly lower compliance ratings than most other industries surveyed (see III.3.3.1). Regarding search and social media sites, German professionals deemed compliance significantly less sufficient than respondents in the United States, China, and Brazil (see III.3.3.2). All this is, again, particularly noteworthy as, overall, Germany qualified as a truly intermediate case between countries with low and high perceived compliance (see IV.3.3.2). The other countries, however, in which only a minority of professionals assessed compliance by these industries as *sufficient* or *rather sufficient*, were either countries with low perceived compliance (Japan, Switzerland) or countries leaning toward them (Ghana; see IV.3.3.2).

Regarding the enforcement of legislation, Europe mainly relies on "hard power," i.e., "punitive action," in the form of a "powerful regulatory body, law enforcement, and punishment" (Wang 2020, 679; drawing on Miyashita 2016, 108). This stands in contrast to Japan's "soft power" approach (see V.3.3). Indeed, a majority of German professionals considered the government's enforcement of data protection and informational privacy laws to be heavy or robust (see IV.3.3.3), which is in line with this tendency. However, in our cross-cultural comparison based on considerations of statistical significance, Germany does not constitute a country with high perceived government enforcement in this respect, but occupies the midfield below China (a country with high perceived government enforcement) and the United States (which leaned toward the category of high perceived government enforcement countries). This reflects Europe's limited level of enforcement compared to the United States and China, which has been characterized as a weak spot of German (European) data protection:

> [One] problem of the German (and in particular European) system is its enforcement dimension: Even though [it has] the most intensive substantial regulation, its enforcement system does not reach the same capabilities as China or the USA (including California) in terms of enforcement instruments and actual enforcement activities. (Sonnenberg 2024, 78)

3.8 United States

Whereas privacy in Europe is above all linked to an individual's dignity (see V.3.7), the American concept of privacy can be explained in terms of "privacy as an aspect of liberty."[57] The "foundation of American privacy thinking," has always been "[s]uspicion of the state," according to Whitman,

57 Whitman (2004) draws conceptually here on Post's (2001) concepts of privacy.

> … and American scholarly writing and court doctrine continue to take it for granted that the state is the prime enemy of our privacy. To Americans, the starting point for the understanding of the right to privacy is … to be sought in the late eighteenth century, and especially in the Bill of Rights, with its vigorous circumscription of state power. In particular, "privacy" begins with the Fourth Amendment: At its origin, the right to privacy is the right against unlawful searches and seizures. It is thus a right that inheres in us as free and sovereign political actors, masters in our own houses, which the state is ordinarily forbidden to invade. (Whitman 2004, 1211–1212)

The core American privacy mentality is captured in the famous statement describing the "sanctity of the home" that stems from the *Boyd v. United States* case of 1886 (Whitman 2004, 1212–1213). Whitman considers "Boyd's fundamental understanding of 'privacy' rights as generalizations of the principle of the 'sanctity of the Home'" to be so formative that, he claims, "the standard history of modem American privacy rights should really begin, not with Warren and Brandeis's … ['right to be let alone'], but with *Boyd v. United States*, four years earlier" (Whitman 2004, 1213).

The American privacy mentality can, however, be traced back even further to the settlement period. According to Kohl (2023), "[t]he anti-State focus of American privacy is deeply inscribed with the settler mentality of self-reliance, self-rule and distrust of government" (744). Thus, in contrast to the European idea of privacy, the US concept

> is much more oriented toward values of liberty, and especially liberty against the state. At its conceptual core, the American right to privacy still takes much the form that it took in the eighteenth century: It is the right to freedom from intrusions by the state, especially in one's own home. (Whitman 2004, 1162)

Hence, US concerns about privacy often relate to preserving some sort of "private sovereignty within our own walls" (Whitman 2004, 1162). This attitude to privacy is epitomized in the well-known proverb "My home is my castle" (Kohl 2023, 742). Whitman (2004) observes that "[o]ver time, to the American mind, the early republican commitment to 'privacy' has matured into a much more far-reaching right against state intrusion into our lives" (1212). As a consequence, "Americans are consistently more drawn to problems touching on the depredations of the state" than Europeans (Whitman 2004, 1163). In 2013, these characteristically US fears were reaffirmed by whistleblower Edward Snowden's revelations of global mass surveillance through America's National Security Agency.

This could help explain why US consumers proved to be the most critical of whether their government was using personal data correctly in a survey of our selected countries conducted by Ipsos (2019, 20): Only about one-third (34 %) of US respondents expressed a great deal or fair amount of trust in their government in this

respect (see Wawra 2023b, 74). This is in line with the American "citizens-versus-government conception of privacy" (Kohl 2023, 744) outlined above, according to which "governments cannot be trusted to not interfere unduly with individuals" (Kohl 2023, 744). However, our results regarding US professionals stand in contrast to this notion of privacy: US professionals' trust in their government to use personal data correctly was second highest, and significantly higher than that of three other countries (see IV.3.3.1). One explanation for this discrepancy could be that the professionals were better informed about data protection regulations in the US as well as government compliance and felt that both were satisfactory. The latter is supported by our survey findings: US professionals were the most satisfied with their country's regulation of informational privacy and data protection.

The US fear of the state intruding into the private sphere might also explain why, overall, US professionals' mean sensitivity ratings tended to be the highest and were significantly higher than those of respondents in three other countries. Moreover, it could shed light on why US state laws (CPRA and VCDPA) list the most sensitive data categories of all seven countries (see IV.3.2).

The US concept of privacy is also closely linked to another central tenet of US culture, liberalism, which in the United States is characterized by values such as freedom, individualism, and the free-market economy (see Vorländer 2013, 632). In fact, the US approach to privacy has been termed a "trade paradigm" based on the assumption that data are a commodity that have economic value (see Gao 2023, 714–716). This approach is rooted in neoliberalism, that is, in the belief that markets should regulate themselves without state intervention (see Gao 2023, 717). In relation to data, this means that "the market should serve as the predominant mechanism to price data correctly and allocate it efficiently" (Gao 2023, 716). The default position is that data flows should be free and unrestricted (see Gao 2023, 717–718). Similarly, Wang (2020) characterizes the US approach to privacy as "privatized," meaning that it is defined by restraint on the part of the state and more trust in and reliance on the private sector, i.e., companies that are not state-controlled, when it comes to data protection regulation.

One might thus expect that too much interference from the state in the form of data protection and informational privacy regulations would be viewed as counterproductive to public interest in the United States. However, our survey shows that US professionals tend to be in favor of strengthening such regulations: The United States was found to be a low-satisfaction country, with the majority of professionals advocating to increase the regulation of data protection and informational privacy for certain data types, contexts of data disclosure, purposes of data disclosure, and industries (see IV.3.1). Such regulations protect consumers from privacy violations by companies and other private parties, but also by the state. From this point of view, this finding can be interpreted as being in line with the privacy orientation

outlined above, which seeks to avoid government interference in citizens' private matters. This is an end, which, ironically, can be achieved by means of government interference in the form of stricter privacy regulations.

Though a majority desired stricter regulation for certain data types, contexts of data disclosure, purposes of data disclosure, and industries, we found that US professionals mostly regarded the way in which several industries currently handle consumer data and conform to existing regulations as satisfactory: The United States qualified as a high-trust country (see IV.3.3.1) and a country with high perceived compliance (see IV.3.3.2) in this regard. Moreover, we found the United States to be a high-satisfaction country regarding the levels of consumer data protection offered by various industries (see IV.3.3.4). In particular, the latter finding could be due to assumptions connected to American economic liberalism (see above), according to which "the markets are inherently efficient and self-regulating in the absence of government interference" (Newfield 2014, 66), with "consumer protections," simply "plac[ing] unnatural burdens on these efficient markets" (Newfield 2014, 66). The prevalence of such assumptions may naturally lead to greater satisfaction with or at least acceptance of the status quo when it comes to the consumer data protection offered by several US industries.

Still, it seems that US professionals viewed some of the current government interference in consumer data protection in the corporate sector positively. We found that most of them believed that the regulation of data protection and informational privacy had improved corporate data handling and consumers' ability to easily manage their privacy needs, and those beliefs were also particularly strong in cross-cultural comparison (see IV.3.4.2). However, according to the surveyed professionals, government interference in the form of regulation was such that it did not impede companies' ability to customize products and services, innovate, and cooperate with domestic and international companies (see IV.3.4.1). In fact, US respondents assessed the impact of regulation in their country as significantly more positive on all these points (except for domestic cooperation) than professionals in at least half the other countries. They also generally assessed the impact of regulation on digital development and the implementation of digital innovations as (very) positive (compared to most other countries as well; see IV.3.4.3). Because, according to their assessments, the current regulations still offer American businesses enough freedom to innovate, tailor products and services to consumers' needs, and cooperate with other businesses, it is perhaps unsurprising that most of the professionals surveyed assessed the overall impact of regulation as positive (compared to half the other countries as well; see IV.3.4.3). However, like in most other countries, US professionals believed that current regulations were creating too much bureaucracy for the state, for companies, and for consumers. They stood out in cross-cultural comparison in terms of their particularly negative assessments of how much

bureaucracy was being produced for the state (see IV.3.4.2). This is in line with the basic US mentality of questioning state interference outlined above. Considerable bureaucracy implies that many data are being collected that can potentially be used to learn more about people's behavior and intervene in their lives.

VI Conclusion

The study presented in this book has revealed some cross-cultural trends in professionals' perceptions of data protection and informational privacy regulations and practices, but also many cultural (and intracultural) differences. We have discussed divergent comparative results against the backdrop of specific cultural (privacy) values and norms, which form a fundamental part of the Data Disclosure Model developed here. This model integrates factors that potentially explain differences between individuals and, on the basis of aggregation, cultural differences in perceptions of data protection and informational privacy and the ensuing data disclosure behavior. Key survey findings will be briefly summarized below, including central explanatory factors.

The findings of our survey of data protection professionals in Brazil, China, Germany, Ghana, Japan, Switzerland, and the United States show that there are some common cross-cultural tendencies in perceptions of data protection and informational privacy on which practices and regulations for transnational data flows can be based. A majority of professionals in all the countries surveyed (at least somewhat) agreed that consumers should have autonomy over their data disclosure decisions, i.e., should be able to decide for themselves whether to share data or not. We can also derive a cross-cultural blueprint for good data collection practice from our data, which includes (1) that companies should only be allowed to collect personal data from consumers with their consent, (2) that they should always provide deletion options for personal data, (3) that they should always explicitly communicate what consumers' personal data will be used for, and (4) that they should have to request consumers' consent once more when using their data for purposes other than those previously stated. Moreover, a majority of professionals in all countries surveyed trusted healthcare providers and financial services companies to use consumers' personal data correctly.

At the same time, however, we sometimes found slight and often significant cultural differences in the scope (in terms of percentages) of professionals' agreement or disagreement with all the items surveyed. Based on the majority responses from each country, we identified the following cultural differences pertaining to central questions of data protection and informational privacy. To start with, Chinese and Japanese professionals were more reserved regarding their commitment to consumers' data autonomy than professionals from the other countries. While a majority of respondents in all other countries agreed *strongly* that consumers should be able to decide whether to share their data, only a minority of Japanese and Chinese respondents held the same view, and their agreement was significantly lower than that of respondents in most other countries. This points toward a cultural difference in this basic attitude toward data disclosure: Consumers' data autonomy seems to

https://doi.org/10.1515/9783111458366-006

be less important in China and Japan than in the other countries. It was shown in chapter V.3 that this finding is supported by historically shaped privacy attitudes in both countries and, in China, by pressures from the political system.

We were also able to identify cultural differences in professionals' perceptions of the need to adjust data protection and informational privacy regulations and practices, assessments of consumers' data protection literacy, perceived data sensitivity, the data power of companies and governments in terms of their responsibilities in the data collection process, and trust in various industries and governments[58] to use consumer data correctly. We identified the United States, China, and Brazil as high-trust countries regarding the corporate use of consumer data and Japan and Switzerland as low-trust countries.[59] Cultural differences could also be found in the different industries' perceived compliance with consumer data protection and informational privacy regulations. Again, we identified countries with high perceived compliance (the United States, China, and Brazil) and low perceived compliance (Japan and Switzerland). The perceived levels of consumer data protection offered by the different industries varied cross-culturally as well, as did the evaluation of current domestic regulations to prevent the corporate misuse of consumer data: The United States, China, and Brazil were high-satisfaction countries, while Japan and Switzerland were low-satisfaction countries. The latter finding was further corroborated by the fact that only a minority of Japanese and Swiss professionals assessed the current state of regulation as *sufficient* or *rather sufficient* to prevent the corporate misuse of consumer data and exhibited significantly lower ratings in this respect than the high-satisfaction countries China, Brazil, and the United States.[60]

However, these classifications were not necessarily the result of cultural similarities between, for example, the United States and China. We were able to show how different cultural factors may have contributed to these findings. Thus, the United States' status as a high-trust country, a country with high perceived compliance, and a high-satisfaction country regarding the level of consumer data protection offered may—among other things—be due to the widespread belief there in American economic liberalism (see Vorländer 2013, 632; Newfield 2014, 66). China's status as the same, in contrast, could be linked in particular to the country's special privacy profile and the Chinese legal context, which offers comprehensive mechanisms for safeguarding data in private industry (see Sonnenberg 2024, 77). Likewise, Japan's

58 We looked at seven industries, i.e., healthcare providers, financial services companies, shipping/delivery companies, telecommunications companies, retailers selling goods and services, search and social media sites, and media companies, as well as domestic and foreign governments.

59 This and the following categorizations of the countries are based on the survey results for the seven industries only.

60 Japanese sufficiency ratings were actually significantly lower than those of *all* other countries.

status as a low-trust country, a country with low perceived compliance, and a low-satisfaction country regarding the level of consumer data protection in place might reflect Japanese professionals' awareness of their culture's pragmatic approach to privacy (see Scroope 2021; Wawra 2023a; Orito & Murata 2005; Hiramatsu 1993). Switzerland's classification as the same, however, could above all be attributable to the Swiss tendency to distrust the private sector (see Thir et al. 2023) despite being a trusting culture overall (see Bewes 2010; EVS/WVS 2022, 189), and the fact that our survey was conducted before the new Swiss Data Protection Act and Data Protection Ordinance came into force.

Furthermore, perceptions of the enforcement of consumer data protection in the seven countries varied cross-culturally. Again, we were able to determine different cultural factors explaining this finding. We identified China, for example, as a country with high perceived government enforcement, high perceived corporate enforcement, and high perceived enforcement by private parties. These findings can once more be linked to China's privacy profile and legal context. Regarding enforcement by private parties, Brazil is also a high perceived enforcement country, which primarily reflects current legal practices in Brazil (see Sonnenberg 2024, 70–71). By contrast, Japan is a country with low perceived enforcement in this respect, as well as low perceived government enforcement (as is Ghana) and low perceived corporate enforcement. This can be attributed in particular to the Japanese inclination to use "soft power" (e.g., via a corporation's public image) (see Miyashita 2011, 233; as cited in Wang 2020, 679) rather than legal punishment. Ghana's status as a country with low perceived government enforcement, however, is probably best explained by the country's limited resources in this respect (see Hoffmann 2022, 19; Hoffmann 2023).

When considering the pros and cons of current data protection and informational privacy regulations, it was Japanese and Swiss respondents who consistently drew attention by deviating from professionals in the other countries in their assessments. In all countries except Switzerland and Japan, a majority of professionals believed that their data protection and informational privacy regulations still allowed for international cooperation between companies and that they had a positive or very positive impact on digital development and the implementation of digital innovation. Swiss and Japanese respondents' assessments were significantly less positive in both respects than those given by professionals in at least half the other countries. A majority of respondents in all countries but Japan also believed that current regulations still allowed companies to customize and develop products and services and to cooperate *domestically*. Their assessments were significantly more negative in this respect than those given by respondents in almost all other countries. Swiss respondents were significantly more negative about product and service development and corporate cooperation on the national level than at least

half the other countries. It should be noted that a majority of both Swiss and Japanese respondents did not answer on the negative end of the scale for any of these points either, but many were often neutral. In Japan, this tendency toward neutrality is in line with the country's "pragmatic" attitude toward privacy, though Japanese respondents' comparatively negative view of the impact on companies was somewhat surprising given that the Japanese approach to data protection is said to be "pro-economy" (Murata 2019; as cited in Wang 2020, 670). Swiss respondents' rather negative assessments in this respect may again be predominantly attributable to the fact that their data protection framework had not yet been updated to align with the GDPR at the time of surveying and was thus potentially detrimental to business relations with EU corporations.

Regarding other aspects of data protection regulation, however, Japanese and Swiss respondents were *less* negative than the others. Thus, apart from Japanese and Swiss respondents, a majority of professionals from the other countries agreed that the regulation of data protection and informational privacy created too much bureaucracy for the state, for companies, and for consumers. Japanese respondents stood out regarding excessive bureaucracy for consumers as they were significantly less negative than respondents from most other countries. They also drew attention alongside Ghanaian respondents in that, unlike respondents from other countries, a majority of them did not think that the regulation of data protection and informational privacy overloaded consumers with information. Japanese respondents were significantly less negative in this respect than respondent from half the other countries. The Japanese legal context here can only partly explain these results, with bureaucracy related to the protection of informational privacy in Japan most likely falling somewhere in the middle in cross-cultural comparison (see Sonnenberg 2024; V.3.3). The comparatively positive Swiss assessments of the impact of their regulations on bureaucracy may, again, be predominantly due to the fact that respondents had the old data protection regulation in mind, which likely kept bureaucracy in check compared to the new law. In addition, Swiss respondents possibly unconsciously compared Swiss data protection laws with the GDPR, whose bureaucracy-intensive character has been emphasized repeatedly in Swiss media (see V.3.6).

At the other end of the scale, Chinese professionals were significantly more negative about the burden of bureaucracy on companies and information overload for consumers than respondents from most other countries, which we attributed to a fatalistic attitude (see V.3.2). US respondents were significantly more negative about bureaucracy for the state than respondents from half the other countries. Since excessive bureaucracy in this respect may imply extensive data collection by the state, this finding could be linked to the basic US privacy mentality of being critical of state interference (see Kohl 2023, 744).

On the positive side, a majority of Brazilian, Chinese, German, Ghanaian, and US respondents agreed that data protection and informational privacy regulation had led to companies handling data more professionally and that it enabled consumers to easily manage their privacy needs. Regarding companies' professional handling of data, Chinese, Brazilian, and US respondents were significantly more positive than respondents from the other four countries, which is in line with their status as high-satisfaction countries regarding the level of consumer data protection offered by the various industries mentioned above. When it came to the impact of regulation on privacy management, Chinese and US respondents were more positive than respondents from at least half the other countries, which is in line with China's privacy profile. By contrast, Japanese and Swiss professionals were significantly less positive than at least half the other countries regarding the impact of their regulatory scheme on both privacy management and corporate data handling. It is noteworthy that there was no majority response on the negative end of the scale from either Japanese or Swiss professionals, but once more, many of them took a neutral stance. Swiss professionals' comparatively negative assessments might again be explained by the period in which the survey was administered, namely when the old data protection law was still in force. Unlike the revised law, the old one did not yet mention consumer protection (see Sonnenberg & Hoffmann 2022, 3). Japanese professionals' assessments may be attributable to their awareness of the "laissez-faire" approach to privacy in their country (see V.3.3). The latter may also explain why Japan was the only country without a majority that believed that current regulation of data protection and informational privacy was *sufficient* or *rather sufficient* to protect the fundamental rights of individuals. A majority of Japanese professionals, however, did not think that they were inadequate either, and many of them again gave a neutral answer. Still, they were significantly more critical of their country's regulations in this respect than respondents from *all* other countries.

Finally, overall, a majority of professionals from China, the United States, Brazil, and Germany expressed the opinion that the regulation of data protection and informational privacy had a positive impact. The majority of Japanese professionals responded that the impact was neutral, as did half of Swiss professionals and most Ghanaian professionals. While Swiss and Japanese professionals' assessments were significantly less positive than those given by professionals in at least half the other countries, Chinese and US professionals' assessments were significantly more positive than those made by professionals in most other countries. Chinese respondents' favorable assessments are in line with the country's privacy profile, particularly against the backdrop of China's Social Credit System, which rewards positive comments about the government (see Bartsch & Gottske 2018).

The high frequency of neutral responses from Japanese data protection professionals that drew our attention in our comparative study are, as mentioned above,

in line with Japan's "pragmatic" privacy orientation, while the neutral answers from Swiss respondents were most likely due to the fact that the survey was carried out before the reformed version of the main data protection law, the Data Protection Act and the associated Data Protection Ordinance (Federal Assembly of the Swiss Confederation 2020; Swiss Federal Council 2022), came into force.

We have also seen that professionals' attitudes toward and assessments of central data protection and informational privacy issues were sometimes in line with consumers' views and sometimes diverged from them. We have thus been able to show that there was considerable intracultural variation at times, for example, in Brazilian professionals' and consumers' trust in companies to handle consumer data. While Brazil qualified as a high-trust country in this regard according to professionals' assessments, consumers' views are in line with the country's distrust bias, effected by Brazilian *jeitinho* (among other things), the (accepted) bending of formal rules (see Ferreira et al. 2012, 321, 335; Pilati Rodrigues et al. 2011, 32). This fundamental aspect of Brazilian culture also helps to explain several other results from our survey, such as Brazilian respondents' comparatively positive view of the impact of their data protection and privacy regulations on corporate innovation, cooperation with other companies, and product and service customization, despite intense regulation in Brazil.

Furthermore, we found that Ghanaian respondents were more concerned about data protection and informational privacy than might be expected given the country's collectivist orientation, which is said to attribute much less importance to individual privacy (see Hofstede et al. 2010). However, our analysis showed that Western notions of privacy and their connection to the individualism/collectivism dichotomy might simply be ineffective to grasp Ghanaian privacy values. Recent historical events such as Ghana's history with cybercrime and its coverage in Ghanian media were identified as additional contributory factors (see Agyei-Bekoe 2013; V.3.5).

In the final parts of our study, we established that the causes of people's attitudes toward and perceptions of data protection and informational privacy and their ensuing data disclosure behavior, are manifold, multifactorial, and intertwined. We first developed a Data Disclosure Model that integrates key factors potentially influencing data disclosure behavior. It can be used as a starting point for theoretical and empirical studies on data disclosure. Simultaneously, we emphasized that the impact of each single factor can vary, depending on the concrete data disclosure situation. We then predominantly focused on one fundamental part of our model, historically shaped cultural (privacy) values and norms, and discussed their potential to help explain our survey findings for each country.

As illustrated by Gao (2023), one major challenge in regulating global, transnational data flows is navigating between three different perspectives, which are represented by the three key global players: the United States, Europe, and China.

Whereas the United States follows a "trade paradigm," the EU adheres to a "fundamental rights paradigm" and China to a "a national security paradigm" (Gao 2023). Regarding Germany, our literature review showed how the country's past has affected Europe's dignity-focused approach to privacy and the resulting data protection legislation (see V.3.7). Similarly, our review of the literature on the US privacy perspective showed how the latter has been influenced by neoliberalist thinking and a deep suspicion of the state, with its historical roots, among other things, in the settlement period (see Kohl 2023; V.3.8). These findings concur with Whitman's observation that specific, historically shaped cultural factors impact privacy regulations and practices:

> [P]rivacy law … is the product of local social anxieties and local ideals. In the United States those anxieties and ideals focus principally on the police and other officials, and around the ambition "to secure the blessings of liberty," while on the Continent they focus on the ambition to guarantee everyone's position in society, to guarantee everyone's "honor." This was already true in 1791, in the French Revolution … , and it remains true today. (Whitman 2004, 1219–1220)

Furthermore, he points out that regulations will only be effective in a society if they reflect its basic values (see Whitman 2004, 1220). Thus, as noted by Miyashita, acknowledging and accommodating specific cultural features is of the utmost importance in the context of cross-border data transactions:

> Information flows across cultures, but privacy is deeply rooted in individual cultures. The task of creating rules for cross-border privacy is hard, but must be realized in the age of a global information community. Our task is not to realize the universal values of privacy which persist in every society, but rather to tolerate the differences between cultures of privacy in the process of developing cross-border privacy rules. We will be able to complete the task by recognizing the essence of privacy and its cultural background. (Miyashita 2009, 280)

Our cross-cultural study aimed to contribute to a better understanding of cultural specificities regarding perceptions of data protection and informational privacy regulations and practices. The more we know about cross-cultural and intracultural variation as well as common trends across cultures regarding central issues of data protection and informational privacy, the better we can shape the contexts and processes of data disclosure in and between our societies. This seems increasingly important in a world where digital technology and AI are continuing to develop at a rapid pace and have already become formative, integral parts of our ever-more networked communities. The cross-cultural trends and cultural differences we have identified should therefore assist in informing regulatory reforms of data protection and informational privacy as well as related practices not only in the countries we have studied but also transnationally.

References

Acemoglu, Daron; Robinson, James A. (2012). *Why nations fail: The origins of power, prosperity and poverty*. New York, NY: Crown Publishers.

Ackermann, Kurt Alexander; Burkhalter, Linda; Mildenberger, Thoralf; Frey, Martin; Bearth, Angela. (2021). Willingness to share data: Contextual determinants of consumers' decisions to share private data with companies. *Journal of Consumer Behaviour* 2021. 1–12. https://doi.org/10.1002/cb.2012 (last access: 11/16/2023).

Aden, Hartmut. (2021). Privacy and security: German perspectives, European trends and ethical implications. In Iphofen, Ron; O'Mathúna, Dónal (eds.). *Ethical issues in covert, security and surveillance research. Volume 8*. Bingley: Emerald Publishing Limited. 119–129. https://doi.org/10.1108/S2398-601820210000008009 (last access: 05/31/2023).

Adjei, Stephen Baffour; Sam, Sarah Tara; Sekyere, Frank Owusu; Boateng, Philip. (2024). *Ubuntu* philosophy and the experiences of deaf people in Ghana. In Mutanga, Oliver (ed.). Ubuntu *philosophy and disabilities in sub-Saharan Africa*. Abingdon, Oxon: Routledge. 163–183. https://doi.org/10.4324/9781003343684-10 (last access: 03/20/2024).

Adu, Elizabeth Nyaadu. (2023). Ghanaians advised to build strong skills in cyber security. *Graphic Online*. Graphic Communications Group Limited. Published Oct – 13 – 2023, 03:00. https://www.graphic.com.gh/business/business-news/ghanaians-advised-to-build-strong-skills-in-cyber-security.html (last access: 12/12/2023).

Agyei-Bekoe, Eric. (2013). Empirical investigation of the role of privacy and data protection in the implementation of electronic government in Ghana. Doctoral thesis, De Montfort University. https://dora.dmu.ac.uk/bitstream/handle/2086/11150/Eric%20Agye-Bekoe%20PhD%20Thesis%20report.pdf?sequence=1 (last access: 11/16/2023).

Akira Miura, Marco; Pilati, Ronaldo; Milfont, Taciano Lemos; Ferreira, Maria Cristina; Fischer, Ronald. (2019). Between simpatia and malandragem: Brazilian jeitinho as an individual difference variable. *PloS One* 14(4). 1–16. https://doi.org/10.1371/journal.pone.0214929 (last access: 01/22/2024).

Anaraky, Reza Ghaiumy; Byrne, Kaileigh Angela; Wisniewski, Pamela J.; Page, Xinru; Knijnenburg, Bart. (2021). To disclose or not to disclose: Examining the privacy decision-making processes of older vs. younger adults. *CHI '21: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. New York, NY: Association for Computing Machinery. 1–14. http://dx.doi.org/10.1145/3411764.3445204 (last access: 02/07/2022).

André, Quentin; Carmon, Ziv; Wertenbroch, Klaus; Crum, Alia; Frank, Douglas; Goldstein, William; Huber, Joel; van Boven, Leaf; Weber, Bernd; Yang, Haiyang. (2018). Consumer choice and autonomy in the age of artificial intelligence and big data. *Customer Needs and Solutions* 5(1–2). 28–37. https://www.researchgate.net/publication/321914602_Consumer_Choice_and_Autonomy_in_the_Age_of_Artificial_Intelligence_and_Big_Data (last access: 08/30/2023).

Armour, John; Schmidt, Caroline. (2017). Building enforcement capacity for Brazilian corporate and securities law. *European Corporate Governance Institute (ECGI) – Law Research Paper Series* 344. http://dx.doi.org/10.2139/ssrn.2901698 (last access: 01/25/2024).

Awiah, Dominic Moses. (2017). Sharing personal information on social media risky – Cyber security experts. *Graphic Online*. Graphic Communications Group Limited. Published Dec – 07 – 2017, 06:41. https://www.graphic.com.gh/news/general-news/sharing-personal-information-on-social-media-risky-cyber-security-experts.html (last access: 12/12/2023).

Barbosa, Livia. (2006). *O Jeitinho Brasileiro: A arte de ser mais igual do que os outros. [The Brazilian jeitinho: The art of being more equal than others]*. Rio de Janeiro: Elsevier.

https://doi.org/10.1515/9783111458366-007

Bartsch, Bernhard; Gottske, Martin. (2018). China's social credit system. Gütersloh: Bertelsmann Stiftung. https://www.bertelsmann-stiftung.de/fileadmin/files/aam/Asia-Book_A_03_China_Social_Credit_System.pdf (last access: 02/07/2023).

Bewes, Diccon. (2010). *Swiss watching: Inside Europe's landlocked island*. London: Nicholas Brealey Publishing.

Bonney, Emmanuel. (2023). Cyber security awareness month launched. *Graphic Online*. Graphic Communications Group Limited. Published Sep – 04 – 2023, 07:20. https://www.graphic.com.gh/news/general-news/cyber-security-awareness-month-launched.html (last access: 12/12/2023).

Bradford, Anu. (2019). *The Brussels effect: How the European Union rules the world*. New York, NY: Oxford University Press.

Bruce, Emmanuel. (2022). Financial institutions breach Cybersecurity Act – Only 28 % registered their infrastructure. *Graphic Online*. Graphic Communications Group Limited. Published Nov – 01 – 2022, 11:48. https://www.graphic.com.gh/business/business-news/financial-institutions-breach-cyber security-act-only-28-registered-their-infrastructure.html (last access: 12/12/2023).

Bühlmann, Lukas; Reinle, Michael. (2020). Neues Schweizer Datenschutzrecht: Wichtigste Regelungen der DSG-Revision im Überblick. *Mondaq: Connecting knowledge & people*. Published Dec – 9 – 2020. https://www.mondaq.com/privacyprotection/1014308/neues-schweizerdatenschutzrecht-wichtigste-regelungen-der-dsgrevision-im-berblick (last access: 01/11/2024).

Cambridge Dictionary. (2024). Portuguese–English dictionary. "jeito". Cambridge University Press & Assessment. https://dictionary.cambridge.org/dictionary/portuguese-english/jeito (last access: 02/05/2024).

Cephas, Dapuri M. (2023). Combatting cybercrime: 2024 election in perspective. *Graphic Online*. Graphic Communications Group Limited. Published Nov – 14 – 2023, 09:32. https://www.graphic.com.gh/features/opinion/ghana-news-combatting-cybercrime-2024-election-in-perspective.html (last access: 12/12/2023).

Chen, Mo; Grossklags, Jens. (2022). Social control in the digital transformation of society: A case study of the Chinese social credit system. *Social Sciences* 11(6). 1–23. https://www.mdpi.com/2076-0760/11/6/229 (last access: 02/07/2023).

Chin, Josh. (2023). 'Rule of law' or 'rule by law'? In China, a preposition makes all the difference. *The Wall Street Journal*. Dow Jones & Company. Published Oct – 20 – 2014, 2:03. https://www.wsj.com/articles/BL-CJB-24523 (last access: 07/31/2023).

CIGI-Ipsos. (2019a). CIGI-Ipsos global survey on internet security & trust. Part 6: Cross-border data flows. Centre for International Governance Innovation. https://www.cigionline.org/cigi-ipsos-global-survey-internet-security-and-trust/ (last access: 12/15/2021).

CIGI-Ipsos. (2019b). CIGI-Ipsos global survey on internet security & trust. Detailed results tables. Centre for International Governance Innovation. https://www.cigionline.org/cigi-ipsos-global-survey-internet-security-and-trust/ (last access: 19/06/2023).

Cisco. (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: 06/22/2023).

Cohen, Jacob. (1988). *Statistical power analysis for the behavioral sciences*. (2nd edition). Hillsdale, NJ: Lawrence Erlbaum Associates.

Coleman, James S. (1986). Social theory, social research, and a theory of action. *American Journal of Sociology* 91(6). 1309–1335.

Credit Suisse. (2022). Credit Suisse Sorgenbarometer 2022: Helvetischer Alleingang oder europäische Allianz? https://www.credit-suisse.com/media/assets/corporate/docs/about-us/responsibility/worry-barometer/schlussbericht-credit-suisse-sorgenbarometer-2022.pdf (last access: 12/19/2023).

Cullen, Rowena. (2008). Citizens' concerns about the privacy of personal information held by the government: A comparative study, Japan and New Zealand. In Sprague, Ralph H. Jr. (ed.). *Proceedings of the 41st Hawaii International Conference on System Sciences.* Waikoloa, HI. 224–224. https://doi.org/10.1109/HICSS. 2008.91 (last access: 05/30/2023).

Cyber Security Authority Ghana. (2021). Facebook post by the verified profile "Cyber Security Authority Ghana". Published Aug. – 11 – 2021. https://www.facebook.com/280228785796871/posts/every-year-in-october-the-national-cyber-security-centre-holds-the-national-cybe/1158329564653451/ *(last access: 12/12/2023).*

Dagbanja, Dominic. (2016). The right to privacy and data protection in Ghana. In Makulilo, Alex (ed.). *African data privacy laws*. Cham: Springer International. 229–248. https://doi.org/10.1007/978-3-319-47317-8_10 (last access: 06/26/2023).

DDV (Deutscher Dialogmarketing Verband)/Acxiom. (2022). Datenschutz in Deutschland: Was Verbraucher wirklich denken. https://marketing.acxiom.com/rs/982-LRE-196/images/GDMA_GER_Data_Privacy_2022.pdf (last access: 05/31/2023).

Deffenti, Fabiano. (n.d.). Dispute resolution. *Laws of Brazil.* https://lawsofbrazil.com/dispute-resolution/#:~:text=Brazil%20is%20one%20of%20the,hundreds%20of%20thousands%20every%20year (last access: 01/25/2024).

DLA Piper. (2023). Data protection laws of the world: Compare data protection laws around the world. https://www.dlapiperdataprotection.com/ (last access: 10/23/2023).

Dotse, Dickson Worlanyo. (2023). Ghana leads Africa on cybersecurity issues. Graphic Online. Graphic Communications Group Limited. Published Dec – 06 – 2023, 09:00. https://www.graphic.com.gh/news/general-news/ghana-news-ghana-leads-africa-on-cybersecurity-issues.html (last access: 04/08/2024).

Duarte, Fernanda. (2005). The Brazilian Jeitinho as a structural fix: A 'snapshot' from an urban sustainability partnership program. Paper prepared for the *X APROS International Colloquium,* Oaxaca, Mexico, 7–10 December.

Duarte, Fernanda. (2006). Exploring the interpersonal transaction of the Brazilian jeitinho in bureaucratic contexts. *Organization* 13(4). 509–527. https://doi.org/10.1177/1350508406065103 (last access: 01/24/2024).

Elul, Elad Ben. (2022). *Urban Ghana and privacy in the digital age: An ethnographic exploration*. Abingdon, Oxon: Routledge.

Ennin, Daniel; Mensah, Ronald Osei. (2019). Cybercrime in Ghana and the reaction of the law. *Journal of Law, Policy and Globalization* 84. 36–45. https://doi.org/10.7176/JLPG (last access: 12/12/2023).

Ennin, Daniel; Mensah, Ronald Osei. (2022). Cybercrime in Ghana and victims accounts. *Mediterranean Journal of Social Sciences* 13(3). 1–14. https://doi.org/10.36941/mjss-2022-0019 (last access: 12/12/2023).

Essah, Naa Korkoi. (2018). Cyber Security awareness month in perspective. *Graphic Online.* Graphic Communications Group Limited. Published Nov – 05 – 2018, 17:17. https://www.graphic.com.gh/features/features/cyber-security-awareness-month-in-perspective.html (last access: 12/12/2023).

European Commission. (n.d.). Data protection in the EU: The General Data Protection Regulation (GDPR), the Data Protection Law Enforcement Directive and other rules concerning the protection of personal data. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en (last access: 12/21/2023).

EVS/WVS. (2022). European Values Study and World Values Survey: Joint EVS/WVS 2017-2022 Dataset (version 4.0.0). Documentation. Frequency Tables: WVS/EVS Joint v4.0 Results by Country. JD Systems Institute & WVSA. https://doi.org/10.14281/18241.21 (last access: 12/19/2023).

Federal Assembly of the Swiss Confederation. (2020). Federal Act on Data Protection (Data Protection Act, FADP). https://www.fedlex.admin.ch/eli/cc/2022/491/en (last access: 05/27/2024).

Federal Statistical Office. (2023). Vertrauen in Institutionen, nach verschiedenen soziodemografischen Merkmalen. Published May – 02 – 2023. https://dam-api.bfs.admin.ch/hub/api/dam/assets/24205329/master (last access: 12/19/2023).

Ferreira, Maria Cristina; Fischer, Ronald; Porto, Juliana Barreiros; Pilati, Ronaldo; Milfont, Taciano L. (2012). Unraveling the mystery of Brazilian jeitinho: A cultural exploration of social norms. *Personality & Social Psychology Bulletin* 38(3). 331–344. https://doi.org/10.1177/0146167211427148 (last access: 01/22/2024).

Field, And; Miles, Jeremy; Field, Zoë. (2012). *Discovering statistics using R*. London: SAGE.

Freude, Alvar; Freude, Trixy. (2016). Echoes of history: Understanding German data protection. *Newpolitik: German Policy. Translated*. Gütersloh: Bertelsmann Stiftung. 85–91. https://www.bertelsmann-stiftung.de/en/publications/publication/did/newpolitik (last access: 07/16/2024).

Gao, Raymond Yang. 2023. A battle of the Big Three? Competing conceptualizations of personal data shaping transnational data flows. *Chinese Journal of International Law* 22(4). 707–787. https://doi.org/10.1093/chinesejil/jmad040 (last access: 02/21/2024).

GDPR.eu. General Data Protection Regulation (GDPR) (VO (EU) 2016/679), https://gdpr.eu/tag/gdpr/ (last access: 03/07/2023).

Ghana Chamber of Telecommunications. (2020). Ghana records over 11,000 cybercrime cases since 2019. Published Oct – 06 – 2020. https://telecomschamber.com/news-media/industry-news/ghana-records-over-11-000-cybercrime-cases-since-2019 (last access: 12/12/2023).

Ghana Statistical Service. (2022). *Ghana 2021 population and housing census. Volume 3. General report: highlights*. https://census2021.statsghana.gov.gh/gssmain/fileUpload/reportthemelist/Volume%203%20Highlights.pdf (last access: 12/07/2023).

Ghose, Anindya; Li, Beibei; Macha, Meghanath; Sun, Chenshuo; Foutz, Natasha Zhang. (2022). Trading privacy for public good: How did America react during COVID-19? *NYU Stern School of Business.* http://dx.doi.org/10.2139/ssrn.3624069 (last access: 11/20/2023).

Grant, A. (2020). Internet privacy index. https://bestvpn.org/privacy-index/ (last access: 06/03/2022).

Grice, Paul. (1975). Logic and conversation. In Cole, Peter; Morgan, Jerry L. (eds.). *Syntax and semantics*. *Vol. 3: Speech acts*. New York: Academic Press. 41–58.

Hedström, Peter; Swedberg, Richard. 1998. *Social mechanisms: An analytical approach to social theory.* Cambridge: Cambridge University Press.

Hennemann, Moritz. (2021). Das Schweizer Datenschutzrecht im Wettbewerb der Rechtsordnungen. In Paal, Boris P.; Poelzig, Dörte; Fehrenbacher, Oliver (eds.). *Deutsches, europäisches und vergleichendes Wirtschaftsrecht: Festschrift für Werner F. Ebke zum 70. Geburtstag.* München: C.H. Beck. 371–382.

Herbert, Franziska; Schmidbauer-Wolf, Gina Maria; Reuter, Christian. (2020). Differences in IT security behavior and knowledge of private users in Germany. *Proceedings of the International Conference on Wirtschaftsinformatik (WI)*. 168–184. https://doi.org/10.30844/wi_2020_v3-herbert (last access: 04/09/2024).

Hiramatsu, Tsuyoshi. (1993). Protecting telecommunications privacy in Japan. *Communications of the ACM* 36(8). 74–77. https://dl.acm.org/doi/pdf/10.1145/163381.163400 (last access: 04/08/2024).

Hoffmann, Timo. (2022). Data Protection Act(ion): Report on the law of data disclosure in Ghana. *University of Passau IRDG Research Paper Series* 22(1). https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/ (last access: 12/13/2023).

Hoffmann, Timo. (2023). The laws of data disclosure: Examining the regulation of individuals' personal data disclosure in Brazil, China, the European Union, Ghana, Japan, Russia, Switzerland and the United States of America. In Hennemann, Moritz; von Lewinski, Kai; Wawra, Daniela; Widjaja,

Thomas (eds.). *Data disclosure: Global developments and perspectives*. Berlin: De Gruyter. 1–34. https://doi.org/10.1515/9783111010601-003 (last access: 03/20/2024).

Hofstede, Geert; Hofstede, Gert Jan; Minkov, Michael. (2010). *Cultures and organizations: Software of the mind.* New York, NY: McGraw-Hill.

Holm, Sture. (1979). A simple sequentially rejective multiple test procedure. *Scandinavian Journal of Statistics* 6(2). 65–70. http://www.jstor.org/stable/4615733 (last access: 04/08/2024).

Howe, Sarah. (2022). Cultural influences on personal data disclosure decisions: German perspectives. *University of Passau IRDG Research Paper Series* 22(14). https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/ (last access: 11/16/2023).

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: 06/19/2023).

Johnson, Baaba. (2023). Combating cyber crime: A crucial time to be security conscious. *Modern Ghana*. Published June – 30 – 2023. https://www.modernghana.com/news/1241541/combating-cyber-crime-a-crucial-time-to-be-securi.html (last access: 12/12/2023).

Kamwangamalu, Nkonko M. (1999). Ubuntu in South Africa: A sociolinguistic perspective to a pan-African concept. *Critical Arts* 13(2). 24–41. https://doi.org/10.1080/02560049985310111 (last access: 12/07/2023).

Kempken, Daniel. (2021). Rule by Law statt Rule of Law: Das chinesische Rechtsstaatskonzept als Herausforderung für Deutschland und Europa. *Analysen & Argumente* 460. https://www.kas.de/documents/252038/11055681/Rule+by+Law+statt+Rule+of+Law.pdf/9b5dbff8-4999-33dd-464d-7d4d636b5758?version=1.2&t=1635177691268 (last access: 02/05/2024).

Kessel, Lena. (2022). Cultural influences on personal data disclosure decisions: US-American perspectives. *University of Passau IRDG Research Paper Series* 22(4). https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/ (last access: 11/16/2023).

Kim, Melanie; Ly, Kim; Soman, Dilip. (2015). A behavioural lens on consumer privacy. Toronto: Rotman School of Management, University of Toronto. https://www.slideshare.net/slideshow/consumer privacybear2015final-1/64948255#1 (last access: 10/03/2024).

Kisselburgh, Lorraine; Beever, Jonathan. (2022). The ethics of privacy in research and design: Principles, practices, and potential. In Knijnenburg, Bart P.; Page, Xinru; Wisniewski, Pamela; Richter Lipford, Heather; Proferes, Nicholas; Romano, Jennifer (eds.). *Modern socio-technical perspectives on privacy*. Cham: Springer. 395–426. https://doi.org/10.1007/978-3-030-82786-1_17 (last access: 03/20/2024).

Kohl, Uta. 2023. The right to be forgotten in data protection law and two Western cultures of privacy. *The International and Comparative Law Quarterly* 72(3). 737–769. https://doi.org/10.1017/S0020589323000258 (last access: 11/30/2023).

Kozyreva, Anastasia; Herzog, Stefan; Lorenz-Spreen, Philipp; Hertwig, Ralph; Lewandowsky, Stephan. (2020). Künstliche Intelligenz in Online-Umgebungen: Repräsentative Umfrage zur öffentlichen Meinung in Deutschland. Berlin: Max-Planck-Institut für Bildungsforschung. https://pure.mpg.de/rest/items/item_3190264_15/component/file_3195146/content (last access: 05/31/2023).

Kuehnhenrich, Daniel. (2012). *Entwicklung oder Profit? Die staatliche und private Presse in Ghana*. Stuttgart: ibidem. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-66193-4 (last access: 12/12/2023).

Lasswell, Harold. (1964 [1948]). The structure and function of communication in society. In Bryson, Lyman (ed.). *The communication of ideas*. New York: Cooper Square Publishers. 37-51.

Li, Yao. (2022). Cross-cultural privacy differences. In Knijnenburg, Bart P.; Page, Xinru; Wisniewski, Pamela; Richter Lipford, Heather; Proferes, Nicholas; Romano, Jennifer (eds.). *Modern socio-technical*

perspectives on privacy. Cham: Springer. 267–292. https://doi.org/10.1007/978-3-030-82786-1_12 (last access: 05/30/2023).

Marschner, Ian C. (2011). glm2: Fitting generalized linear models with convergence problems. *The R Journal* 3(2). 12–15. https://journal.r-project.org/archive/2011-2/RJournal_2011-2_Marschner.pdf (last access: 11/16/2023).

Mensah, Ronald Osei; Mensah, Pius; Opoku, Daniel. (2023) Experiences and perceptions of cybercrime victims in Ghana: The perspective of digital consumers of agricultural produce. *Cogent Education* 10(2). 1–14. https://doi.org/10.1080/2331186X.2023.2285623 (last access: 12/12/2023).

Ministry of Communications and Digitalisation, Ghana. (2022). CSA. https://moc.gov.gh/csa/ (last access: 02/21/2024).

Miyashita, Hiroshi. (2009). Changing privacy and data protection in Japan. *The Sedona Conference Journal* 10. 277–280. https://thesedonaconference.org/sites/default/files/publications/Miyashita%20277-280_0.pdf (last access: 06/01/2023).

Miyashita, Hiroshi. (2011). The evolving concept of data privacy in Japanese law. *International Data Privacy Law* 1(4). 229–238. https://doi.org/10.1093/idpl/ipr019 (last access: 07/16/2024).

Miyashita, Hiroshi. (2016). A tale of two privacies: Enforcing privacy with hard power and soft power in Japan. In Wright, David; De Hert, Paul (eds.). *Enforcing privacy: Regulatory, legal and technological approaches*. Cham: Springer. 105–122. https://doi.org/10.1007/978-3-319-25047-2_5 (last access: 07/16/2024).

Morris, Kate; White, Timothy J. (2011). Neutrality and the European Union: The case of Switzerland. *Journal of Law and Conflict Resolution* 3(7). 104–111. https://academicjournals.org/article/article1379862766_Morris%20and%20White.pdf (last access: 12/14/2023).

Murata, Kiyoshi. (2019). Interview with Kiyoshi Murata, Professor and Director of the Centre for Business Information Ethics, Meiji University, in Tokyo, Japan (Jan. 18, 2019).

Newfield, Christopher. (2014). Corporation. In Burgett, Bruce; Hendler, Glenn (eds). *Keywords for American cultural studies*. (2nd edition). New York, NY: New York University Press. 63–68.

Olinger, Hanno N.; Britz, Johannes J.; Olivier, Martin S. (2007). Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa. *The International Information & Library Review* 39(1). 31–43. https://doi.org/10.1080/10572317.2007.10762729 (last access: 12/07/2023).

Orito, Yohko; Murata, Kiyoshi. (2005). Privacy protection in Japan: Cultural influence on the universal value. Paper presented at *ETHICOMP 2005*. https://www.researchgate.net/publication/260021544_Privacy_Protection_in_Japan_Cultural_Influence_on_the_Universal_Value (last access: 05/30/2023).

Orizet, Joël. (2019). Ein Jahr EU-DSGVO: Warum die DSGVO bislang mehr Bürokratie statt Datenschutz bringt. [Interview with Martin Steiger]. *Netzwoche*. Netzmedien AG. Published May – 25 – 2019, 09:00. https://www.netzwoche.ch/news/2019-05-25/warum-die-dsgvo-bislang-mehr-buerokratie-statt-datenschutz-bringt/0lt0 (last access: 01/18/2024).

Osterwinter, Norbert; Wortmann, Marcus. (2020). Deutsche sind offen für Innovationen und wünschen sich mehr europäische Kooperation. Gütersloh: Bertelsmann Stiftung. https://www.bertelsmann-stiftung.de/de/publikationen/publikation/did/deutsche-sind-offen-fuer-innovationen-und-wuenschen-sich-mehr-europaeische-kooperation (last access: 05/31/2023).

Oud, Malin. (2023). Rule of law. In Oud, Malin; Drinhausen, Katja (eds.). *The Decoding China dictionary*. https://decodingchina.eu/rule-of-law/ (last access: 07/31/2023).

Pernot-Leplay, Emmanuel. (2020). China's approach on data privacy law: A third way between the U.S. and the EU? *Penn State Journal of Law & International Affairs* 8(1). 49–117. https://ssrn.com/abstract=3542820 (last access: 02/21/2024).

Petty, Richard E.; Cacioppo, John T. (1986). The elaboration likelihood model of persuasion. *Advances in Experimental Social Psychology* 19. 123–205. https://doi.org/10.1016/S0065-2601(08)60214-2 (last access: 04/08/2024).

Pilati Rodrigues, Ronaldo; Milfont, Taciano L.; Ferreira, Maria Cristina; Porto, Juliana B.; Fischer, Ronald. (2011). Brazilian Jeitinho: Understanding and explaining an indigenous psychological construct. *Revista Interamericana de Psicología* 45(1). 29–38. https://journal.sipsych.org/index.php/IJP/article/download/134/112/425 (last access: 04/08/2024).

Porto, Juliana B.; Pilati Ronaldo. (2021). Trust in Brazil: The interplay of jeitinho and trust conception. In Kwantes, Catherine T.; Kuo, Ben C. H. (eds.). *Trust and trustworthiness across cultures: Implications for societies and workplaces*. Cham: Springer. 17–32.

Positive Technologies. (2023). Cybersecurity threatscape of African countries 2022–2023. Published July – 28 – 2023. https://www.ptsecurity.com/ww-en/analytics/africa-cybersecurity-threatscape-2022-2023/#id4 (last access: 12/12/2023).

Post, Robert C. (2001). Three concepts of privacy. *The Georgetown Law Journal* 89(6). 2087–2098. https://openyls.law.yale.edu/bitstream/handle/20.500.13051/1114/Three_Concepts_of_Privacy.pdf?sequence=2 (last access: 11/29/2023).

Puaschunder, Julia. (2022). Behavioral International Law: Law-in-books vs. law-in-action resembling the neoclassical economics vs. behavioral economics debate. In Rotaru, Ioan-Gheorghe; Sarwar, Huma (eds.). *RAIS conference proceedings: The 28th International RAIS Conference on Social Sciences and Humanities*. Cambridge, MA: The Scientific Press. 1-9. https://doi.org/10.5281/zenodo.6945854 (last access: 02/06/2024).

Reidenberg, Joel R. (2015). The transparent citizen. *Loyola University Chicago Law Journal* 47(2). 437–463. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2674313 (last access: 10/03/2024).

Richthammer, Martin; Widjaja, Thomas. (2023). Vectors of data disclosure: The information systems perspective. In Hennemann, Moritz; von Lewinski, Kai; Wawra, Daniela; Widjaja, Thomas (eds.). *Data disclosure: Global developments and perspectives*. Berlin: De Gruyter. 35–50. https://doi.org/10.1515/9783111010601-004 (last access: 03/20/2024).

Richthammer, Martin; Widjaja, Thomas. (2024). Assuring or enabling privacy? How different types of regulatory measures for data privacy affect individual disclosure behavior. *ECIS 2024 Proceedings*. 21. https://aisel.aisnet.org/ecis2024/track02_general/track02_general/21 (last access: 07/16/2024).

Robinson, Stephen Cory. (2018). Factors predicting attitude toward disclosing personal data online. *Journal of Organizational Computing and Electronic Commerce* 28(3). 214–233. https://www.tandfonline.com/doi/pdf/10.1080/10919392.2018.1482601 (last access: 11/20/2023).

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

Rosenn, Keith S. (1971). The jeito: Brazil's institutional bypass of the formal legal system and its developmental implications. *The American Journal of Comparative Law* 19(3). 514–549. https://doi.org/10.2307/839559 (last access: 04/08/2024).

Rosenn, Keith S. (1998). *O jeito na cultura jurídica brasileira*. [*Jeito in Brazilian legal culture*]. Rio de Janeiro: Renovar.

Rustad, Michael L.; Koenig, Thomas H. (2019). Towards a global data privacy standard. *Florida Law Review* 71(2). 365–453. https://scholarship.law.ufl.edu/flr/vol71/iss2/3 (last access: 05/27/2024).

Scroope, Chara. (2018). Brazilian culture. *The Cultural Atlas*. https://culturalatlas.sbs.com.au/brazilian-culture (last access: 06/24/2023).

Scroope, Chara. (2021). Japanese culture. *The Cultural Atlas: Core concepts*. https://culturalatlas.sbs.com.au/japanese-culture/japanese-culture-core-concepts (last access: 02/07/2023).

Scroope, Chara; Evason, Nina. (2017). Chinese culture. Core concepts. *The Cultural Atlas.* https://culturalatlas.sbs.com.au/chinese-culture/chinese-culture-core-concepts#chinese-culturecore-concepts (last access: 02/07/2023).

Sonnenberg, Peer. (2024). A regulatory clustering of privacy laws: An approach to quantifying (comparative) law as an instrument for interdisciplinary research. (Extended version). *University of Passau IRDG Research Paper Series* 24(1). https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/ (last access: 04/10/2024).

Sonnenberg, Peer; Hoffmann, Timo. (2022). Data protection revisited: Report on the law of data disclosure in Switzerland. *University of Passau IRDG Research Paper Series* 22(17). https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/ (last access: 12/21/2023).

Swiss Federal Council. (2022). Ordinance on Data Protection (Data Protection Ordinance, DPO). https://www.fedlex.admin.ch/eli/cc/2022/568/en (last access: 05/27/2024).

Takahashi, Bruno. (2019). Why do we have so many social security claims in Brazil? *Shinshu University Economic Law Collection* 5. 91–115. https://soar-ir.repo.nii.ac.jp/record/20650/files/economics_law05-07.pdf (last access: 25/01/2024).

The Culture Factor Group. (2024). Country comparison tool. [last updated: October 16, 2023]. https://www.hofstede-insights.com/country-comparison-tool (last access: 04/26/2024).

The Economist. (2018). Can the EU become another AI superpower? Published Sept – 20 – 2018. https://www.economist.com/business/2018/09/20/can-the-eu-become-another-ai-superpower (last access: 03/05/2024).

The Ghana Report. (2019). Ghana physically secure; now needs to be cyber secure – TripleCyber CEO. Published May – 20 – 2019, 9:29. https://www.theghanareport.com/ghana-physically-secure-now-needs-to-be-cyber-secure-triplecyber-ceo/ (last access: 12/12/2023).

Thir, Veronika; Wawra, Daniela. (2023). Cultural influences on personal data disclosure decisions: Ghanaian perspectives. *University of Passau IRDG Research Paper Series* 23(4). https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/ (last access: 09/25/2023).

Thir, Veronika; Wawra, Daniela; Kindsmüller, Katharina; Vollenschier, Vanessa. (2023). Cultural influences on personal data disclosure decisions: Swiss perspectives. *University of Passau IRDG Research Paper Series* 23(5). https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/ (last access: 09/25/2023).

Trepte, Sabine; Masur, Philipp K. (2017). Privacy attitudes, perceptions, and behaviors of the German population: Research report. In Friedewald, Michael; Ammicht Quinn, Regina; Hansen, Marit; Heesen, Jessica; Hess, Thomas; Lamla, Jörn; Matt, Christian; Roßnagel, Alexander; Trepte, Sabine; Waidner, Michael (eds.). *Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt*. Karlsruhe: Fraunhofer, ISI. https://www.philippmasur.de/documents/pubs/Trepte_Masur_2017_Research_Report_Hohenheim.pdf (last access: 02/05/2024).

Van Norman Law. (2017). Rule of Law vs. Rule by Law. Published April – 28 – 2017. https://vannormanlaw.com/rule-law-vs-rule-law/ (last access: 02/05/2024).

Vorländer, Hans. (2013). Liberalism. In Mauch, Christof; Wersich, Rüdiger B. (eds.). *USA-Lexikon: Schlüsselbegriffe zu Politik, Wirtschaft, Gesellschaft, Kultur, Geschichte und zu den deutsch-amerikanischen Beziehungen*. (2nd edition). Berlin: Erich Schmidt, 631–633.

Wang, Flora. (2020). Cooperative data privacy: The Japanese model of data privacy and the EU-Japan GDPR adequacy agreement. *Harvard Journal of Law and Technology* 33(2). 661–691. https://jolt.law.harvard.edu/assets/articlePDFs/v33/33HarvJLTech661.pdf (last access: 11/16/2023).

Wang, Rui; Hempton, Brian; Dugan, John; Komives, Susan. (2008). Cultural differences: Why do Asians avoid extreme responses? *Survey Practice* 1(3). https://doi.org/10.29115/SP-2008-0011 (last access: 03/26/2023).

Warren, Samuel; Brandeis, Louis. (1890). The right to privacy. *Harvard Law Review* 4(5). 193–220. https://doi.org/10.2307/1321160 (last access: 06/26/2023).

Watson. (2022). Nur noch 6,5 Prozent der jungen Schweizerinnen und Schweizer befürworten EU-Beitritt. Zürich: CH Regionalmedien AG. Published Sept – 23 – 2022, 10:36. https://www.watson.ch/schweiz/schweiz-eu/225624015-nur-noch-6-5-prozent-der-jungen-schweizer-befuerworten-eu-beitritt (last access: 12/14/2023).

Wawra, Daniela. (2022). The cultural context of personal data disclosure decisions. *University of Passau IRDG Research Paper Series* 22(2). https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/ (last access: 09/25/2023).

Wawra, Daniela. (2023a). Data sensitivity and data protection literacy in cross-cultural comparison. In Hennemann, Moritz; von Lewinski, Kai; Wawra, Daniela; Widjaja, Thomas (eds.). *Data disclosure: Global developments and perspectives*. Berlin: De Gruyter. 169–194. https://doi.org/10.1515/9783111010601-010 (last access: 03/20/2024).

Wawra, Daniela. (2023b). Parameters of personal data disclosure decisions in cross-cultural comparison. In Hennemann, Moritz; von Lewinski, Kai; Wawra, Daniela; Widjaja, Thomas (eds.). *Data disclosure: Global developments and perspectives*. Berlin: De Gruyter. 51–88. https://doi.org/10.1515/9783111010601-005 (last access: 03/20/2024).

Wawra, Daniela; Kindsmüller, Katharina; Tawfiq, Memoona; Vollenschier, Vanessa; Walbert, Franziska; Woldrich, Lisa. (2022a). Cultural influences on personal data disclosure decisions: Chinese perspectives. *University of Passau IRDG Research Paper Series* 22(9). https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/ (last access: 11/16/2023).

Wawra, Daniela; Kindsmüller, Katharina; Tawfiq, Memoona; Vollenschier, Vanessa; Walbert, Franziska; Woldrich, Lisa. (2022b). Cultural influences on personal data disclosure decisions: Japanese perspectives. *University of Passau IRDG Research Paper Series* 22(10). https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/ (last access: 11/16/2023).

Wawra, Daniela; Kindsmüller, Katharina; Tawfiq, Memoona; Vollenschier, Vanessa; Walbert, Franziska; Woldrich, Lisa. (2022c). Cultural influences on personal data disclosure decisions: Russian perspectives. *University of Passau IRDG Research Paper Series* 22(11). https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/ (last access: 11/16/2023).

Wawra, Daniela; Kindsmüller, Katharina; Vollenschier, Vanessa; Walbert, Franziska; Woldrich, Lisa. (2022d). Cultural influences on personal data disclosure decisions: Brazilian perspectives. *University of Passau IRDG Research Paper Series* 22(08). https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/ (last access: 11/16/2023).

Wertenbroch, Klaus; Schrift, Rom Y.; Alba, Joseph W.; Barasch, Alixandra; Bhattacharjee, Amit; Giesler, Markus; Knobe, Joshua; Lehmann, Donald R.; Matz, Sandra; Nave, Gideon; Parker, Jeffrey R.; Puntoni, Stefano; Zheng, Yanmei; Zwebner, Yonat. (2020). Autonomy in consumer choice. *Marketing Letters* 31(4). 429–439. https://link.springer.com/article/10.1007/s11002-020-09521-z (last access: 06/05/2023).

Westin, Alan. (2003). Social and political dimensions of privacy. *Journal of Social Issues* 59(2). 431–453. https://doi.org/10.1111/1540-4560.00072 (last access: 06/26/2023).

Whitman, James Q. (2004). The two Western cultures of privacy: Dignity versus liberty. *The Yale Law Journal* 113(6). 1151–1222. https://openyls.law.yale.edu/bitstream/handle/20.500.13051/5038/The_Two_Western_Cultures_of_Privacy___Dignity_versus_Liberty.pdf?sequence=2&isAllowed=y (last access: 05/31/2023).

Zapletal, Jaroslav; Barter, Shane J. (2021). Review of Sebastian Heilmann (ed.) (2017). *China's political system*. Lanham, MD: Rowman & Littlefield. *The Newsletter* 88 (Spring 2021). https://www.iias.asia/the-newsletter/article/chinas-political-system (last access: 11/20/2023).

Zhang, Changqing; Cui, Changqi; Yao, Qi. (2021). "I" am willing to disclose, but "we" are unwilling: The impact of self-construal on individuals' willingness to disclose. *Psychology Research and Behavior Management* 14. 1929-1945. https://doi.org/10.2147/PRBM.S336223 (last access: 11/20/2023).

Zhicheng, Wang. (2018). China – Official data on internet censorship. *AsiaNews.* Fondazione PIME Onlus – AsiaNews. Published Sept – 1 – 2018, 13:56. https://www.asianews.it/news-en/Official-data-on-internet-censorship-42781.html (last access: 02/07/2023).

Zimmermann, Augusto. (2009). Law and society in Brazil: The prevailing perceptions of law in Brazilian society. *International Journal of Private Law* 2(1). 15–30. https://www.inderscienceonline.com/doi/abs/10.1504/IJPL.2009.02151 (last access: 01/22/2024).

Appendix I—Sample details

The main criterion for being included in our sample of data protection professionals was that the individual had to have decision-making authority *or* influence over spending/purchasing in the IT or legal services department of a company or institution. As can be seen in Fig. 80, most respondents (37 %) in the sample were some sort of executive.[61] One-third (33 %) were employed in IT, ICT, or as computer specialists (some of them also holding leadership roles, such as IT directors or heads of IT). Another considerable proportion stated that their current job title was (some sort of) "manager" (e.g., account manager, general manager, project manager, or sales manager; 17 %).

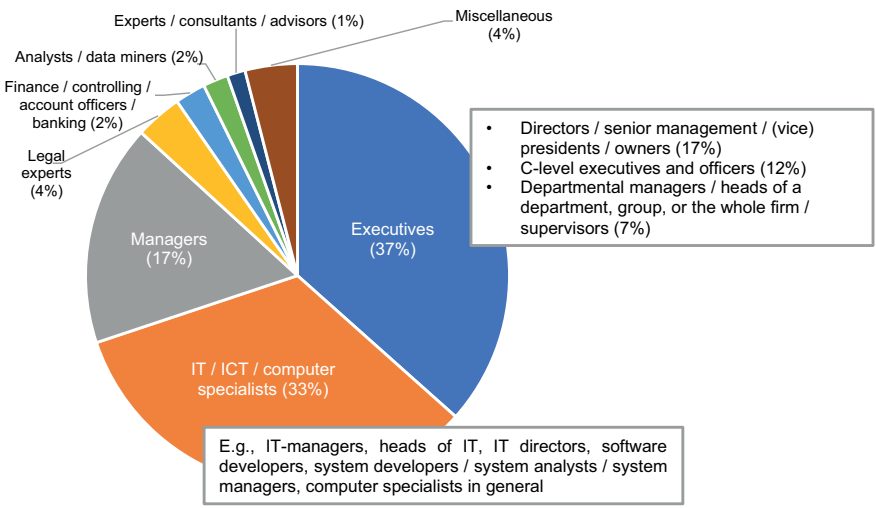

Fig. 80: Job descriptions in the sample.

Most of the 727 respondents in the sample were male (69 %), about one-third were female (31 %), and less than 1 % identified as non-binary (Fig. 81). This tendency was also reflected in the gender distributions of most national subsamples, except for Brazil and China. In the Brazilian subsample, the gender distribution was a lot more even, with 55 % male respondents and 44 % female respondents. In China, two-thirds of respondents (66 %) were female and only 34 % were male.

61 This proportion does not include respondents assuming a leadership role within IT or ICT.

https://doi.org/10.1515/9783111458366-008

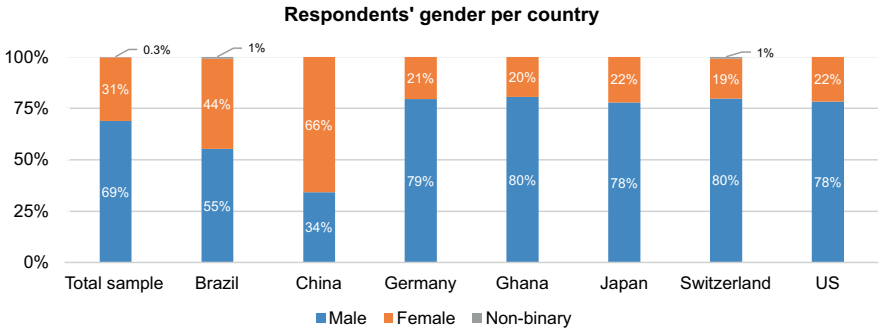

Fig. 81: Gender distribution of the total sample and each national subsample.

The majority of respondents (64 %) were aged 40 years old or younger,[62] with 31–40-year-olds making up the largest age group (38 %; Fig. 82), resulting in a mean age of 37.7 years. This tendency also applied to most countries in the sample, that is, to Brazil (M = 35.5), China (M = 33.2), Germany (M = 38.0), and Switzerland (M = 35.7). In Ghana, the largest group of respondents was aged 18–30 years, and respondents were on average the youngest (M = 31.9 years). In Japan and the United States, the majority of respondents were aged over 40 years (74 % and 51 % respectively). Accordingly, Japanese respondents were on average the oldest (M = 47.2), followed by US respondents (M = 41.2).

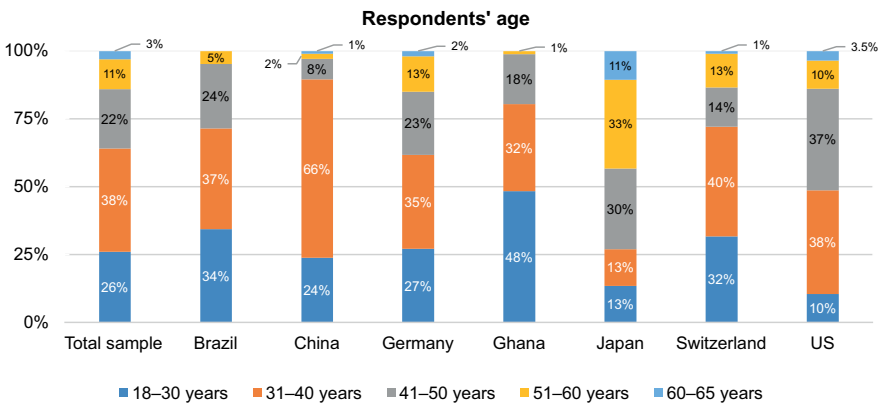

Fig. 82: Age distribution of the total sample and each national subsample.

62 The minimum age was 18, the maximum age was 65.

Furthermore, the vast majority of respondents (90 %) lived in urban regions, while only 10 % resided in rural regions at the time of the survey (Fig. 83). This tendency applied to all national subsamples, but was least pronounced in Switzerland, where almost a quarter of respondents (24 %) lived in a rural region. By contrast, in Brazil and China, all respondents were located in urban regions.

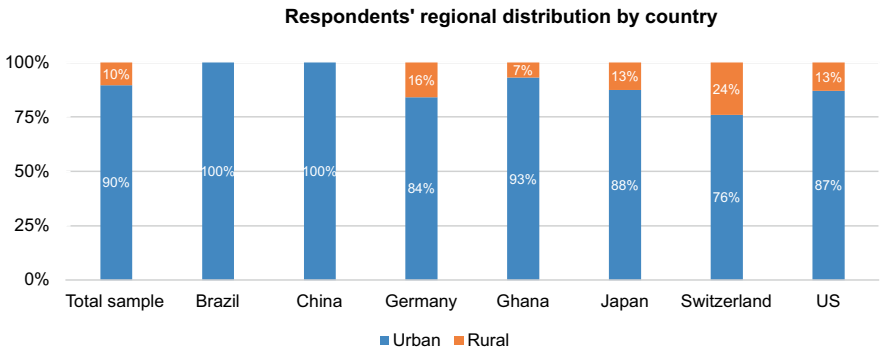

Fig. 83: Regional distribution of the total sample and each national subsample.

The vast majority of respondents in the sample (84 %) were highly educated, having completed higher education (that is, an education equivalent to a bachelor's, master's, or doctoral degree; Fig. 84). This tendency held true for all national subsamples. In all countries, a majority of respondents were graduates of higher education, and in most countries, this majority amounted to more than 80 % (89 % in Brazil, 99 % in China, 82 % in Ghana, 83 % in Japan, and 88 % in the United States). In Germany and Switzerland, "only" 71 % and 74 % of respondents respectively had completed higher education, but in both countries, the proportion of respondents with a master's degree was comparatively high, at 35 % and 38 % respectively. The proportion of master's graduates was highest in the US sample, at 50 %.

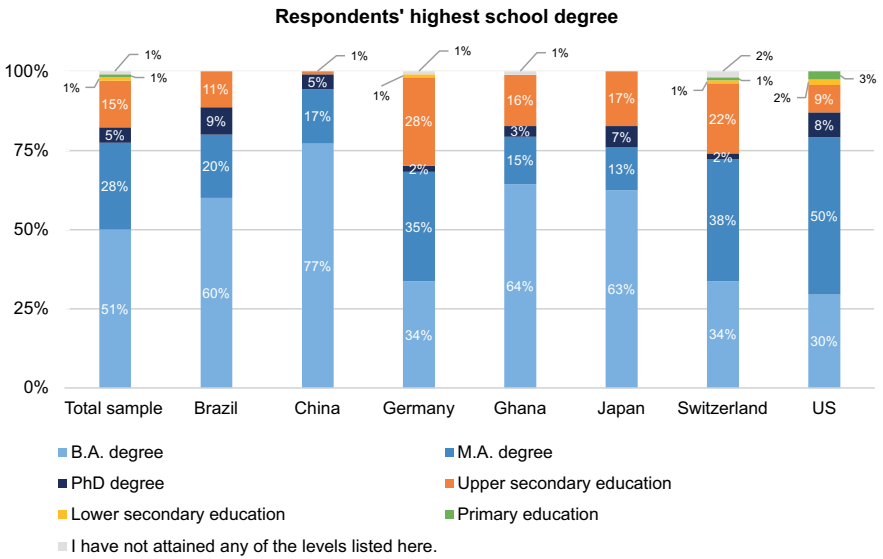

Fig. 84: Distribution of education levels in the total sample and each national subsample.

Appendix II—Questionnaire

Q1: To what extent do you agree or disagree with the following statements:

	strongly agree	somewhat agree	neither agree nor disagree	somewhat disagree	strongly disagree
(r1) In general, consumers should have the possibility to make self-determined decisions about the disclosure of their personal data.	○	○	○	○	○
(r2) In general, consumers in my country can make self-determined decisions about the disclosure of their personal data.	○	○	○	○	○

Q2: In your expert opinion, are consumers in your country sometimes restricted in their data autonomy (i.e. they cannot always make self-determined decisions about the disclosure of their personal data)?

○	Yes, in the following ways: _____
○	No.

Q3: Legislation in my country is ... to ensure consumers' self-determined decisions about the disclosure of their personal data.

sufficient	rather sufficient	neutral	rather insufficient	insufficient
○	○	○	○	○

Q4: Are there certain types of data (e.g., health data, financial data, personal identification numbers, etc.) for which you think the regulation of data protection and informational privacy should be ...

○	stricter: _____
○	weaker: _____
○	No adjustments are necessary.

https://doi.org/10.1515/9783111458366-009

Q5: Are there certain contexts of data disclosure (e.g., when using smartphone apps, when disclosing data to foreign governments, etc.), for which you think the regulation of data protection and informational privacy should be …

○	stricter: _____
○	weaker: _____
○	No adjustments are necessary.

Q6: Are there certain purposes of data collection (e.g., law enforcement, medical research, marketing, etc.) for which you think the regulation of data protection and informational privacy should be …

○	stricter: _____
○	weaker: _____
○	No adjustments are necessary.

Q7: Are there certain industries (e.g., healthcare, social media companies, financial sector, etc.) for which you think the regulation of data protection and informational privacy should be …

○	stricter: _____
○	weaker: _____
○	No adjustments are necessary.

Q8: In your expert opinion, how aware are consumers of the regulation of data protection and informational privacy in your country?[63]

very aware	rather aware	rather not aware	not aware at all
○	○	○	○

63 Adapted from CIGI-Ipsos (2019a, 8, 2019b, 281).

Q9: In general, consumers do enough to protect their personal data.[64]

strongly agree	somewhat agree	neither agree nor disagree	somewhat disagree	strongly disagree
○	○	○	○	○

Q10: Please indicate on a scale from 1 (not at all sensitive) to 5 (very sensitive) how sensitive you consider the following data to be. Please also indicate whether the data category should be or stay included in the definition of sensitive data in your country's legal framework.[65]

	1 not at all sensitive	2 not sensitive	3 neutral	4 sensitive	5 very sensitive	Please select the categories that should be or stay included in the definition of sensitive data in your country's legal framework:
religious beliefs	○	○	○	○	○	☐
religious activities	○	○	○	○	○	☐
health data	○	○	○	○	○	☐
genetic information	○	○	○	○	○	☐
biometric information	○	○	○	○	○	☐
sex life	○	○	○	○	○	☐
gender identity	○	○	○	○	○	☐
ethnicity or race	○	○	○	○	○	☐
political views	○	○	○	○	○	☐
political activities	○	○	○	○	○	☐
union membership	○	○	○	○	○	☐
union activity	○	○	○	○	○	☐
membership in a philosophical organization	○	○	○	○	○	☐

64 Adapted from CIGI-Ipsos (2019a, 29; 2019b, 283).

65 The 33 data categories were presented in randomized order.

	1 not at all sensitive	2 not sensitive	3 neutral	4 sensitive	5 very sensitive	Please select the categories that should be or stay included in the definition of sensitive data in your country's legal framework:
philosophical beliefs	○	○	○	○	○	☐
criminal records	○	○	○	○	○	☐
data on having been the victim of a crime	○	○	○	○	○	☐
personal information of a minor	○	○	○	○	○	☐
financial data in general	○	○	○	○	○	☐
income	○	○	○	○	○	☐
assets	○	○	○	○	○	☐
social security measures	○	○	○	○	○	☐
location (tracking)	○	○	○	○	○	☐
personal identification number	○	○	○	○	○	☐
account login	○	○	○	○	○	☐
digital signature	○	○	○	○	○	☐
correspondence records	○	○	○	○	○	☐
contents of correspondences	○	○	○	○	○	☐
citizenship or immigrant status	○	○	○	○	○	☐
property information	○	○	○	○	○	☐
social status	○	○	○	○	○	☐
website activity	○	○	○	○	○	☐
browsing history	○	○	○	○	○	☐
diet	○	○	○	○	○	☐

Q11: To what extent do you agree or disagree with the following statements:

	strongly agree	somewhat agree	neither agree nor disagree	somewhat disagree	strongly disagree
(r1) Companies should only be allowed to collect consumers' personal data with their consent.	○	○	○	○	○
(r2) Companies should always be required to provide deletion options for personal data so that consumers can delete their personal data at any time should they change their mind about the disclosure.	○	○	○	○	○
(r3) Companies should always be required to state explicitly what consumers' personal data will be used for.	○	○	○	○	○
(r4) Companies should always be required to ask again for consumers' consent when using their data for purposes other than previously stated.	○	○	○	○	○

Q12: To what extent, if at all, do you trust the following institutions to use consumers' personal data in the right way?[66]

	a great deal	a fair amount	rather little	not at all
Healthcare providers	○	○	○	○
Financial services companies	○	○	○	○
Shipping/delivery companies	○	○	○	○
Telecommunications companies	○	○	○	○
Retailers selling goods and services	○	○	○	○
Search and social media sites	○	○	○	○
Media companies	○	○	○	○
The national government	○	○	○	○
Foreign governments	○	○	○	○

66 Adapted from Ipsos (2019, 18–20).

Q13: How would you assess compliance with the regulation of consumer data protection and informational privacy in your country by the following industries?[67]

	sufficient	rather sufficient	neutral	rather insufficient	insufficient
Healthcare providers	○	○	○	○	○
Financial services companies	○	○	○	○	○
Shipping/delivery companies	○	○	○	○	○
Telecommunications companies	○	○	○	○	○
Retailers selling goods and services	○	○	○	○	○
Search and social media sites	○	○	○	○	○
Media companies	○	○	○	○	○

Q14: How would you assess the enforcement of consumer data protection by the government in your country? It is enforced[68]

heavily	robustly	moderately	to a limited extent	not at all
○	○	○	○	○

Q15: How would you assess the enforcement of consumer data protection by private parties in your country? It is enforced

heavily	robustly	moderately	to a limited extent	not at all
○	○	○	○	○

Q16: How would you assess the enforcement of consumer data protection within companies in your country? It is enforced

heavily	robustly	moderately	to a limited extent	not at all
○	○	○	○	○

67 Industries taken from Ipsos (2019, 18–20).

68 The first four answer options are adapted from the categories used in DLA Piper (2023).

Q17: How would you assess the level of consumer data protection in your country for the following industries?[69]

	sufficient	rather sufficient	neutral	rather insufficient	insufficient
Healthcare providers	○	○	○	○	○
Financial services companies	○	○	○	○	○
Shipping/delivery companies	○	○	○	○	○
Telecommunications companies	○	○	○	○	○
Retailers selling goods and services	○	○	○	○	○
Search and social media sites	○	○	○	○	○
Media companies	○	○	○	○	○

Q18: Current regulation in my country is ... to ensure that companies do not misuse consumers' personal data for purposes other than those stated.

sufficient	rather sufficient	neutral	rather insufficient	insufficient
○	○	○	○	○

Q19: Do you agree or disagree that the regulation of data protection and informational privacy in your country still allows companies

	strongly agree	somewhat agree	neither agree nor disagree	somewhat disagree	strongly disagree
(r1) to tailor their products and services to consumers' needs	○	○	○	○	○
(r2) to develop new products and services	○	○	○	○	○
(r3) to cooperate with other companies in your country	○	○	○	○	○

69 Industries taken from Ipsos (2019, 18–20).

	strongly agree	somewhat agree	neither agree nor disagree	somewhat disagree	strongly disagree
(r4) to cooperate with companies in other countries with essentially equivalent regulation of data protection and informational privacy	○	○	○	○	○
(r5) to cooperate with companies in other countries, no matter what their regulation of data protection and informational privacy is	○	○	○	○	○

Q20: To what extent do you agree or disagree with the following statements:

	strongly agree	somewhat agree	neither agree nor disagree	somewhat disagree	strongly disagree
(r1) The regulation of data protection and informational privacy in my country creates too much bureaucracy for the state.	○	○	○	○	○
(r2) The regulation of data protection and informational privacy in my country creates too much bureaucracy for companies.	○	○	○	○	○
(r3) The regulation of data protection and informational privacy in my country creates too much bureaucracy for consumers.	○	○	○	○	○
(r4) The regulation of data protection and informational privacy in my country creates too much information overload for consumers.	○	○	○	○	○
(r5) The regulation of data protection and informational privacy in my country has led to a more professional handling of data by companies.	○	○	○	○	○
(r6) The regulation of data protection and informational privacy in my country enables consumers to easily manage their privacy needs.	○	○	○	○	○

Q21: In your expert opinion, the current regulation of data protection and informational privacy in your country is ... to protect the fundamental rights of individuals.

sufficient	rather sufficient	neutral	rather insufficient	insufficient
○	○	○	○	○

Q22: In your expert opinion, the regulation of data protection and informational privacy in your country has a ... effect on digital development and the implementation of digital innovations.

very positive	positive	neutral	negative	very negative
○	○	○	○	○

Q23: Overall, the regulation of data protection and informational privacy in your country has a ... .[70]

positive impact	neutral impact	negative impact
○	○	○

70 Adapted from Cisco (2021, 10).